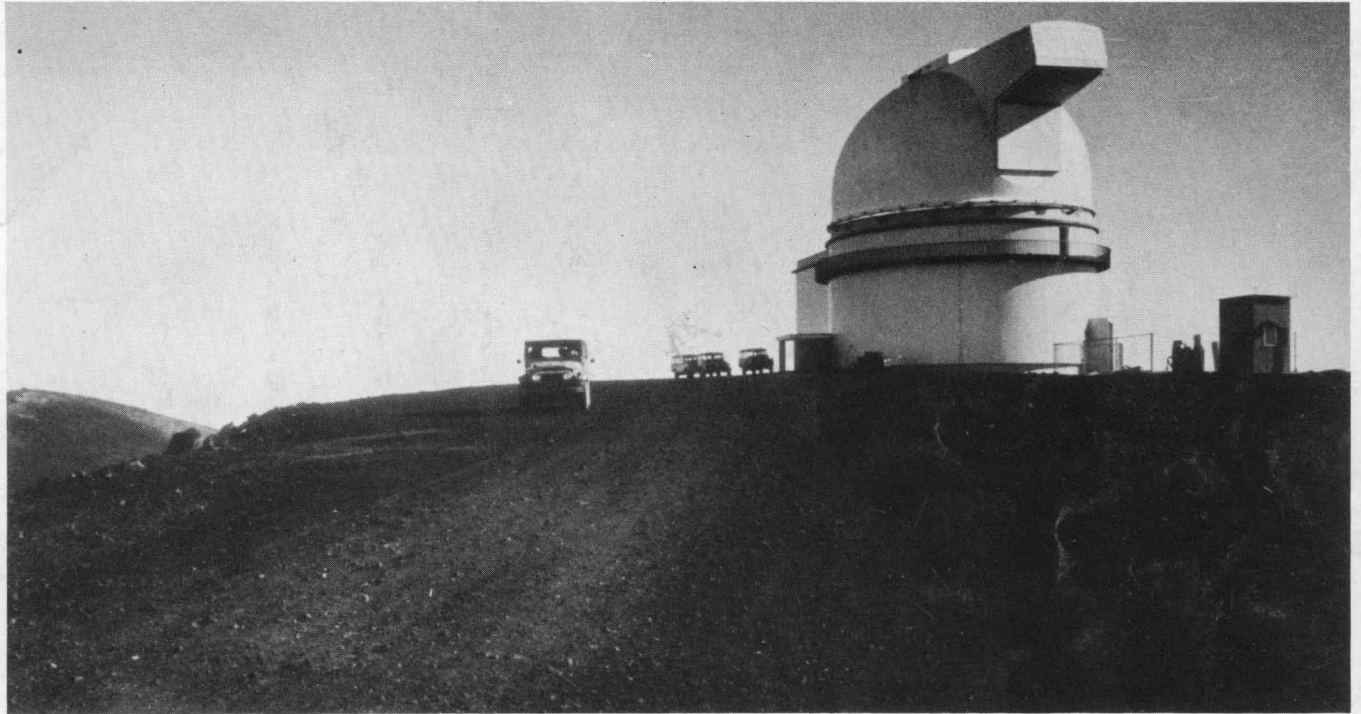


April, 1972

Vol. 21, No. 4

computers and automation



COMPUTERIZED OBSERVATORY AT MAUNA KEA, ON THE ISLAND OF HAWAII

"Do What I Mean": The Programmer's Assistant
Cryptology, The Computer, and Data Privacy
Computerizing a Membership Organization
The Information Industry and Government Policy
The Bad Image That Computers Are Earning

Political Lies: An Acceptable Level?

- W. Teitelman
- M. B. Girsdansky
- W. R. Pollert
- C. T. Whitehead
- H. W. G. Gearing,
and others
- A. E. Kahn

SAN TECH180 1P02121147F6 7301
~~SAN JOSE PUBLIC LIBRARY~~ *N
 TECHNICAL SERVICES 00808
 180 W SAN CARLOS ST ■■
 SAN JOSE CA 95113

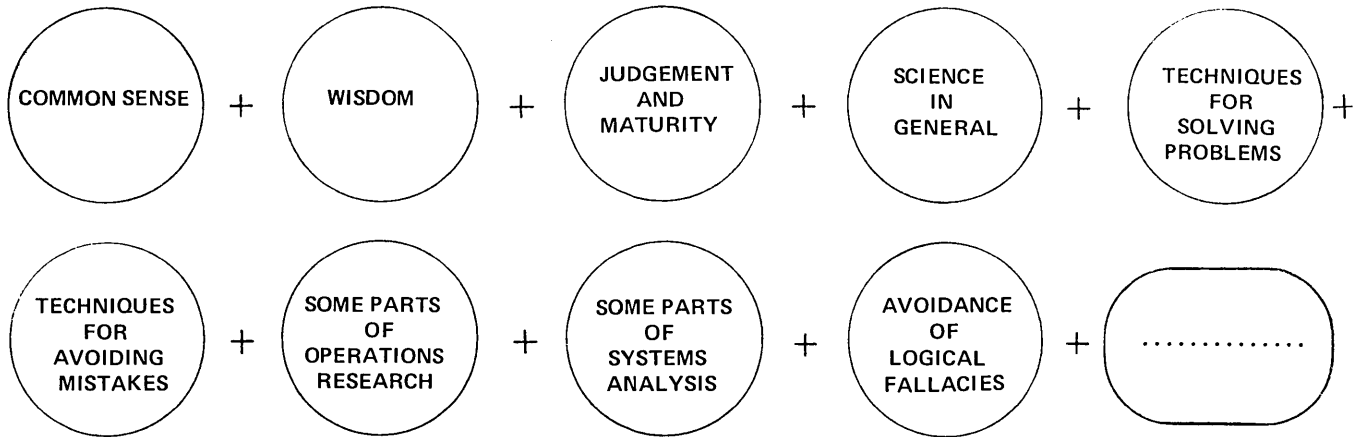
DO YOU WANT TO PREVENT MISTAKES BEFORE THEY HAPPEN?

- avoid pitfalls?
- find new paths around old obstacles?
- apply in practical situations the observations and wisdom of great scientists and wise men?
- stimulate your resourcefulness?
- see new solutions to old problems?
- distinguish between sense and nonsense?
- increase your accomplishments?
- improve your capacities?

IF SO, TRY -

The C&A Notebook on COMMON SENSE, ELEMENTARY AND ADVANCED

devoted to research, development, exposition, and illustration of one of the most important of all branches of knowledge, i.e. the subject of -
WHAT IS GENERALLY TRUE AND IMPORTANT =



Editor: Edmund C. Berkeley, author, businessman, actuary, scientist, computer professional, first secretary of the Association for Computing Machinery 1947-53, editor of *Computers and Automation*.

RETURNABLE IN 7 DAYS FOR FULL REFUND, IF NOT SATISFACTORY —

WHY NOT TAKE A LOOK?HOW CAN YOU LOSE?

THE FIRST SIX ISSUES ARE FREE — see the coupon — THE NEXT 21 ISSUES ARE:

- | | |
|--|--|
| 7. The Elephant and the Grassy Hillside | 17. Doomsday in St. Pierre, Martinique — Common Sense vs. Catastrophe |
| 8. Ground Rules for Arguments | 18. The History of the Doasyoulikes |
| 9. False Premises, Valid Reasoning, and True Conclusions | 19. Individuality in Human Beings,... |
| 10. The Investigation of Common Sense, Elementary and Advanced | 20. How to be Silly |
| 11. Principles of General Science, and Proverbs | 21. The Three Earthworms |
| 12. Common Sense — Questions for Consideration | 22. The Cochrans vs. Catastrophe |
| 13. Falling 1800 Feet Down a Mountain | 23. Preventing Mistakes from Forgetting |
| 14. The Cult of the Expert | 24. What is Common Sense? — An Operational Definition |
| 15. Preventing Mistakes from Failure to Understand | 25. The Subject of "What is Generally True and Important": Common Sense, Elementary and Advanced |
| 16. The Stage of Maturity and Judgment in any Field of Knowledge | 26. Natural History, Patterns, and Common Sense |
| | 27. Rationalizing and Common Sense |

— (may be copied on any piece of paper) —

To: COMPUTERS AND AUTOMATION
815 Washington St., R5, Newtonville, Mass. 02160

- () YES, please enter my subscription to the C&A Notebook on Common Sense at \$12 a year, 24 issues (newsletter style), and extras.
- () Please send me (as FREE premiums for subscribing) the first six issues:
- | | |
|--|---------------------------------|
| 1. Right Answers — A Short Guide to Obtaining Them | 4. Strategy in Chess |
| 2. The Empty Column | 5. The Barrels and the Elephant |
| 3. The Golden Trumpets of Yap Yap | 6. The Argument of the Beard |
- () I enclose \$ _____ () Please bill me () Please bill my organization

Name _____ Title _____
Organization _____
Address _____
Signature _____ Purchase Order No. _____

QUESTIONS AND ANSWERS

about "The C&A Notebook on COMMON SENSE, ELEMENTARY AND ADVANCED"

INTERESTING: Q: Is the Notebook interesting?

A: We think so — but you can judge for yourself. You can see the issues, and if not satisfactory, tell us to discontinue your subscription.

EXCITING: Q: Is the Notebook exciting?

A: Some of the issues, like "Falling 1800 Feet Down a Mountain" and "Doomsday in St. Pierre, Martinique", are among the most exciting true stories we know.

USEFUL: Q: Is the Notebook useful?

A: It ought to be useful to anybody — as useful as common sense. There exists no textbook on common sense; the Notebook tries to be a good beginning to common sense, science, and wisdom.

UNDERSTANDABLE: Q: Can I understand the Notebook?

A: Yes. It is nontechnical — written in everyday language and using vivid examples.

COVERAGE: Q: Do you cover in the Notebook all parts of common sense, wisdom, and science in general?

A: Yes, we plan to. The main subjects so far are: systematic prevention of mistakes; avoiding certain fallacies; important principles; important concepts; illustrative anecdotes; etc.

MISTAKES: Q: Will the Notebook save me from making important mistakes?

A: It ought to. One of the main purposes of the Notebook is preventing mistakes.

COST: Q: Will the Notebook be worth the cost to me?

A: At about 40 cents per issue (30 issues for \$12), it is hard for you to lose out. EVEN ONE important mistake prevented, may save you much time, much trouble, and much money.

GUARANTEE: Q: If I do not like the Notebook, can I cancel at any time?

A: Yes. You will receive a refund for the unmailed portion of your subscription.

A reprint from
computers
and automation

FOUR-STAR REPRINT

SCIENCE AND THE ADVANCED SOCIETY, by C. P. Snow, Ministry of Technology, London, England (April, 1966 issue of Computers and Automation).
THE INFORMATION REVOLUTION AND THE BILL OF RIGHTS, by Dr. Jerome B. Wiesner, M.I.T. (May, 1971)
EMPLOYMENT, EDUCATION, AND THE INDUSTRIAL SYSTEM, by Prof. John Kenneth Galbraith, Harvard Univ. (Aug. 1965)
COMPUTERS AND THE CONSUMER, by Ralph Nader Washington, D.C. (Oct. 1970)

NUMBER OF ISSUES PER YEAR: Q: How many issues a year do you put out?

A: We promise 24 (newsletter style); we anticipate putting out 30 in each yearly volume.

PAST ISSUES: Q: I do not want to miss past issues. How do I get them?

A: Every subscriber's subscription starts at Vol. 1, no. 1. Every subscriber eventually receives all issues. Here is how it works. The past issues are sent him four at a time, every week or two, until he has caught up — and thus he does not miss important and interesting issues that never go out of date.

BOOK: Q: Are you going to publish all the issues of Volume 1 together as a book?

A: No; they do not fit together into a book.

PREMIUMS: Q: If I subscribe at the same time to "Computers and Automation", can I receive a premium for subscribing to the Notebook?

A: Yes, the Four Star Reprint — see the description below.

Q: Can I receive the 6 free issues (No. 1 to 6 of the Notebook) without subscribing?

A: No. Here is what happens. You subscribe. We send you 8 issues and bill you. You can send them all back in seven days, and the bill is canceled. If you do pay the bill, you receive the 6 free issues, 24 more issues of Vol. 1, and six issues of Vol. 2, no. 1 to 6.

----- (may be copied on any piece of paper) -----

TO: Computers and Automation
815 Washington St., Newtonville, Mass. 02160

() YES, you have convinced me to try the Notebook on Common Sense, Elementary and Advanced. Please enter my subscription at \$12 a year, 24 issues, newsletter style, and extras.

() Please send me Issues 1 to 6 as FREE PREMIUMS for subscribing.

() Please enter my subscription to "Computers and Automation" at the same time () with directory \$18.50; () without directory \$9.50, and send my FREE premium, the Four Star Reprint.

() I enclose \$_____.

() Please bill me.

() Please bill my organization.

RETURNABLE IN SEVEN DAYS FOR FULL REFUND
IF NOT SATISFACTORY

Name _____

Title _____

Organization _____

Address _____

Signature _____ P.O. No. _____

Editor Edmund C. Berkeley

Assistant Editors Barbara L. Chaffee
Linda Ladd Lovett
Neil D. Macdonald

Software Editor Stewart B. Nelson

Advertising Director Edmund C. Berkeley

Art Director Ray W. Hass

Publisher's Assistant Paul T. Moriarty

Contributing Editors John Bennett
Moses M. Berlin
Andrew D. Booth
John W. Carr III
Ned Chapin
Alston S. Householder
Leslie Mezei
Ted Schoeters
Richard E. Sprague

Advisory Committee James J. Cryan
Alston S. Householder
Bernard Quint

Editorial Offices Berkeley Enterprises, Inc.
815 Washington St.,
Newtonville, Mass. 02160
617-332-5453

Advertising Contact THE PUBLISHER
Berkeley Enterprises, Inc.
815 Washington St.,
Newtonville, Mass. 02160
617-332-5453

"Computers and Automation" is published monthly, 12 issues per year, at 815 Washington St., Newtonville, Mass. 02160, by Berkeley Enterprises Inc. Printed in U.S.A. Second Class Postage paid at Boston, Mass.

Subscription rates: United States, \$9.50 for one year, \$18.00 for two years. Canada: add 50 cents a year for postage; foreign, add \$3.50 a year for postage.

NOTE: The above rates do not include our publication "The Computer Directory and Buyers' Guide"; see "Directory Notice" on the page stated in the Table of Contents. If you elect to receive "The Computer Directory and Buyers' Guide", please add \$9.00 per year to your subscription rate.

Please address all mail to: Berkeley Enterprises Inc., 815 Washington St., Newtonville, Mass. 02160.

Postmaster: Please send all forms 3579 to Berkeley Enterprises Inc., 815 Washington St., Newtonville, Mass. 02160.

© Copyright 1972, by Berkeley Enterprises, Inc.

Change of address: If your address changes, please send us both your new address and your old address (as it appears on the magazine address imprint), and allow three weeks for the change to be made.

computers and automation

The magazine of the design, applications, and implications of information processing systems — and the pursuit of truth in input, output, and processing.

Computers and Programming

8 "DO WHAT I MEAN": THE PROGRAMMER'S ASSISTANT [T A]

by Warren Teitelman, Bolt Beranek and Newman, Cambridge, Mass.

How to design and implement in a computer, a "programmer's assistant", so that the sometimes mistaken and often experimental behavior of a human programmer is handled with the least waste of his time and effort.

12 CRYPTOLOGY, THE COMPUTER, AND DATA PRIVACY [T A]

by M. B. Girsdansky, IBM Research Division, Yorktown, Heights, N.Y.

An exploration of how to use the principles and technology of secret or "hidden" writing, in order to secure privacy in computerized records through computer programming.

The Computer Industry

24 THE INFORMATION INDUSTRY AND GOVERNMENT POLICY [NT A]

by Clay T. Whitehead, Director, Office of Telecommunications Policy, Executive Office of the President, Washington, D.C.

A survey of regulation, competition, and other new forms of economic interaction in the field of communications and computers.

21 COMPUTERIZING A MEMBERSHIP ORGANIZATION [NT A]

by William R. Pollert, National Association of Manufacturers, Washington, D.C.

How a large membership association planned and implemented a computer facility using a time-sharing system.

35 THE MEANING OF AN INTEGRATED DATA SYSTEM [T A]

by W. R. Larson, Western Electric, Corporate Education Center, Princeton, N.J.

A proposed definition of an integrated data system for an organization, with special attention given to the areas of data storage and retrieval and improvement of system performance.

29 THE BAD IMAGE THAT COMPUTERS ARE EARNING [NT A]

by H. W. G. Gearing, Worcester, England — and others
Half a dozen examples, in Great Britain and the U.S., of fouled-up computer output and exasperated customers.

The Computer Industry (continued)

- 7 **On the Legal Side: THE OUTSIDE DIRECTOR** [NT F]
by Milton R. Wessel, Attorney, New York, N.Y.
- 7 **"COMPUTERS ENTER THE BUSING CONTROVERSY" – ADDENDUM** [NT F]
by Robert L. Glass, Kent, Wash.
- 34 **INTERNAL REVENUE SERVICE: USE OF COMPUTERS** [NT F]
by William H. Stewart, Jr., University of Alabama
- 31 **IBM'S POWERFUL PARTNER: THE ACCOUNTING PRINCIPLES BOARD** [NT F]
Samson Science Corp., New York, N.Y.
- 31 **DO YOU WANT TO STOP CRIME?** [NT F]
by William P. Wood, III, Richmond, Va.
- 32 **CDC VS IBM – CORRECTION** [NT F]
by F. O. Parlova, New York, and the Editor
- 33 **Fall Joint Computer Conference: Topics** [NT F]
Edmund C. Berkeley, Editor, *Computers and Automation*
- 20 **"The 1972 Computer Directory and Buyers' Guide"** [T G]

The Selection of Personnel – for Computers and Other Purposes

- 26 **PICTORIAL REASONING TESTS – PART 5** [NT F]
by Neil Macdonald, Assistant Editor
- 27 **Pictorial Reasoning Test – C&A No. 6** [NT F]

Common Sense, Wisdom, Science in General, and Computers

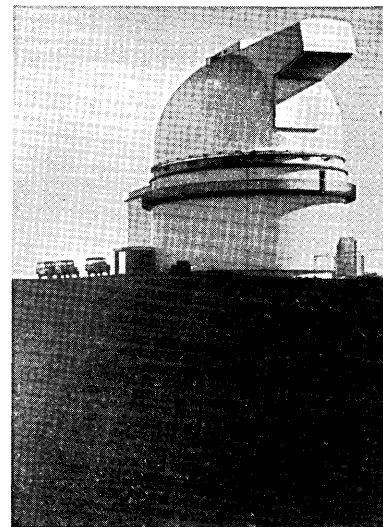
- 6 **The Old Brain, The New Brain, The Giant Brain and Common Sense** [NT E]
by Edmund C. Berkeley, Editor
- 2 **The C&A Notebook on Common Sense** [NT G]
- 3 **Questions and Answers About "The C&A Notebook"** [NT G]

The Profession of Information Engineer and the Pursuit of Truth

- 37 **DALLAS: WHO, HOW, WHY? – Part II** [NT A]
by Mikhail Sagatelyan, Moscow, USSR
A report published in Leningrad, USSR, by an ace Soviet reporter about the circumstances of the assassination of President John F. Kennedy and their significance from a Soviet point of view: Part 2.
- 44 **Political Lies: An Acceptable Level?** [NT A]
by Richard M. Nixon, J. W. Fulbright, and others
- 33 **A Concerted Campaign To Deny the American People Essential Knowledge About the Operation of Their Government** [NT G]
by Prof. Henry Steele Commager, Amherst, Mass.
- 32 **Reducing and Dismantling Science and Research Institutions, and Social Responsibility** [NT G]
by A. G. Michalitsanos, Cambridge, England
- 7 **Dealing With Today's Problems** [NT F]
by John Skowronski, DPMA, Kansas City, Mo.
- 34 **Some Responsibility for Our Chaotic Society** [NT G]
by S. R. Harrison, Trondheim, Norway
- 34 **Unsettling, Disturbing, Critical . . .** [NT F]
Statement of policy by "Computers and Automation"

Computers, Games, and Puzzles

- 36, 43 **Numbles**, by Neil Macdonald [T C]
- 49 **Problem Corner**, by Walter Penney, CDP [T C]



Front Cover Picture

The front cover shows the Mauna Kea Observatory, highest in the world at 13,796 feet above sea level, on the Island of Hawaii on the top of an inactive volcano. The 88-inch telescope and the dome aperture are controlled by an IBM 1800 data acquisition and control system. The system now responds automatically to star motion and the air distortion along the line of sight, and will eventually respond automatically to temperature, humidity, and wind speed.

Departments

- 49 **Advertising Index**
- 20 **Calendar of Coming Events**
- 32 **Correction**
- 48 **Monthly Computer Census**
- 46 **New Contracts**
- 47 **New Installations**

Key

- [A] – Article
- [C] – Monthly Column
- [E] – Editorial
- [F] – Forum
- [G] – The Golden Trumpet
- [NT] – Not Technical
- [T] – Technical

The Old Brain, The New Brain, The Giant Brain, and Common Sense

All computer people from time to time think about brains — those interesting and complex devices made out of common chemicals that we human beings and other animals carry around inside our heads and by means of which we think.

The prototype brain began in the course of evolution more than 400 million years ago. As mammals and birds developed, their brains became very efficient instruments. These brains accept thousands of simultaneous impressions from one or more senses, and make use of a built-in yet trainable evaluating function. The evaluating function uses observations, context, surroundings, instincts, learned experiences, and other information in order to make decisions. The decisions are the ordinary everyday decisions that are useful and relevant to solving the age-old problems of surviving:

- How to recognize and avoid danger;
- How to find and choose food and shelter;
- How to satisfy other wants, how to mate, etc.

This brain is what I like to call "the old brain". It is present, of course, in all human beings. Two of its most remarkable parts are: the way it deals with streams of multiple input sensations; and the evaluating function. Together these parts enable the animal to decide swiftly and almost automatically what to do next and how fast he or she should do it. The output of the old brain is a great quantity of "common sense" behavior — consisting mainly of directions to the body for survival purposes.

At some point more than one million years ago (and probably not more than 10 million years ago) a branch of the primates began to develop a new brain. The new brain has produced language, words to refer to ideas, tool making, culture, the invention of symbols and writing, the solving of problems by using symbols, and much more. The new brain is able to analyze problems into many logical steps, to talk about these steps, to imagine these steps in different arrangements. Most extraordinary of all, the new brain possesses the equipment (unlike any other animal except perhaps the dolphin) to deal with the meanings of tens of thousands of words. The output of the new brain, when brought up in an environment of education and civilization, is intellectual behavior that no other species of animal can come close to producing.

The origin of the new brain is illuminated in the following quotation from "The Naked Ape" by Desmond Morris (a fascinating book):

Of all the non-specialists, the monkeys and the apes are perhaps the most opportunist. As a group, they have specialized in non-specialization. And among the monkeys and apes, the naked ape is the most supreme opportunist of them all. ... All young monkeys are inquisitive but the intensity of their curiosity tends to fade

as they become adult. With us the infantile inquisitiveness is strengthened and stretched into our mature years. We never stop investigating. We are never satisfied that we know enough to get by. Every question we answer leads on to another question. This has become the greatest survival trick of our species. For the opportunist the going may always be rough, but the creature will be able to adapt quickly to any quick-change act that the environment decides to put on.

The new brain, in spite of its power, has some severe limitations. It seems to be able to pay attention to only one idea at a time, while the old brain seems to be able to pay attention to many aspects of the environment simultaneously and to react almost immediately to any suddenly disturbing event, like something noticed out of the corner of one's eye. The new brain makes far more mistakes than the old brain. The new brain seems to have rather a small memory — at least, only when human beings make use of external recording can they remember more than a small part of what they consciously want to remember. The old brain in contrast seems to have a very large amount of information ready for use, especially in emergencies. And the new brain seems not to have access to all the information stored in the old brain.

The giant brain of course is the computer. The phrase has been applied to computers since 1949. The giant brain is strictly an imitation of the new brain. It is not at all an imitation of the old brain — because it does not automatically receive thousands of sense impressions per second; it does not automatically integrate these impressions into representations of the environment; it does not automatically operate an evaluating function which solves the problem of living and surviving from moment to moment.

Like the new brain, the giant brain deals with symbols; it performs operations of logic and arithmetic in enormous quantities, and at a speed that is on the order of a million times the speed of human beings.

"Common sense" behavior is what an animal displays when he is using his old brain: the sense to avoid danger, to find and choose food, to survive according to the bag of survival tricks developed by his species.

Computers are enormously busy in these days performing the functions of the new brain. We are just beginning to apply computers to performing the functions of the old brain — as in optical character recognition. It is time to pay more attention to the construction of computers that will perform adequately the functions of the old brain, and produce "common sense" behavior.

Edmund C. Berkeley

Editor

On The Legal Side: THE OUTSIDE DIRECTOR

*Milton R. Wessel, Attorney
New York, N.Y.*

A person who accepts election as an "outside director" of a public company merely for honor or prestige, is making a serious mistake.

During the last decade a host of litigations have made very clear that a director — outside or inside — has affirmative personal responsibility to a large number of persons, including stockholders, employees, suppliers, customers, and the public generally. Often the standard corporate indemnification arrangement will not help him where he fails to perform that responsibility, and he must pay money damages and in extreme cases even suffer criminal conviction. The fact that the organization involved is a church, hospital, college or other non-profit organization does not relieve him of even a shred of his responsibility.

What is the director's responsibility? A complete answer requires a book, and much has been written. The short, practical answer here is that a director must act reasonably under the circumstances; he must act as one would expect a director to act. Section 717 of the New York Business Corporation Law puts it thus:

"Directors and officers shall discharge the duties of their respective positions in good faith and with that degree of diligence, care, and skill which ordinarily prudent men would exercise under similar circumstances in like positions."

All of this means that the outside director must pay sufficient attention to the business to satisfy his responsibility. He cannot successfully defend against liability by saying, "I didn't know" or "I didn't attend meetings" or "They wouldn't give me the financial data I asked for". For example, a director of a computer company, whose programs and banks of data are its main asset, should satisfy himself that they are reasonably protected against fire and fraud. If he does not and the company is wiped out, he may be liable to shareholders for negligence. He can't just sit and wait for management to ask for his approval of a security program.

Nor can a director avoid liability by closing his eyes to facts about which he should know. If he hears something at a board meeting which he doesn't like, he can't say, "Don't discuss that here" or "Don't tell me about it." He must be able honestly to say that in his judgment, the company is doing the best it can under all circumstances. If he cannot, he must let the other directors know what is wrong in his opinion. If they do not agree and cannot persuade him to the contrary, he must withdraw promptly; he cannot sit and wait until he spots trouble just ahead.

This column deals only with the affirmative duties of a public director to be a reasonably effective one. In addition, there are a host of other somewhat more specific prohibitions which are of an essentially negative character and which are far more precisely defined (not to disclose confidences; not to profit by corporate opportunities; not to engage in short swing or other improper insider trading, — in short, not to deal unfairly with the company), which need discussion.

The result of these two sets of increased obligations is that informed businessmen and professionals

are more and more reluctant to accept appointment to public boards without compensation commensurate to the degree of responsibility assumed, or a major stake in the enterprise, or (more usually) both.

I predict this trend will continue until all directors finally recognize their responsibilities and boards become true and effective management units, rather than the dummy operations which characterize so many newly public companies.

"COMPUTERS ENTER THE BUSING CONTROVERSY" — ADDENDUM

*Robert L. Glass
26414 124th Ave., SE
Kent, Wash. 98031*

For the sake of journalistic completeness, I am sending this note on Seattle's program of busing for integration as discussed in my article "Computers Enter the Busing Controversy" which was published in your July issue.

My statement "Politics and public outcry may yet negate the integration plan which technology has been able to produce" was, unfortunately, prophetic.

A last-minute local court decision blocked busing and nearly scuttled Seattle's entire middle school concept. Schools opened, but busing itself was postponed (nominally) a year.

Citizens Against Mandatory Busing (CAMB), instigator of the suit which led to the decision, was jubilant. The School Board, with too little time left for an effective countermove, could only acknowledge temporary defeat.

Busing advocates in Seattle, and the computing technologists who constructed the busing implementation plan, can only fall back on the traditional loser's cry, "Wait 'til next year."

DEALING WITH TODAY'S PROBLEMS

*John Skowronski
Director of Publications
Kansas City Chapter, DPMA
P.O. Box 2425
Kansas City, Mo. 64142*

I would like your permission to reprint the article "The Handwriting on the Wall" (June, 1971, p. 6) which editorializes a piece entitled "Computerized" by "Margo". I am also writing to the Boston Globe for their permission to reprint the "Margo" article.

Data Processing Management Association (D.P.M.A.) as you probably know is a non-profit organization of data processing professionals with approximately 260 members in the Kansas City Chapter. Our local newsletter has a monthly distribution of approximately 300.

I would also like to congratulate you for a very fine magazine that deals with today's problems. Your articles "The Case of Secret Service Agent Abraham W. Bolden" (June, 1971, p. 41) and "The Issue is Hypocrisy" (June, 1971, p. 45) were quite revealing. My wife was so impressed that she is going to subscribe personally for your magazine.

"DO WHAT I MEAN": The Programmer's Assistant

Warren Teitelman
Bolt Beranek and Newman
50 Moulton St.
Cambridge, Mass. 02140

"The programmer's environment influences, and to a large extent determines, what sort of problem he can tackle, and how far he can go in a given time."

This article deals with the design and actual implementation in a computer programming system of "a programmer's assistant". The general function of the "programmer's assistant" is to make it possible for the human programmer to say to the computer "do what I mean" instead of "do what I say", and "undo what I just tried — it did not work", instead of leaving the programmer with the sad consequences of his actual instructions.

In other words, the programmer's assistant deals with such factors as:

- ease of interaction;
- level of interaction;
- forgiveness for errors (both spelling errors and errors of thought);
- going back and taking a different path;
- changing one's mind; etc.

and in general, the programmer's environment.

This area of improvement in interactive programming is important. For many applications, the programmer's environment influences, and to a large extent determines, what sort of problem he can tackle, and how far he can go in a given time. If the "environment" is "cooperative" and "helpful", then the programmer can be more ambitious and productive. If not, he may spend much of his time and energy performing routine clerical tasks and "fighting the system".

An Analogy

The conceptual role of the programmer's assistant can perhaps best be explained by using an analogy with a well-equipped chemistry laboratory. We are attempting to recreate for the programmer the type of laboratory assistant who works closely with the chemical scientists. As an example of his duties, the assistant can watch the scientist perform a sequence of operations, and then be instructed to repeat the operation, perhaps with some rearrangements, omissions, or other modifications, or to clean up the mess and make things ready for another run.

This kind of general purpose assistance complements the facilities in the laboratory, but does not of course substitute for them. Its value is greatest in those situations which are (1) not standardized, so that special equipment has not already been built for that purpose, or (2) not sufficiently repetitive, so that new equipment cannot be designed and built cost-effectively. These situations usually require the scientist to achieve

his goal by executing many small steps, with perhaps some similarities or repetitions, while deciding at each point what to do next on the basis of the previous results, with occasional, or even frequent, "backing and filling."

In the realm of programming, it is easier to build and discard tools for just a few applications than in the physical sciences. However, all too frequently the programmer may not realize he is going to need an operation repeated, or else the operation is not exactly the same in each case, or else the effort of building the tool (and debugging it) may not be worth interrupting his train of thought and action. If it were convenient for him to specify repeating a previous operation, including possible modifications, without his having previously prepared for it, he would certainly do so. Then like our hypothetical scientist, he would be able to turn his attention to evaluating the results of his "experiment" so far, and deciding what to do next, while his assistant performs the dog work.

Undo

One of the important functions of the laboratory assistant is cleaning up an abortive experiment and getting things ready for the next run. In the realm of programming, users prepare for possible disasters such as a program running wild and chewing up a data structure, by saving the state of part or all of their environment before attempting some not yet reliable process. Undoing then consists of backing up to some previous state and starting over from there. However, this saving and dumping operation is usually expensive and time-consuming.

Of course disaster may also strike as a result of supposedly innocuous operation. As a result, the user all too often finds himself in a situation where he wishes, either idly or desperately, that he could reverse the effect of a previous operation or operations. Here we have an advantage over the physical sciences: a laboratory assistant may not be able to reverse the effect of mixing two chemicals together, no matter how hard or skillfully he tries. However, in the programmer's assistant, we can provide such a capability.

BBN-LISP

At Bolt, Beranek, and Newman, Cambridge, Mass., and at over a dozen other installations around the United States, the language called BBN-LISP is in

common use. BBN-LISP as a programming language, is an implementation of LISP, a language designed for list processing and symbolic manipulation. BBN-LISP as a programming system, is the product of, and vehicle for, a research effort supported by the Advanced Research Projects Agency for improving the programmer's environment.

Design Philosophy

BBN-LISP contains many user-support facilities. These include:

- a sophisticated structure editor which can either be used interactively or as a sub-routine;
- a debugging package for inserting conditional programmed interrupts around or inside of specified procedures;
- a "prettyprint" facility for producing structured symbolic output;
- a program analysis package which produces a tree-structured representation of the flow of control between procedures;
- a concordance listing indicating for each procedure the procedures that call it, the procedures that it calls, and the variables it references, sets, and binds; etc.

Most on-line programming systems contain similar features. But the essential difference between BBN-LISP and other systems is embodied in the philosophy that the user addresses the system through an (active) intermediary agent, whose task it is to collect and save information about what the user and his programs are doing, and to utilize this information to assist the user and his programs. This intermediary has been named the programmer's assistant (or p.a.).

The Programmer's Assistant

For most interactions with the BBN LISP system, the programmer's assistant is an invisible interface between the user and LISP: the user types a request, for example, specifying a function to be applied to a set of arguments; the indicated operation is then performed, and a resulting value is printed. The system is then ready for the next request. However, in addition, in BBN-LISP, each input typed by the user, and the value of the corresponding operation, are automatically stored by the p.a. on a global data structure called the history list.

The history list contains information associated with each of the individual "events" that have occurred in the system, where an event corresponds to an individual type-in operation. Associated with each event is the input that initiated it, the value it yielded, plus other optional information such as side effects, messages printed by the system or user programs, information about any errors that may have occurred during the execution of the event, etc. As new events occur, existing events are aged, and the oldest event or events are "forgotten." The length of the history list is set by the user, and is typically somewhere between 30 and 100 events.

The user can refer to an event on the history list by its relative event number, for example, -1 refers to the most recent event, -2 the event before that, etc. He may refer by an absolute event number, or by a pattern which is then used for searching the history list. For example, the user can retrieve an event in order to REDO a test case after making some program changes. Or, having

typed a request that contains a slight error, the user may elect to FIX it, rather than retyping the request in its entirety. The p.a. recognizes such requests as REDO and FIX as being directed to it, not the LISP interpreter, and executes them directly. For example, when given a REDO command, the p.a. retrieves the indicated event, obtains the input from that event, and treats it exactly as though the user had typed it in directly. Similarly, the FIX command directs the p.a. to allow the user to edit the indicated input. When the user has fixed up this input, it is again processed by the p.a. exactly as though it had been typed in.

Fifteen Commands

The p.a. currently recognizes about 15 different commands (and includes a facility for the user to define additional ones). For example, the USE command provides a convenient way of specifying simultaneous substitutions for lexical units and/or character strings, e.g. USE X FOR Y AND + FOR *. This permits after-the-fact parameterization of previous events. The p.a. also enables the user to treat several events as a single unit, (e.g. REDO 47 THRU 51), and to name an event or group of events.

All of these capabilities allow, and in fact encourage, the user to construct complex console operations out of simpler ones in much the same fashion as programs are constructed, i.e. simpler operations are checked out first, and then combined and rearranged into large ones. The important point to note is that the user does not have to prepare in advance for possible future use or reuse of an event. He can operate straightforwardly as in other systems; yet the information saved by the p.a. enables him to implement his "after-thoughts."

Undoing

Perhaps the most important after-thought operation made possible by the p.a. is that of undoing the side-effects of a particular event or events. In most systems, if the user suspects that a disaster might result from a particular operation, e.g. an untested program running wild and chewing up a complex data structure, he would prepare for this contingency by saving the state of part or all of his environment before attempting the operation. If anything went wrong, he would then back up and start over.

Such "accidents" happen all too often in typical console sessions, and result in the user's either having to spend what may involve a great deal of effort in reconstructing the inadvertently destroyed information, or alternatively in returning to his last back-up, in which case the user would have to redo any useful work performed since that backup. Instead with the p.a., the user can recover by simply typing UNDO, and then perform the originally intended operation.

The existence of UNDO frees the user from worrying about such oversights. He can be relaxed and confident in his console operations, yet still work rapidly. He can even experiment with various program and data configurations, without necessarily thinking through all the implications in advance.

One might argue that this would promote sloppy working habits. However, the same argument can be and has been leveled against interactive systems in general. In fact, freeing the user from having to anticipate all of the consequences of an (experimental) change usually results in his being able to

pay more attention to the conceptual difficulties of the problem he is trying to solve.

Another advantage of undoing as it is implemented in the programmer's assistant is that it enables events to be undone selectively.

Finally, since the operation of undoing an event itself produces side effects, it too is undoable. The user can often take advantage of this fact, and employ strategies that use UNDO for desired operation reversals, not simply as a means of recovery in case of trouble. For example, suppose the user wishes to interrogate a complex data structure in each of two states while successively modifying his programs. He can interrogate the data structure, change it, interrogate it again, undo the changes, modify his programs, and then repeat the process using successive UNDOs to flip back and forth between the two states of the data structure.

Implementation

The UNDO capability of the programmer's assistant is implemented by making each function that is to be undoable save on the history list enough information to enable reversal of its side effects. For example, when a list node is about to be changed, it and its original contents are saved. For each primitive operation that involves side effects, there are two separate functions, one which always saves this information, i.e., is always undoable, and one which does not save it.

Although the overhead for saving undo information is small, the user may elect to make a particular operation not be undoable if the cumulative effect of saving the undo information seriously degrades the overall performance of a program, because the operation in question is repeated so often. The user, by his choice of function specifies which operations are undoable. In a sense, the user's choice of function acts as a declaration about frequency of use versus need for undoing. For those cases where the user does not want certain functions undoable once his program becomes operational, but does wish to protect himself against malfunctioning while debugging, the p.a. provides a facility called TESTMODE. When in TESTMODE, the undoable version of each function is executed, regardless of whether the user's program specifically called that version or not.

Side Effects

Finally, all operations involving side effects that are typed-in by the user are automatically made undoable by the p.a. by substituting the corresponding undoable function name in the expression before evaluation, as in the earlier example with the REMOVE PROPERTY operation. This procedure is feasible because operations that are typed-in rarely involve iterations or lengthy computations directly nor is efficiency usually important. However, as a precaution, if an event occurs during which more than a user-specified number of pieces of undo information are saved, the p.a. interrupts the operation to ask the user if he wants to continue having undo information saved.

Automatic Error Correction — The DWIM Facility

The previous discussion has described ways in which the programmer's assistant is explicitly invoked by the user. The programmer's assistant is also called when certain error conditions are encountered. A surprisingly large percentage of these

errors, especially those occurring in type-in, are of the type that can be corrected without any knowledge about the purpose of the program or operation in question, e.g. misspellings, certain kinds of syntax errors, etc.

The p.a. attempts to correct these errors, using as a guide both the program's environment at the time of the error, and information gathered by monitoring the user's requests. This form of implicit assistance provided by the programmer's assistant is named the DWIM (Do-What-I-Mean) capability. DWIM is also used to correct other types of conditions not considered errors, but nevertheless obviously not what the user meant. For example, if the editor is called on a function that is not defined, rather than typing NOT EDITABLE, the editor invokes the spelling corrector to try to find what function the user meant to edit, giving DWIM as possible candidates a list of user-defined functions. Similarly, the spelling corrector is called to correct misspelled edit commands, p.a. commands, names of files, etc. The spelling corrector can also be called by user programs.

As mentioned above, DWIM also uses information gathered by monitoring user requests. This is accomplished by having the p.a., for each user request, "notice" the functions and variables being used, and add them to appropriate spelling lists, which are then used for comparison with (possibly) misspelled units. Thus, DWIM "may know" that FACT was the name of a function, and is therefore able to correct FATC to FACT.

As a result of knowing the names of user functions and variables (as well as the names of the most frequently used system functions and variables), DWIM seldom fails to correct an error the user feels it should have. And since the spelling corrector knows about common typing errors, e.g. transpositions, doubled characters, shift and case mistakes, etc., DWIM almost never mistakenly corrects an error. However, if DWIM did make a mistake, the user could simply interrupt or abort the computation, UNDO the correction (all DWIM corrections are undoable), and repair the problem himself. Since an error had occurred, the user would have had to intervene anyway, so that DWIM's mistaken correction did not result in extra work for him. It is this benign quality that makes DWIM so appreciated by users.

Example

Suppose the user defines a function FACT of one argument, N. The value of FACT[N] is to be N factorial.

```
<DEFINE((FACT (LAMBDA (N) (COND
((ZEROP N9 1) ((T (ITIMS N (FACCT 8SUB1 N]
(FACT)
<
```

Note that the definition of FACT contains several mistakes: ITIMES and FACT have been misspelled.

The 9 in N9 was intended to be a right parenthesis, but the teletype shift key was not depressed; similarly, the 8 in 8SUB1 was intended to be a left parenthesis; and finally, there is an extra left parenthesis in front of the first T, according to LISP, on the second line.

```
<PRETTYPRINT((FACCT] [1]
=PRETTYPRINT [2]
=FACT [3]
```

```
(FACT
  [LAMBDA (N)
    (COND
      ((ZEROP N9 1)
        ((T (ITIMS N (FACCT 8SUB1 N)))
          NIL
          ←
```

Now, after defining FACT, the user wished to look at its definition using PRETTYPRINT, which he unfortunately misspells, [1]. Since there is no function PRETTYPRINT in the system, an "undefined function" error occurs, and DWIM is called. DWIM invokes its spelling corrector, which searches a list of functions frequently used (by this user) for the best possible match. Finding one that is extremely close, DWIM proceeds on the assumption that PRETTYPRINT meant PRETTYPRINT, notifies the user of this, [2] and calls PRETTYPRINT.

At this point, PRETTYPRINT would normally print (FACCT NOT PRINTABLE) and exit, since FACCT has no definition. Note that this is not a LISP error condition, so that DWIM would not be called as described above. However, it is obviously not what the user meant.

This sort of mistake is corrected by having PRETTYPRINT itself explicitly invoke the spelling corrector portion of DWIM whenever given a function with no satisfactory definition. Thus with the aid of DWIM, PRETTYPRINT is able to determine that the user wants to see the definition of the function FACT, [3] and proceeds accordingly.

```
←FACT(3) [4]
N9(IN FACT) >>--> N)
(IN FACT) (COND -- ((T --))) >>--> (COND -- (T --))
ITIMS(IN FACT)->ITIMS [5]
FACCT(IN FACT)->FACT
8SUB1(IN FACT) >>--> (SUB1
6
←PP FACT [6]

(FACT
  [LAMBDA (N)
    (COND
      ((ZEROP N)
        1)
      (T (ITIMS N (FACT (SUB1 N)))
        NIL
        ←
```

The user now calls his function FACT, [4]. During its execution, five errors occur, and DWIM is called five times, [5]. At each point, the error is corrected, a message printed describing the action taken, and the computation allowed to continue as if no error had occurred. Following the last correction, the value of FACT (3) is printed. Finally, the user prettyprints the new, now correct, definition of FACT, [6].

In this particular example, the user was shown operating in TRUSTING mode, which gives DWIM carte blanche for all corrections. The user can also operate in CAUTIOUS mode, in which case DWIM will inform him of intended corrections before they are made, and allow the user to approve or disapprove of them. For most corrections, if the user does not respond in a specified interval of time, DWIM automatically proceeds with the correction, so that the user need intervene only when he does not approve. Sample output is given below. Note that the user responded to the first, second, and fifth questions; DWIM responded for him on the third and fourth.

```
←FACT(3)
U.B.A. N9(IN FACT) FIX? YES [1]
N9(IN FACT) >>--> N)
U.D.F. T(IN FACT) FIX? YES [2]
(COND -- ((T --))) >>--> (COND -- (T --))
ITIMS(IN FACT)->ITIMS ? ...YES [3]
FACCT(IN FACT)->FACT ? ...YES [4]
U.B.A. 8SUB1(IN FACT) FIX? NO [5]
U.B.A.
(8SUB1 BROKEN)
```

A great deal of effort has been put into making DWIM 'smart'. Experience with perhaps a dozen different users indicates we have been very successful; DWIM seldom fails to correct an error the user feels it should have, and almost never mistakenly corrects an error. However, it is important to note that even when DWIM is wrong, almost always no harm is done; since an error had occurred, the user would have had to intervene anyway if DWIM took no action. Thus, if DWIM mistakenly corrects an error, the user simply interrupts or aborts the computation, UNDOes the DWIM change using UNDO, and makes the correction he would have had to make without DWIM. It is this benign quality of DWIM that makes it a valuable part of the programmer's assistant.

Conclusion

When a user types a request which contains a misspelling, having to retype it is a minor annoyance (depending, of course, on amount of typing required and the user's typing skill). However, if the user has mentally already performed that task, and is thinking ahead several steps to what he wants to do next, then having to go back and retype the operation represents a disruption of his thought processes, in addition to being a clerical annoyance. The disruption is even more severe when the user must also repair the damage caused by a faulty operation, instead of simply UNDOing.

We have found that in addition to making life a lot more pleasant for users, the p.a. has a synergistic effect on user productivity. This effect seems to be related to the overhead that is involved when people have to switch tasks or levels:

The DWIM facility greatly facilitates construction of complex programs because it allows the user to remain thinking about his program operation at a relatively high level without having to descend into manipulation of details.

Even more important, however, is that DWIM and the p.a. act to minimize user distractions and diversions at whatever level the user is operating or chooses to operate.

We believe that p.a. facilities should be built into low-level debugging packages, the executive language of time sharing systems, etc., as well as other 'high-level' programming languages, for these facilities provide the user with a significant 'mental mechanical advantage' in attacking problems. □

References

1. Teitelman, W., Bobrow, D.G., Hartley, A.K., and Murphy, D.L., "BBN-LISP TENEX Reference Manual", BBN Report, July 1971.
2. Teitelman, W., "Toward a Programming Laboratory", IJCAI, January 1969.
3. Bobrow, D.G., "The Future of List Processing Languages", to be published in a forthcoming issue of the "Communications of the ACM".

Cryptology, The Computer, and Data Privacy

M. B. Girdansky
Scientific Information Dept.
IBM Research Division
P.O. Box 218
Yorktown Heights, N.Y. 10598

"In the modern digital computer, cryptology has gained a valuable ally, but in ever-growing measure, the computer may find itself in need of cryptology."

English writer and wit G. K. Chesterton once observed that a nighttime view of neon-lit Broadway would be singularly beautiful—to someone unable to read.

Implicit in the quip was realization that any alphabetic (or syllabic) system of writing in fact constitutes a cipher to one ignorant of the system.* An unfamiliar script long concealed the language and content of the ancient writings known as Minoan Linear B. It was only in the early 1950s that cipher-breaking techniques identified the material as Greek of the Late Bronze Age (c. 1300-1000 B. C.), radically revising our notions of early Mediterranean history.

Such "hidden writing" (the etymological meaning of "cryptography") is the result of historical accident, but there are examples of intentional cryptography which are even older. Deliberately enciphered hieroglyphics were inscribed more than half a millennium before Linear B was set down. Closer to our own day—in the India of the Fourth Century B. C.—ambassadors to foreign courts were explicitly advised to practice "the decipherment of secret writings." Over the centuries since, cryptology—the discipline concerned with the making and breaking of codes and ciphers—has led a sometimes raffish, but usually important and frequently fascinating existence.

Like much else, cryptology has been profoundly affected by technology. Telegraph, telephone, radio, and a variety of subsequently developed means of processing information electronically have presented problems as well as opportunities. Thus, encoded or enciphered messages had to be made far more resistant to garbling

*A *cipher* transforms low-order constituents of a message—such as individual characters or, more rarely, small groups of characters—according to some definite strategy. In contrast, a *code* consists of an agreed-upon but essentially arbitrary listing of natural-language segments vs. code equivalents, allowing a small group of symbols to represent an entire word, sentence, or even group of sentences. A volume containing such entries as DABLI = "Consignment two weeks overdue/Customer threatens cancellation/Expedite or give particulars" is a true code book. The so-called Morse Code is a misnomer; actually the system is a form of simple substitution cipher.

(Based on a report published in 'IBM Research Reports', Vol. 7, No. 4, 1971, and reprinted with permission)

over noisy lines or during poor atmospheric conditions. New techniques for encrypting data (e. g., such novelities as high-speed transmission and signal-scrambling) were devised and in turn had to be countered. Increasingly, cryptology drew upon the insights and skills of mathematicians, electrical engineers, and others from the physical sciences.

Of perhaps greatest ultimate significance at the cryptology/technology interface was development of the modern digital computer. In it, cryptology has gained a valuable ally, but in ever-growing measure, the computer may well find itself in need of cryptology.

As the computer is used to store and process data on individuals, concern has been voiced lest much that is personal and legitimately private lie open to those with access to "data banks." In response, cryptologic techniques have been suggested as a logical means of shielding a computer's contents, which might otherwise be readily called out from the machine. Depending on the purposes to which the data bank is to be put, some or all of its contents should be inaccessible and unreadable to anyone but a given authorized user. Granted, just who is to be "an authorized user" is largely a question of public policy. Exploration of technical possibilities is, however, the province of the scientist and the engineer. In this area, workers at the IBM Research Division have been among those seeking effective privacy systems, as well as probing the weaknesses of systems already proposed.

If, as seems likely, data banks are to be embodied as centralized computers reached through a network of remote terminals, it would be desirable to have many features of the system—not only a cipher itself—work together to provide privacy and security from tampering. Such an approach has been evolved by IBM's Horst Feistel, and implemented in an experimental system developed by William A. Notz and J. Lynn Smith which features critical hardware designed by Smith.

Perhaps logically prior to system details, however, is the matter of what type of cipher to use. It has long been realized that certain classes of ciphers are, by their very nature, weaker than others. At IBM, Bryant Tuckerman has gone somewhat further, showing that one popular

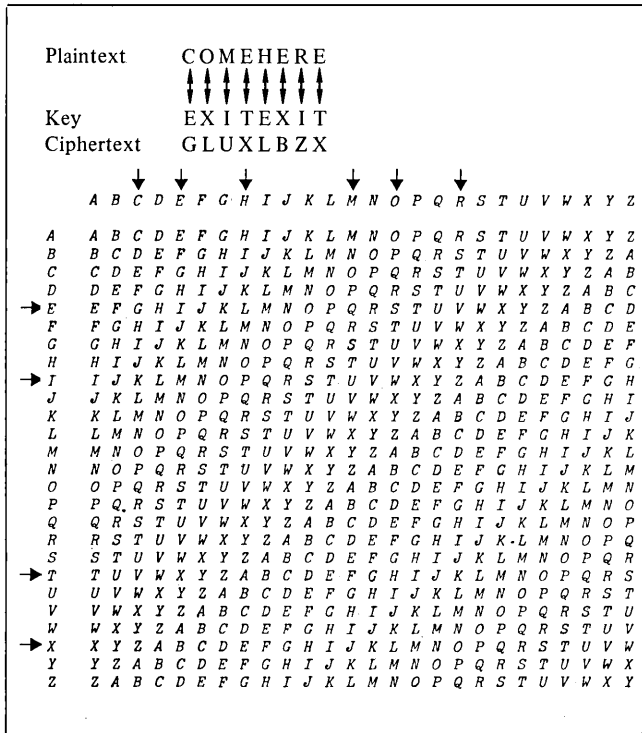


Figure 1. "Classic Vigenère" enciphered by establishing a one-to-one correspondence between plaintext and key characters. The key is repeated in whole or in part when necessary. Ciphertext characters are then those which stand at the intersections of key rows and plaintext columns.

class of ciphers is, indeed, far weaker than even a skilled amateur at cryptology might think.

VIGENÈRE-VERNAM CIPHERS

The cipher class studied by Tuckerman occupies a classic position in traditional cryptology. Although some members of the class are centuries old, one variety was devised a matter of decades ago to provide on-line encipherment of teletypewriter text. The class has been proposed by some as a means of furnishing privacy in modern data storage and transmission systems. Both theoretically and by practical demonstration, Tuckerman has shown that an unauthorized user ("opponent") having only limited material and information with which to work can readily extract the original text of messages enciphered by members of this class by making use of the speed, capacity, and computational abilities of the computer.

Representatives of this cipher-class have historically been kept distinct under the names, "Vigenère cipher" and "Vernam cipher," but in spite of superficial differences, their underlying mathematical structures are fundamentally alike. Tuckerman therefore employs the phrase "V-V systems" to encompass them both.

In its simplest form, the Vigenère cipher is familiar to even the amateur cryptologist as the "tableau" of alphabets shown in figure 1 and 2. The horizontal and vertical alphabets set slightly apart from the main block are for the convenience of the user in specifying the characters

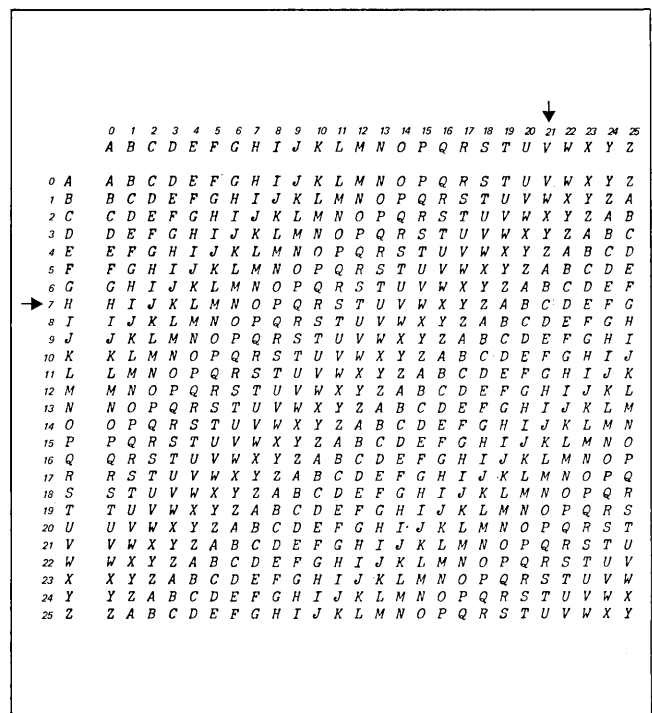


Figure 2. Vigenère encipherment considered as addition modulo 26. If the letters of the alphabet are given the values A = 0, . . . Z = 25, and combination of a row and a column is defined as "addition," then the character at the intersection of row and column is the sum, modulo 26. Here, 21 + 7 = 2, corresponding to V + H = C.

of the plaintext and of the key. For mnemonic ease, it was formerly customary for the key to consist of an intelligible word or meaningful phrase, although this feature constitutes a weakness; incoherent keys, which reduce the number of clues, are certainly preferable.

Encipherment of "classic Vigenère" begins by establishing a one-to-one correspondence between the characters of the plaintext and the characters of the key (see figure 1), the key being partially or completely repeated if shorter than the plaintext. The cipher character may then be defined as the character standing at the intersection of a plaintext column and the appropriate key-letter row. If, for example, "EXIT" is used as the key to encipher the plaintext message, "COME HERE," the tableau provides a ciphertext of GLUXLBZX: G at the intersection of "C" column and "E" row; L at the intersection of "O" and "X"; and so on. (Most encipherments omit spaces between words and sentences, since they can provide valuable hints to the cryptanalyst—the code-breaker. However, a good enciphering system should not need this precaution.)

There is an extremely simple mathematical model which can represent such encipherment. If the letters of the alphabet are assigned numerical values A=0, B=1, . . . Z=25; if combination of a column and a row is defined as "addition"; and if the character at the intersection is defined as the "sum"—then encipherment consists of addition modulo 26. According to such addition, 21 + 7 = 2. Inspection of an appropriately labeled tableau (figure 2) shows that the corresponding "letter equation" also holds true: V + H = C. Under this modu-

1) Ciphertext

BMXZJXKCVFMEGRIEWDOCKUCXNWZSSKBLNFTZFPNSKXGRFDTKVKVRSBTVSJONTDWPFIYIJ
 NDOGIDNKIXOVZHMNDSEVONUNDTGYEVFCJZPFPHPDGJNGDOOPFDNTEKESPLVYTKRR
 NFDJDFGRXEEETWMLFMCZVFPPOZYEMDYDEHYRSUJFDCUZZICZJYBUODDIPEFUZEEB
 LNTFKHJXKGTGHOH"-----"WTGYEOPBOPMDBKUYKRN"-----"IAWEMFSXDNSEXZNF
 XESGRHJXV"-----"HRVXCOVA"-----"HUPJTTCIYGD

2) Phrase probably in plaintext

IBMSYSTEMOPERATINGSYSTEM

3) $\mu (=21)$ - differencing of 2) [in numerical form]

8 12 18 24 18 19 4 12 14 15 4 17 0 19 8 13 6 18
 12 24 18 19 4 12 14 15 4 17 0 19 8 13 6 18

4) Difference-sequence

11 3 0

5) $\mu (=21)$ - differenced ciphertext [in numerical form]

19 16 14 25 0 16 8 8 6 6 1 15 25 8 23 11 17 15 22
 8 0 12 15 18 7 20 11 3 0 20 6 0 25 22 20 16 3
 22 22 3 9 6 16 24 0 21 15 15 14 3 8 23 19 16
 20 15 16 14 0 8 6 4 16 14 8 20 22 22 5 0 17
 25 23 5 16 19 14 22 24 17 7 10 8 13 12 18 15 11
 8 18 22 19 19 0 1 21 9 7 25 18 14 8 21 3 16 22
 16 17 4 7 11 8 0 9 6 15 17 16 1 14 10 11 20 15
 1 7 1 16 7 19 18 8 8 8 16 6 12 11 19 19 13 15
 25 20 10 11 11 12 6 13 8 7 6 4 7 15 10 19 12
 1 10 20 15 17 16 0 25 1 17 13 13 0 16 25 1 25
 17 14 11 3 0 1 9 12 15 9 7 3 25 25 3 2 0 0 1
 7 0 9 22 3 14 7 14 23 1 6 4 19 9 5 15 20 3 0
 25 16 25 12 11 4 4 14 11 11 22 8 15 11 2 3 11
 0 12 8 10 25 4 9 0 0 10 4 11 15 8 8 0 5 11 17

6) Two instances of recovered key

19 11 13 5 1 17 17 24 9 13 21 0 1 13 17 0 9
 1 10 17 15
 19 11 13 5 1 17 17 24 9 13 21 0 1 13 17 0 9
 1 10 17 15

Probable phrases

- 1) THIS PUBLICATION PROVIDES BASIC INFORMATION
- 2) THIS PUBLICATION DESCRIBES THE GENERAL
- 3) THIS PUBLICATION LISTS AND EXPLAINS THE
- 4) THIS PUBLICATION CONTAINS SPECIFICATIONS

(μ, ν) - differenced probable phrases

- 5) 24 16 10 20 10 8 15 9 11 24 20
- 6) 6 3 17 3 6 21
- 7) 2 25 23 10 12 5
- 8) 8 14 21 11 21 1 2 24 21

(μ, ν) - differenced ciphertext

9)

12 15 4 19 4 10 19 19 0 14 10 5 25 18 11 0 21 9 0
 25 20 12 11 24 5 6 0 1 2 5 20 21 5 10 21 1 3
 18 14 15 3 22 4 22 14 6 11 4 25 13 25 21 6 2
 9 1 11 20 21 17 19 24 16 10 8 23 2 25 23 10 12
 5 8 12 9 20 7 17 23 13 2 25 14 8 7 3 11 17 21
 25 1 25 16 24 20 25 2 25 10 0 8 16 15 21 25 20
 16 25 12 12 13 24 23 17 14 11 22 23 20 13 9 10
 13 19 3 18 14 9 6 5 2 10 6 22 7 4 7 6 23 21
 9 11 12 0 21 19 9 25 13 5 9 20 17 18 10
 16 14 23 13 2 0 9 10 7 4 25
 23 2 4 1

Program finds 7 in 9

Figure 3. Decipherment of a one-loop cipher of key-length $\mu = 21$, via μ -differencing. Such differencing of a suspected plaintext phrase and ciphertext shows probable beginning points of suspected phrase at boxed sites in 5; two instances of recovered key are shown at 6.

Figure 4. Some stages in decipherment of 2-loop cipher. Differencing here proceeds in two steps, of length μ and ν , for the suspected or known lengths of the two keys. An instance of one of the probable phrases—3—is thus found (shown in boxed region) within the differenced ciphertext, so yielding a portion of secondary key which can be suitably processed to give one of the primary keys and thence the other.

In addition, the alphabet constitutes a special case of a commutative (Abelian) group.

Vernam encipherment is the kind which was originally applied to teletypewriter text. It consists, in the abstract, of addition modulo 2—logically, the exclusive OR—of the individual bits of binary-coded key together with binary-coded plaintext characters. This operation also converts a given alphabet—say the $2^5 = 32$ characters of the Baudot teletypewriter code (actually a form of cipher) or the $2^8 = 256$ characters of the computer character-set EBCDIC—into an Abelian group. Although the group operation of addition no longer has as its modulus the number of characters in the alphabet—the modulus is 2—almost all of the mathematics is the same as in the Vigenère case. (In Vernam's original encipherment, the alphabet was in fact the Baudot code and the key was fed from a quasi-randomly punched loop of tape.)

Repeated use of the key in linear combinations is the Achilles' heel of such systems, and key-predictability is another weakness. If a key were (1) random, (2) at least as long as the number of plaintext characters to be enciphered, and (3) destroyed after use for a single message, the resulting ciphertext would be unbreakable, even in theory.

Why, then, are such truly unbreakable ciphers seldom used? They are, in fact, sometimes made use of, by espionage agents employing unique pairs of pads containing "one-time keys"—but only for relatively short text and in situations where the requirement for absolute secrecy is of the highest. The need for ever-different random keys, and the attending logistical problems, have apparently made "the perfect cipher" only a marginally useful approach. Incoherent Vigenère keys and Vernam's use of an unsystematically punched tape were implicit recognition of the dangers of predictable keys. For moderate amounts of text, such tactics can, in fact, supply one-time keys; but as message-traffic increases, re-cycling becomes a practical necessity. That is, the key becomes a loop and the cipher becomes vulnerable.

LOOPS AND FRAGMENTS OF TEXT

The weakness of relatively short Vigenère keys has long been known, and valid—though often tedious and time-consuming—methods have been evolved to read material so enciphered. In an attempt to mitigate the defect of key-length, while using practical short sequences, a technique in electromechanical encipherment was developed not long after Vernam's original system came

into use. Two tapes (primary keys) of only moderate length were "geared" in such a fashion that they produced a cyclical permutation of their contents, which were then added to provide a secondary key for addition to the plaintext. Thus, two tapes, one containing $\mu = 999$ values and the other $\nu = 1,000$, would produce a sequence of $\mu\nu = 999,000$ values before repeating periodically. Such a system may be termed a 2-loop system; similarly, 3-, 4-, . . . n-loop systems can also be created, for Vigenère or for Vernam applications. According to such nomenclature, the classic forms of the two ciphers would be one-loop systems, regardless of their specific physical embodiment.

It might intuitively be supposed that the use of a 2-loop system with relatively prime key-lengths μ and ν would provide security equivalent to that of a one-loop system with a key $\mu\nu$ characters long. Tuckerman's analyses and demonstrations have shown, however, that such is by no means the case. The security obtained is, in fact, that of a far shorter loop only ($\mu + \nu$) to about $5(\mu + \nu)$ characters long, depending upon the amount and types of data available to the "opponent." Most of the apparent additional security provided by 2-loop or higher-order systems is illusory.

Tuckerman's initial work consisted of systematizing and automating established techniques for the solution of the classic one-loop system. The resulting program permits solutions within minutes, rather than the hours which were often previously required. Following this, he developed techniques whereby 2-loop (and sometimes higher-order) systems may be broken. In both instances, the analyses were made under a range of different assumptions as to the amount and kinds of data at the "opponent's" disposal.

The most stringent assumption—and the most prudent in assessing a cipher system,—was that a certain amount of corresponding plaintext and ciphertext would fall into the hands of the adversary. Provided the texts were at least as long as the key, it is apparent that a one-loop encipherment will yield the key by simple subtraction of plaintext from ciphertext.

It is less evident, but has been shown true by Tuckerman, that the primary keys for any n-loop system can also be recovered by methods of differencing and summing, provided that corresponding plaintext and ciphertext are available which are at least as long as the *sum*, not the product, of the key-lengths.

Next, an intermediate assumption was made for the various loops systems: namely that the available data consisted only of ciphertexts and ascertained or guessed fragments of plaintext whose location within the ciphertext was *not* known. Even under this weaker assumption, the proper location of the fragment can be deduced and the primary keys recovered for any number of loops, provided the available sets of ciphertext and (possibly guessed) plaintext exceed the sum of the key-lengths. A knowledge of the key-lengths themselves reduces the amount of computation required, but is not essential. Examples of the differencing procedure followed by Tuckerman in such instances are shown (in

computer print-out form) for the one-loop case in figure 3 and for the 2-loop case in figure 4; the aspects of the one-loop computation will be described in some detail for illustrative purposes.

For a one-loop key of length of μ , Tuckerman terms the process μ -differencing. In figure 3 it is supposed that ciphertext (a portion of which is shown in literal form at 1) is available and that key-length is 21. It is also known—or strongly suspected on the basis of a logically plausible "probable phrase"—that the fragment shown at 2, IBMSYSTEMOPERATINGSYSTEM (of length 24) occurs in the plaintext. Differencing this plaintext (in digital form, 3) by a step of $\mu = 21$ yields the sequence (11 3 0) of length $24 - 21 = 3$, shown at 4. Carrying out this same μ -differencing on the digital version (not shown) of the ciphertext yields the sequence at 5. Whenever the known or suspected fragment 2 occurs in the plaintext, the (11 3 0) sequence must occur in 5. Tuckerman's program seeks out such occurrences, two of which can be seen embedded in the portion of 5 shown. At either or both places, the assumed plaintext fragment may be subtracted from the *undifferenced* ciphertext to yield a tentative key, which is probably correct. Trial decipherment can then be used to confirm the analysis. In this example, subtraction was carried out at both locations, and the two keys—listed at 6—are found to agree.

A somewhat analogous procedure for n-loop systems was developed by Tuckerman and is in part shown for the 2-loop case in figure 4. Here, differencing of plaintext and ciphertext proceeds in two steps, one of length μ the other of length ν , where these two values are the known or guessed key-lengths. This (μ, ν) -differencing of the (conjectured) plaintext fragments 1 through 4, and of the ciphertext (here omitted), produces the sequences 5 through 8, and 9. The program finds an instance of 7 at sites 66-71 within 9. Subtraction of 3 from the *undifferenced* ciphertext, beginning at the 66th position of the latter, yields a portion of secondary key which can be singly differenced, permuted, cumulated and "depermuted," to yield one of the primary keys and thence the other.

PLAINTEXT UNKNOWN

As a final step, Tuckerman has demonstrated the feasibility of largely automated decipherment under the weakest assumption: merely that sufficient ciphertext be available.

In the one-loop case, such decipherment consists of systematic and automated application of largely already-known cipher-breaking techniques. Parts of an example are shown in figure 5, where statistical tests are carried out on ciphertext at 1, which determine that the key-length is 10. The ciphertext frequency distribution for each key column (whose array is displayed at 2) is calculated and displayed at 3. Correlation of these distributions allows a calculation of the differences between the key characters, on which basis decipherment can proceed along lines similar to those developed by earlier workers in cryptology. As little as 20μ char-

acters of ciphertext (μ = key-length) are sufficient for such decipherment. It is striking that the text can be recovered without the underlying frequency distribution of the message being known. At worst, at the next-to-last step, the decipherer is left with a so-called "Caesar cipher" (here, at 4 in figure 5) in which a single unknown constant (in this case, 3) has been added to each character. Such a cipher can readily be broken (deciphered French text is shown at 5)—either by statistical analysis if the underlying language and its statistics are known; or else by the inspection process sometimes called "running down the alphabet," which produces as many potential decipherments as there are characters in the alphabet. One of these *must* be the correct decipherment, hopefully (and probably) recognizable.

Even more impressive has been the demonstration that a 2-loop cipher for which *no* plaintext is known succumbs readily, provided one has sufficient ciphertext—approximately 100 ($\mu + \nu$) characters, for key-lengths μ and ν . Here, the first step is to difference the ciphertext by a displacement of various multiples of one of the (possibly guessed) key-lengths. The result is a set of one-loop ciphers whose known ciphertext characters, and unknown key and plaintext characters, are differences of the original ones. It is perhaps surprising—but nonetheless true—that the quasi-random differences of unknown plaintext characters "inherit" a sufficient non-uniform distribution from the "parent" plaintext to allow application of various estimation techniques to establish the keys and permit decipherment.

An illustrative sample of ciphertext (1), recovered keys (2 and 3), and deciphered plaintext (5) is shown in figure 6. As in the one-loop case above, the decipherer may be confronted with a Caesar cipher at the next-to-last stage. The entry 16 listed at 4 in figure 6 represents the constant which had to be subtracted from the text at this stage in order to produce the plaintext.

Although the Vigenère and Vernam ciphers have been of lively interest to certain cryptologists over the years, Tuckerman has shown that they are highly vulnerable to attack by a computer-aided and resourceful analyst. He has also shown that much smaller amounts of material—and of less favorable kinds—are needed for decipherment than naive intuition might suppose.

Thus, it is apparent that far stronger methods are needed for adequate data security. Here, it is appropriate to consider the work of IBM Research's Feistel, Notz, and Smith.

A SYSTEMS APPROACH TO DATA SECURITY

A fundamental aspect of the data security system developed by Feistel, and implemented by Notz and Smith, is—as we shall see—a cipher-class far stronger than that whose weakness was demonstrated by Tuckerman. But more is involved than simply the greater strength of some other variety of cipher. The cryptologic component of a security system can prove unsatisfactory in ways other than its powers of concealment. Certain ciphering procedures, for example, present a variety of

logistical problems in a realistic environment—in some instances because of difficulty in efficiently realizing them within an electronic network. An example of the latter is a problem of synchronization which arises when additive, pseudorandom streams of bits are used.*

Moreover, procedural—as well as strictly cryptologic—features should contribute to the security of data entered or contained within a system. The prospective user of a system should have some means of assuring himself that he is, in fact, dealing with "his own" (time-shared) computer. The computer, in turn, should have some means of guarding itself against a clever "intruder" into the system. As much system activity as possible—ideally, all—should be automated, to provide additional security as well as speed.

The Feistel/Notz/Smith system promises to avoid such weaknesses and has a number of positive virtues, including amenability to complete automation.

Time-independent techniques are employed which obviate the need for bit-stream synchronism, information being enciphered in discrete blocks under the control of a cipher key. This "block cipher" can also be termed a "product cipher" because of its successive application of two or more distinctly different kinds of transformations to the original data (plaintext).

Smith has adapted Feistel's principles for use in a hardware cryptographic device named "Lucifer," the design of which includes interfacing to an IBM 2770 Data Communications System. An experimental interactive computer/terminal system was developed by Notz and Smith and concretely illustrates the use of cryptology in suggested solutions to certain data-security problems.

THE BLOCK CIPHER SYSTEM

Although the general principles of a product (and block) cipher were described and discussed in rough outline as long ago as the mid-Nineteenth Century, such ciphers had to await the rise of modern electronic and computer technology for real-time use in more complex forms and for heavy data-traffic. A simple yet surprisingly effective product transformation on plaintext is the successive application of substitution and transposition. In substitution, a character is replaced by another character; in transposition, the resulting characters are subjected to re-ordering. (It may be noted in passing that even a paper-and-pencil form of this type of cipher, used as a field cipher by the Germans in World War I, presented a formidable challenge to a noted cryptanalyst of the time.)

Elaboration of this class of ciphers and its adaptation to the computer, in which many successive transformations and rounds of transformations can be performed quickly and automatically, have resulted in a highly complex yet flexible encipherment procedure which can process large blocks of data as a unit. This latter characteristic is desirable not only logistically, but cryptologically—the

*Note Vernam's early version of this tactic, cited on page 14.

1) Ciphertext

```
JXYRWBCCQJFVZZFOLVJMHVCLUUFXPJSATRNOKIMMXVEVTOXVLNUTVYFJCYWHVFPXJKYBN
PHCEJTGFLMUKORRBTPLBHVCRYFVJRJXLDVFOTZCWQXBHJMYFKVHWPFSYRTECBGXNE
NULICBAXNEJUVJQNUXYPKICWHLAXMVKSMHWPOTVYVQHLNVAJCCQJNBZAXNVD
CUHLAYZTIVADOXPFHFHGLWRNDRSTVZEWJFRQBZQLLWVFSHLNQCNCNUVYCYLUR
ACTHIRNQLXLRZBKFPSCHLWRXFCPODHLORXBUNVCHLAYZTFLKXLDFTJZRSG
```

2) Ciphertext array by determined key length

```
JXYRWBCCQJ
FVZZFOLVJM
HVCLUUFXPJ
SATRNOKIMM
XVEVTOXVLN
UTWVYFJCYW
HVFPXJKYBN
PHCEJTGFLM
UXORRBTPLB
HVCRYFVJRJ
XLDVFOTZCW
QXBHJMYFKV
HWPFYSRTEC
GXNENULICB
VXNEJUVJQN
UXYPTOKICW
WHLAXMVKSM
HWPOTVYVQU
HLNVAJCCQJ
WBAZAXNVDU
HLAYZTIVAD
OXPFHFHGLW
RNDRSVZEW
HJFRQBZQLL
LIWVFSHLCW
QNCNHUVCYL
URACTHIRNQ
LXLRZBKFPSC
HLWRXFCPOD
HLORXBUNVC
HLAYZTFLKX
LGDFTJZRSG
```

3) Ciphertext frequency distributions by key column

A	0	1	3	2	1	0	0	0	1	0
B	0	1	1	0	0	5	0	0	1	3
C	0	0	4	0	0	0	2	3	5	2
D	0	0	3	0	0	0	0	1	0	2
E	0	0	1	3	0	0	0	0	1	0
F	2	0	1	3	2	5	2	5	0	0
G	1	1	0	2	0	0	2	0	2	1
H	11	1	0	1	1	1	2	0	0	0
I	0	1	0	0	0	0	2	3	0	0
J	1	1	0	0	4	2	1	2	1	4
K	0	0	0	1	0	5	1	2	0	0
L	3	6	2	1	0	0	2	3	3	2
M	0	1	0	0	0	2	0	0	1	4
N	0	1	3	1	3	1	0	0	2	4
O	1	0	2	0	0	6	0	0	1	0
P	0	0	0	4	1	0	0	0	1	0
Q	2	0	0	0	1	0	0	0	5	1
R	1	1	0	0	0	0	1	2	1	0
S	1	0	0	0	2	1	0	0	3	0
T	0	1	1	1	4	4	2	1	0	0
U	4	0	0	0	1	4	2	0	0	2
V	1	5	0	5	0	1	6	6	0	1
W	2	3	3	0	1	0	0	0	0	5
X	2	8	0	0	5	0	1	1	0	1
Y	0	0	2	2	3	0	1	0	2	0
Z	0	0	2	1	3	0	1	4	0	0

Figure 5. One-loop cipher broken, plaintext unknown and unguessed. Statistical tests show key-length to be 10, and correlation of ciphertext frequency distribution allows calculation of differences between key characters. Automated and rapid versions of already known cryptanalysis techniques can then be used for decipherment. Beginning of French plaintext reads: "General Sacco Manual of Cryptology Introduction Generalities . . ."

4) Caesar-cipher version of plaintext

```
JHQHUDOVDFFRPDQXHOCHFUBSWRJDUSKHLHLQWURQXFNLRQJHQHUDOLWHYODQHFFVVLWHGH
FRUHHVSRQGUHGIDFRQVHFUHHVWDXVVLQDQFLHQHTXHKRPPHGHVWDFHVGFU
LWXUHVHVFUHHVHURQFRQWUHQWGDQVOHGXGHGRXWHVYONVFLYLOLVDLRLQVPH
HOHVSOXVUHFXOHVVFHTXLQRXVHQVHLJQHTXHODGLVFLSOLQHTXLHQVUDLWODFUB
SWRJDUSKLDHDXDRXWHVHVSRTXHVGHVGDGSHVWSOXVRXPRLQVJHQLDXA
```

5) Results of back-stepping 4 by 3 characters (text in French)

```
GENERALLSACCOMANUELEDCRYPTOGRAPHIEINTRODUCTIONGENERALITESLANECESSITEDE
CORRESPONDREDEFACONSECRETEESTAUSSIANCIENTNEQUELHOMMEDESTRACESDECR
ITURESSECRETESSERENCONTRENTDANSLETUDEDETOUTESLESCIVILISATIONSMEM
ELESPLUSRECULEESCEQUINOUSENSEIGNEQUELADTSCIPLINEQUIENTRAITELACRY
PTOGRAPHIEAUAUTOUTESLESEPOQUESEDESADPETESPLUSOINOINGENIAUX
```

larger the data block operated on, the larger the number of substitutional and re-ordering patterns possible.

In Feistel's system, the substitutions are performed under the control of a cipher key, while the transpositions are usually carried out according to a fixed pattern—although Feistel has suggested a variant for transposition under key control as well. Of outstanding importance is the fact that these substitutions are actually nonlinear transformations, thus lessening the amount of cryptologic "leverage" available to a potential cryptanalyst.

In addition to substitutions and transpositions, another step is modulo-2 addition of digits from the cipher key. All of these transformations are "factors" in the execution of a product cipher, and the product itself is executed a number of times ("rounds") before read-out of the ciphertext. The end result is a block of ciphertext the same size as the original plaintext, but resembling a block of random digits.

To give a general notion of the approach, a small subset of the whole system, dealing with only sixteen bits, is described here and shown in figure 7. The steps and sequence of events are representative of the complete system, however.

In the illustration, A is a register containing a cipher key consisting of an arbitrary sequence of bits.* As will be

seen, the key sequence is used to control a variety of different functions occurring within a single encipherment round. After each round, the contents of the key registers would be shifted by one position.

B is a set of 2-bit shift registers, whose top and bottom rows are loaded with data to be enciphered, and whose bottom row can be read without altering the contents. Depending on the value of a key bit, the four bits each contained in C₁ and C₂ move either straight down or are switched over as a block, as shown schematically just below C. At D, the bits then undergo nonlinear transformations which can change any 4-digit input into any 4-digit output, the transformations differing from one box to the next.

At E, the transformed bits undergo a transposition carried out simply by wire-crossings. (Because figure 7 depicts only a thin vertical slice of the full system, there may not be any correspondence between the input points and the output points that are actually shown in this figure.)

*It should be emphasized here that all information—cipher key, ciphertext, and plaintext—is internally processed in the form of bits (binary digits) having possible values of only 1 and 0. Letters of the alphabet, decenary numbers, a variety of symbols and other information: all are represented in the EBCDIC character-set mentioned on page 14 which uses a string of eight bits for each character.

The transformation by key addition is indicated by the circled plus-signs representing modulo-2 adders. The key digits are added to the corresponding outputs from E; the resulting sums are then added to the contents of the top row of the shift registers at B, where these latter sums are stored. In the final step of a single encipherment round, the contents of the top and bottom rows at B are interchanged. (In the variant procedure suggested by Feistel, this interchange on a register-by-register basis is made contingent on the values of bits from the key.)

Following this interchange, the same steps described here are repeated, but with the key shifted. After a number of such rounds have been completed, the finished ciphertext is read out. Deciphering is carried out in essentially the same way, with reverse shifting of the key register.

LUCIFER

Smith's design of the Lucifer device incorporates the main cryptologic notions developed by Feistel. The device enciphers (or decipheres) messages of any length, in groups of 16 bytes—128 bits—under the control of a cipher key consisting of 128 arbitrarily chosen bits. This key can be furnished from a magnetic-stripe card (wallet-sized and unique to each authorized user) or optionally from a plug-in 16-byte read-only store module.

The organization of Lucifer is serial-parallel, 8 bits wide. Each 16-byte group of a message to be enciphered and transmitted is first stored in Lucifer, where it is divided into halves. According to the value of each of 8 selected bits from the key, one of two different nonlinear transformations is performed on each of the 8 bytes in the top half of the message group. The results of these transformed bytes added to 8 selected bytes of the key are permuted and convolved with the 8 bytes in the bottom half of the message by modulo-2 addition. After an interchange of top and bottom halves, the same operations are again performed, but with different selected key bits. After 16 such rounds, alternated with 15 interchanges, the encipherment is complete for this block of the message, which is then read out and transmitted.

Each group of ciphertext received is deciphered in the same way, with the same key used for enciphering. The only difference is that the schedule of using the key bits is altered in a simple manner (that obviates reverse shifting) so that all the byte transformations and modulo-2 additions are repeated in the opposite order, thus undoing every step that was carried out in encipherment.

Lucifer is interfaced to the IBM 2770 terminal in such a way that: (1) it can be switched out of the circuit; (2) it can be switched in for reception only, so that all messages from the terminal are sent in plaintext, but received ciphertext is deciphered; or (3) it can be switched in for transmission and reception both. In either of the latter cases, Lucifer can distinguish between messages received in plaintext and those in ciphertext, so

1) Ciphertext

```
JVPWTEJYRMYURSATGPXMENVXYOVAEBQWKNKSAIZEXJXPAPBFJWCWJQQSIWGLIPRTR
JUUHJAMBSHHKTOTUYAMXSGOPLEJGGGATEPZHVAEAXNPRVCFPHYICWNQGPQSFCCGO
UQSODDVNFIXINLONNWRNEWDTHBIMLNXYOQYEZEQUQMMSJTZIDNRLKJFPWEAGDNFH
GUXMEGTFBWTIPHESKMBHCNXLJGZHXSBVJRAYLZYUGJZVLFQPHDTAWRQKPFWQOWSW
UFQCJERNBXZTNXICAPXCUIHLDPUYLYVTPEEPOOZGFQNOJFUACVQXTUWQZDIDPCZ
AAIDAZYCXKWTIDCVNCQXKXGMBINGUOTCHBRKKSZXEEXZRPCKFDEVHLIYUVBIXQGO
UQZBGEPOEBGXUEMFFXPCTUIEHCMQOEPFOKDCYPARBEAOJNYTEUFMZIKRTRWHVGYR
TZVZVUMDGGCITDNLHETVEAQBCOZOAZSVULNGYRPHRRPOOBYLCYREEBXKPHWMSFD
      "CVRSLTDDGOIVKBLZ"
      "ORBFWPRIF"
      "MUMJ"
      "RQVYXZPBR"
```

Recovered keys

- 2) 0 16 8 10 2 24 14 14 21 6
- 3) 0 8 13 14 0 4 13 22 14 23 4 2 11
- 4) Constant subtracted to produce 5
16
- 5) Plaintext

```
THEBMSYSTEMISASOLIDSTATEPROGRAMCOMPATIBLEDATAPROCESSINGSYSTEMPRO
VIDINGTHE SPEEDPRECISIONANDDATAMANIPULATINGVERSATILITYDEMANDED BYTHE
ECHALLENGEOFCOMMERCE SCIENCE ANDINDUSTRYSYSTEMS WITHADVANCEDLOGICALDE
SIGNIMPLEMENTEDBYMICROMINIATURETECHNOLOGYPROVIDESANEWDIMENSIONOFF
PERFORMANCEFLEXIBILITYANDRELIABILITYTHISDIMENSIONMAKESPOSSIBLEANEW
MOREEFFICIENTSYSTEMSAPPROACHTOALLAREASOFINFORMATIONPROCESSINGWITH
ECONOMYOFIMPLEMENTATIONANDEASEOFUSESYSTEMISASINGLECOORDINATEDSETO
      "PROCESSINGEQUIPMENTINTENDEDTOREPR"
      "CREATIVEDESIGNFORPRESEN"
      "PERMITEFFICIENT"
      "ARRANG"
      "ONTHELOGIC"
```

Figure 6. Decipherment of 2-loop cipher, plaintext unknown and unguessed. Extended calculations (not shown) difference ciphertext by various multiples of a guessed or ascertained length of one of the keys. The result is a family of one-loop ciphers whose ciphertext characters and key and plaintext characters are differences of the original ones. Surprisingly, there is enough "inheritance" of non-uniformity from the original plaintext to allow use of various estimation techniques in establishing keys and permit decipherment.

that it decipheres only the latter. Implementation of the step ciphering described above is also incorporated into the device.

THE EXPERIMENTAL SECURED-DATA SYSTEM

The experimental secured-data system developed by Notz and Smith employs an IBM System/360 Model computer, and includes the IBM 2770 terminal to which Lucifer is attached, as well as several special programs. These programs provide conversational capability for the system. In addition, there is a ciphering program which furnishes the computer with a software analogue of Lucifer. Another program controls the operation of the experimental system itself (included here is also the message authentication procedure already described).

As shown in the figure, there is a file of passwords and a correlated file of cipher keys within the computer. Access to the system is limited to those persons who can furnish a legitimate password at sign-on, and who can furnish Lucifer with a cipher key that corresponds to the password given; the cipher key selected at the computer and the one in Lucifer must be identical.

For demonstration purposes, the computer contains a model personnel file which can be queried and updated as would be a genuine one. Each record contains one field presumed to contain confidential information. By means of a special command issued by a legitimate user of the system, the user can store in this field information enciphered under a key which is strictly private—not

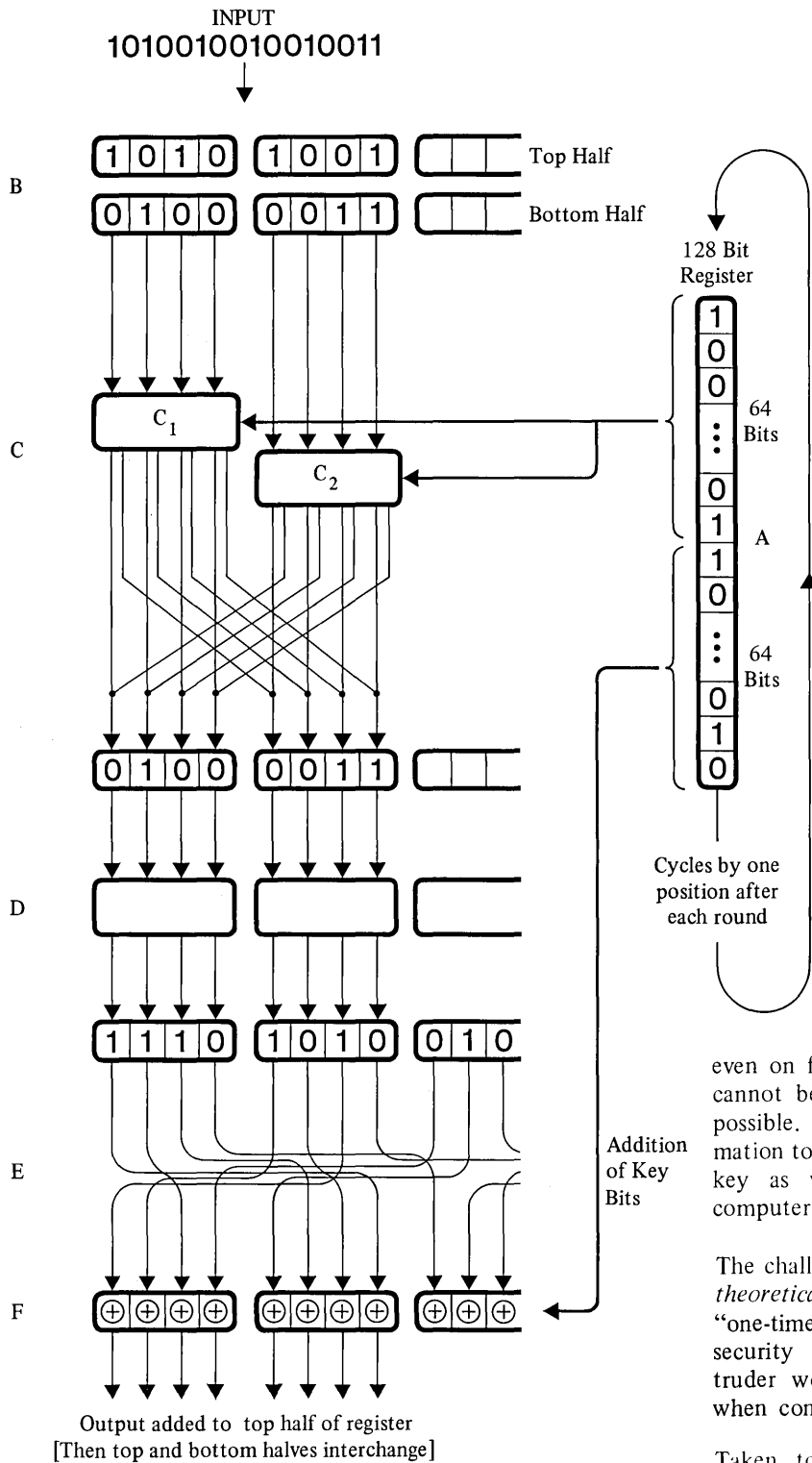


Figure 7. Version of Feistel encipherment procedure, subsequently modified and implemented by Notz and Smith (pp. 10-11). Only 16 of the 128 bits in a single message-block are shown. After input to top and bottom halves of 2-bit registers (B), blocks of 4 bits from the bottom half are "copied" and may undergo limited transposition at C, under control of bit values from key (at A). At D, such blocks are then subjected to differing nonlinear transformations. Individual bits are transposed at E, and are then (F) added modulo 2—see circled plus-signs—to still other key bits. These sums are added to top row of registers and contents of top and bottom halves of registers interchanged. Key then cycles by one position for next round of encipherment.

even on file within the computer. Of course, such data cannot be processed in this form, but retrieval is still possible. This tactic prevents disclosure of the information to anyone not possessing both the strictly private key as well as the individual key known to the computer.

The challenge presented by such a security system is not *theoretically* insoluble, as is the case with properly used "one-time" cipher keys, but the problems in traffic-security and cryptanalysis faced by a potential intruder would appear to be formidable to overcome when considered in realistic terms of time and expense.

Taken together, the various features of the system devised by Feistel, Notz, and Smith seem to furnish both a high degree of security and potentially wide flexibility in application. □

ALLIED READING:

1. H. F. Gaines: *Cryptanalysis*. Dover (New York), 1956.
2. L. S. Hill: "Cryptology in an Algebraic Alphabet." *Amer. Math. Monthly* (36), June-July, 1929.
3. D. Kahn: *The Codebreakers*. Macmillan (New York), 1967.
4. L. Sacco: *Manuel de Cryptographie*. Payot (Paris), 1951.
5. C. Shannon: "Communication Theory of Secrecy Systems." *Bell Syst. Tech. J.* (28), 654-715, 1949.
6. A. Sinkov: *Elementary Cryptanalysis, a Mathematical Approach*. Random House (New York), 1968.

CALENDAR OF COMING EVENTS

- May 3-4, 1972: Univ. of Alabama Seventeenth Annual Data Processing Conference**, Parliament House, Motor Hotel, 420 South 20th St., Birmingham, Ala. / contact: C. E. Adams, Director of Conference Activities, Box 2987, University, Ala. 35486
- May 3-5, 1972: Eighth Annual Data Processing Conference**, National Rural Electric Cooperative Association, Holiday Inn — North, Houston, Tex. / contact: C. E. Aultz, NRECA, 2000 Florida Ave., N.W., Washington, D.C. 20009
- May 11-13, 1972: DECUS Spring Symposium**, Parker House, Boston, Mass. / contact: Digital Equipment Computer Users Society, 145 Main St., Maynard, Mass. 01754
- May 15-18, 1972: 5th Australian Computer Conference**, Brisbane, Queensland, Australia / contact: A. W. Goldsworthy, Chmn., Australian Computer Society, Inc., Computer Center, Australian National Univ., P. O. Box 4, Canberra, A.C.T. 2600
- May 15-18, 1972: Spring Joint Computer Conference**, Convention Ctr., Atlantic City, N.J. / contact: AFIPS Headquarters, 210 Summit Ave., Montvale, N.J. 07645
- May 16-17, 1972: IIT Research Institute Second International Symposium on Industrial Robots**, Chicago, Ill. / contact: K. G. Johnson, Symposium Chairman, IIT Research Institute, 10 West 35 St., Chicago, Ill. 60616
- May 21-24, 1972: 7th Annual Mass Retailers' Convention and Product Exposition**, Marriott Motor Hotel, Atlanta, Ga. / contact: MRI Headquarters, 570 Seventh Ave., New York, N. Y. 10018
- May 21-24, 1972: 1972 International Systems Meeting**, Fontainebleau Hotel, Miami Beach, Fla. / contact: R. B. McCaffrey, Assoc. for Systems Management, 24587 Bagley Rd., Cleveland, Ohio 44138
- May 23-25, 1972: Annual Society for Information Display International Symposium**, Jack Tar Hotel, San Francisco, Calif. / contact: Mr. J. L. Simonds, Eastman Kodak Co., Rochester, N.Y. 14650
- May 24-26, 1972: Second Annual Regulatory Information Systems Conference**, Chase-Park Plaza Hotel, St. Louis, Mo. / contact: William R. Clark, Missouri Public Service Commission, Jefferson City, Mo. 65101
- June 12-14, 1972: Conference on Computers in the Undergraduate Curricula**, Sheraton-Biltmore Hotel and Georgia Institute of Technology, Atlanta, Ga. / contact: Computer Sciences Project, Southern Regional Education Board, 130 Sixth St, N.W., Atlanta, Ga. 30313
- June 12-14, 1972: International Conference on Communications**, Sheraton Hotel, Philadelphia, Pa. / contact: Stanley Zebrowitz, Philco-Ford Corp., 4700 Wissahickon Ave., Philadelphia, Pa. 19144
- June 15-16, 1972: ACM SIG/CPR Tenth Annual Conference on Computer Personnel Research**, Ontario Institute for Studies in Education, Univ. of Toronto, Toronto, Canada / contact: SIGCPR, c/o ACM, 1133 Ave. of the Americas, New York, N.Y. 10036
- June 19-21, 1972: International Symposium on Fault-Tolerant Computing**, Boston, Mass. / contact: John Kirkley, IEEE Computer Society, 8949 Reseda Blvd., Suite 202, Northridge, Calif. 91324
- June 19-21, 1972: Ninth Annual Design Automation Workshop**, Statler Hilton Hotel, Dallas, Tex. / contact: R. B. Hitchcock, IBM Watson Research Center, P.O. Box 218, Yorktown Heights, N.Y. 10598
- June 22-25, 1972: Society of Women Engineers 1972 Convention**, Sheraton Commander Hotel, Cambridge, Mass. / contact: Mrs. Amy C. Spear, RCA, Aerospace Systems Div., Burlington, Mass. 01803
- June 26-27, 1972: First Annual Government Data Systems Conference**, New York City, N.Y. / contact: William A. Kulok, New York Univ., Div. of Business and Management, Suite 2G, 1 Fifth Ave., New York, N.Y. 10003
- June 27-30, 1972: DPMA 1972 International Data Processing Conference & Business Exposition**, New York Hilton at Rockefeller Center, New York, N.Y. / contact: Richard H. Torp, (conference director), or Thomas W. Waters (exposition manager), Data Processing Management Association, 505 Busse Hwy., Park Ridge, Ill. 60068
- July 3-6, 1972: First Conference on Management Science and Computer Applications in Developing Countries**, Cairo Hilton, Cairo, U.A.R. / contact: Dr. Mostafa El Agizy or Dr. William H. Evers, IBM Corporation, Armonk, N.Y. 10504
- Oct. 3-5, 1972: AFIPS and IPSJ USA-Japan Computer Conference**, Tokyo, Japan / contact: Robert B. Steel, Informatics Inc., 21050 Vanowen St., Canoga Park, Calif. 91303
- Oct. 8-11, 1972: International Conference on Systems, Man and Cybernetics**, Shoreham Hotel, Washington, D.C. / contact: K. S. Nurendra, Yale Univ., 10 Hill House, New Haven, Conn. 06520
- Oct. 16-20, 1972: IBI-ICC World Conference on Informatics in Government**, Venice, Italy / contact: Intergovernmental Bureau for Informatics (IBI-ICC), 23 Viale Cività del Lavoro, 00144 Rome, Italy
- Nov. 9-10, 1972: Canadian Symposium on Communications**, Queen Elizabeth Hotel, Montreal, Quebec, Canada / contact: IEEE Headquarters, Technical Conference Svcs., 345 E. 47th St., New York, N.Y. 10017
- Nov. 15-17, 1972: Danish IAG-IFIP International Conference on Data Service Centres**, Copenhagen, Denmark / contact: Danish IAG (DIAG), c/o Danish EDP-Council, 58 Bredgade, DK 1260 Copenhagen K, Denmark
- *December 5-7, 1972: Fall Joint Computer Conference, Anaheim** Convention Center, Anaheim, Calif. / contact AFIPS Headquarters, 210 Summit Ave., Montvale, N.J. 07645

*Please note the change of date and of location for this conference.

"THE COMPUTER DIRECTORY AND BUYERS GUIDE" ISSUE OF "COMPUTERS AND AUTOMATION"

NOTICE

The U.S. Postmaster, Boston, Mass., ruled in January 1972, that we may no longer include "The Computer Directory and Buyers' Guide" issue of "Computers and Automation", calling it an optional, thirteenth issue of "Computers and Automation" regularly published in June.

Accordingly, we have decided to try to turn this ruling to our advantage. We hope to publish "The Computer Directory and Buyers' Guide of Computers and Automation" as a separate publication, probably on a quarterly basis. We hope to issue the usual parts of the directory plus additional reference information in June, September, December, and March. The main advantage of this change to our subscribers "with Directory" is that we can keep the "Computer Directory and Buyers' Guide of Computers and Automation" more up to date with quarterly publication than with annual publication; therefore, it should be more useful.

The domestic annual subscription rate for the "Computer Directory and Buyers' Guide" will be \$14.50. However, regular subscribers to "Computers and Automation" may subscribe to the directory at \$9.00 a year (there is thus no change for them).

We have applied to the Post Office for approval to so publish the "Computer Directory and Buyers' Guide of Computers and Automation" with postal second class mailing privileges. Since they have not yet had time to act on our application, our plans remain, to some extent, tentative.

Nevertheless, the regular computer directory information for 1972 will be gathered and WILL BE PUBLISHED in 1972. "The Computer Directory and Buyers' Guide of Computers and Automation" has been published every year from 1955 to 1971, and 1972 will not be an exception.

COMPUTERIZING A MEMBERSHIP ASSOCIATION

William R. Pollert
Executive Assistant to Vice President
National Association of Manufacturers
1133 15th St. N.W.
Washington, D.C.

"Whether or not a modern association manager meets his challenges depends on how effectively he uses modern management techniques and resources, one of which is the computer."

The National Association of Manufacturers represents over 13,000 large, medium and small manufacturers to the public and, in particular, to the Federal Government. Except for the unique role which NAM plays, as the primary voice of American industry on national affairs, many of the management problems, as well as the operations of NAM, are very similar to those of any other large or medium-sized association. Committees composed of specialists and experts from our membership work closely with staff to develop far-reaching policies which accurately represent the majority views of American industry.

Ability to Communicate

As a service organization whose product is intangible, to a large extent, NAM, similar to most other associations, depends upon its ability to communicate effectively with its members, the public, and the Federal Government. Further, because of the intangible nature of many of the products produced by associations, management control and the measurement of staff and association effectiveness are difficult.

Yet, many association members are increasingly demanding evidence that they are "getting their money's worth" from their association. These and other problems facing NAM and most other associations are a significant challenge to the modern association manager. Whether or not an association executive will meet the challenge depends upon how effectively he uses modern management techniques and resources, one of which includes the computer.

Computerizing the Ability

This article will outline:

- The process by which one association, the NAM, developed one of the most advanced management and membership information systems in existence today.
- The problems which were incurred in developing that system.
- The benefits and capabilities of such an EDP system to an association.

Although this article will describe the process of developing the membership information system for NAM, the managerial considerations should be relevant to any association manager considering developing or expanding an EDP system.

The computer age has been marked by great expectations and bitter disappointments. Many organizations enthusiastically installed EDP systems in anticipation of instant improvement in communications and efficiency, only to become frustrated by slow improvement and frequent setbacks. Why has the computer been such a disappointment to its users?

Possibilities of Failure

Although there is no single answer to this question, a number of recent studies by McKinsey, the Harvard Business School, and the Diebold group as well as our own, have identified several factors which seem to have contributed to the limited success of the computer in many organizations. Among the most important factors are:

- Lack of effective information and system planning.
Over-effective computer salesmen who often sell and lease EDP equipment on the basis of inflated customer expectations rather than customer needs.
- Limited integration of the computer into the total management and operational activities of the organization. Since many computer systems originate in the accounting department, many organizations tend to give primary attention to accounting applications of EDP and only secondary attention to the management applications of the computer.
- Limited evaluation of system effectiveness.
- Executive and organizational egotism, which is bolstered by being able to say "our computer says."

Essential Tasks

Keeping these common causes of system failure in mind, NAM management determined its current and future communications, financial, and information needs, and then attempted to determine which of these might be more effectively met if NAM had an EDP system. Through this "soul searching," management came up with three essential tasks which an NAM EDP system had to perform. It had to:

1. Perform such basic accounting functions as invoicing, statement follow-up, accounts receivable, aging and analysis, cash application, accounting controls, general ledger input, and a routine reporting of financial status.
2. Improve two-way communications with members and government officials so that they are more fully aware of NAM's policy positions, and NAM staff can better understand their needs.
3. Allow NAM management to develop rapidly decision-making information through statistical analysis of membership and non-membership data.

Own System vs. Time Sharing

Having outlined its EDP operating needs, NAM management asked several computer manufacturers and top time-sharing companies to submit proposals and cost estimates for the development of an EDP system which met these system requirements. The proposals varied significantly, both in cost and in system complexity. But they generally fell into one of two categories. The first type of proposal called for NAM to purchase its own computer, hire programmers, systems analysts, and establish a complete EDP department. The second type required only the purchase of an EDP terminal which would connect NAM to an external time-sharing computer system.

Both types of proposals had their strengths and weaknesses. Proponents of a NAM-owned and controlled computer system claimed that in this way EDP requests could be controlled more closely and completed more quickly than through time-sharing. Further, it was pointed out that NAM programmers and systems analysts would be able to modify and expand the system on a continuous basis, thus meeting NAM's evolving information needs more effectively than outside programmers. These advantages of owning a computer and having an inhouse EDP staff were offset, however, by the fact that it was unlikely that NAM would have enough computer work to justify the cost of equipment purchase and/or rental as well as the staff payroll.

Proponents of a time-sharing system on the other hand, pointed out that NAM would have their experienced programmers and systems analysts at its disposal whenever it needed them. In addition, by utilizing a time-sharing system, NAM would not have to worry about equipment obsolescence and would have to pay only for the running time of the computer. The primary disadvantage of a time-sharing system seemed to be: the geographical distance between NAM and the computer; the lack of full-time programmers and systems staff working on NAM's EDP system; and the time lag between an EDP request and printout — approximately 24 hours. Since NAM's information needs were such that a 24-hour lag between request and printout was not only satisfactory, but a great improvement over its manual system, the last point seemed to be of minimal importance.

Weighing the pros and cons of an inhouse versus a time-sharing system, it was decided that the current and future information needs of NAM staff and membership could be best satisfied through a time-sharing system.

Choice of Time-Sharing Supplies

The next step was obvious. Management had to choose which time-sharing firm it would use. Some of the factors which were considered in making this decision were:

1. Previous success of the firm. Each time-sharing firm was asked to submit a list of previous clients, who were then contacted to determine whether or not these companies were satisfied with their respective time-sharing systems.
2. Programmer and systems analyst understanding of NAM's goals, objectives, procedures, and information needs. This was determined by comparing written proposals as well as through in-depth interviews with the person(s) who would be assigned to the NAM account.
3. Size, language, type, and make of the computer for which NAM's programs were to be written.
4. Development cost and per hour computer charges.
5. Geographical distance between the computer and NAM headquarters. The less the distance, the easier it would be to sit down and discuss problems with systems analysts and programmers.
6. General retrieval capabilities of the proposed system. Obviously, we wanted to get the most flexibility, capacity, and sophistication for the least possible money.

Weighing these and other factors, management selected a firm which best met its needs, a leading software consulting firm, best known for the application of computer technology to human resources.

Detailed Definition

The next step was to define in detail the specific information which was to be included in the system and to develop the programs for storing and manipulating information to meet NAM's needs. The project manager analyst responsible for developing NAM's EDP system, spent several weeks meeting with the managers of each NAM department, going over department procedures, information needs, and projected system uses. From these in-depth interviews, a list of all the data which might be included in the system was compiled. This data was then evaluated to determine which bits of information were to be put onto the system first so that the system could be on-line soon, providing management with essential information as soon as possible.

In making this determination, the following factors were carefully weighed:

1. Was the information vital to the everyday operations of NAM? Since, as noted earlier, one of the initial objectives of the system was to computerize our billing, receivables, and accounting control system, financial data used for accounting had to be included on the system. In addition, essential membership profile information such as total employees, congressional district of the corporate headquarters, and the names, expertise and interests of committee members. Management also had to be included on the system.
2. Was the information readily available and at what cost?
3. How often did the information included on the system have to be updated to maintain its usefulness?
4. How would a particular type of data improve management and NAM's legislative effectiveness? When would the data be needed?

Priorities

On the basis of this analysis, information priorities were established, and the initial financial and non-financial data to be included on the system was determined. Each department had an obvious concern in what data was to be included on the system; so NAM management used confrontation meetings and a joint decision-making approach wherever possible in determining the initial data-base of the system. By using a joint decision-making approach, management involvement was maximized; the chance of omitting essential information was minimized; and the potential of inter-departmental conflicts over the EDP system was minimized.

Once the data to be put on the system had been specified, the contractor was able to finalize the programs to store, manipulate, format and print out information upon request.

Components

The five components of NAM's EDP system were:

1. A membership master file. This provided for a centralized data base of information containing all the meaningful elements of data which NAM needed to know about its members on both a corporate and individual level.
2. A membership information record. This program printed out a "hard copy" record of the information contained on the system for each member in the membership master file.
3. A general retrieval program. This program enabled NAM executives to request information directly from the computer in English.
4. A letterwriting program. This program enabled rapid personalized communication, to either the total NAM membership or certain groups within NAM.
5. A termination program. This program provided for the indefinite storage of information about terminated members as well as the capability to retrieve and analyze stored information with the same ease as active member records.

Provision for Expansion

Since it would have been impossible to initially specify every piece of information to be included in the system, several expansion fields for future information inputs were built into the system.

Concurrent with the development of the system programs, NAM began collecting and converting the data which was to be stored on the computer. The success of any EDP system depends to a large extent on the quality of the information put into the system. The task of data inputting was centralized to insure control and data accuracy. With over 100,000 items of information to be input, individuals working on this project had to be meticulous in detail, familiar with NAM, and willing to learn about EDP.


Staff Education

In order to assure a smooth transition from the old manual system to the new EDP system, both systems were run in parallel. In this way, program and data debugging could take place under normal operating conditions. Further, by running the old and new system together, staff responsible for the computer could acquire first-hand experience without the fear of making costly mistakes.

Benefits

If used properly, a computerized membership information system can aid the association manager in ex-

MICRO CARTRIDGES AND SUPPLIES



Operate in the Microfilm Reader 3M—MicroReader—Dietzgen—Microscan—Ednalite—Northstar. Hold 100 ft. of 16 mm film, and equipped with leaders & trailers. Guaranteed as to durability and mechanical efficiency.
Write for literature—prices.

From **95¢** up

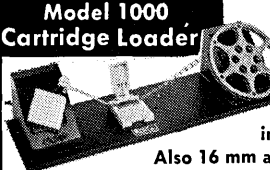
Model 2000 Micro Reader

FOR 16MM FILM
For Cartridges and Reels.
15 x 15" Screen.
Up to 42 x Magnification.
Optional: Image Rotation, Odometers, etc.

Model 3000 Micro Reader

FOR 35MM FILM
For Cartridges and Reels.
15 x 15" Screen. Up to 24 X Magnification.
Optional: Image Rotation, Odometers, etc.

Model 1000 Cartridge Loader



Splices—loads
16 mm film
into Cartridges.
Also 16 mm and 35 mm film
onto reels. High speed. Instant Braking.
Optional: Magnifying mirror for scanning film.
Dealers Invited.

MICROFILM PRODUCTS, INC.
Division of Equity Enterprises, Inc.
40 West 15th St., N. Y. 10011 Dept. **212-243-3443**

panding his membership services and acquire new members. Some of the broader benefits which an EDP system can provide an association are the following:

1. A membership information system can broaden staff understanding of its membership and help guide in the process of setting priorities, developing policies, and marketing memberships.
2. An EDP system can help disseminate the right information to the right person at the right time by name with a personal letter. Further, an EDP system can generate selected mailing lists which can be used as a means of distributing promotional literature, such as marketing publications, advertising meetings, and notifying of other association events. A membership information system can greatly improve the political action functions of an association by providing a means of rapid communication of major legislative developments to members.
3. An EDP system will enable staff to keep track of who comes to association meetings and what impact if any this may have on dues.
4. A computer system can aid staff in determining the effectiveness of their communications and in surveying key members either for their consensus on a vital public issue or in determining their evaluation of the association's performance.

The foregoing are a few of the specific benefits and tangible results that may accrue to an association with a computerized membership information system. Beyond these is the more subtle and intangible benefit, that of a totally new image which is consistent with the computer age. □

The Information Industry and Government Policy

Clay T. Whitehead, Director
Office of Telecommunications Policy
Executive Office of the President
U.S. Government
Washington, D.C.

"Our stress in information technology should be on developing institutions that serve to enhance our abilities and our potential ... and not on creating defenses to meet a conjured-up parade of horrors."

A major proposition in these years which those with leadership and decision-making responsibilities must consider is that information is:

- a major industry,
- an important national resource, and
- a great source of economic and political power.

A broad perspective and a broad definition of the information industry applies: it includes many diverse technologies such as computers, communications, film, etc., and many diverse applications such as education, finance, government, transportation, etc. It seems to me that only through mutual cooperation and exchange between Government and the private sector can we meet the challenges and solve the problems facing us in channeling new technologies.

Impact of the Information Business

The direct impact of the information business is already sizeable and growing at a very rapid rate. Of course, the various parts of the information business will grow and develop somewhat independently, even though there are common technologies and common principles involved. But the indirect impact of the information business is even more pervasive, and it is here that the concept of an information industry is the most important to understanding what is going on.

Almost without our realizing it, the American economy has become heavily organized around information and the utilization of information. The inputs to a productive enterprise are no longer the traditional capital and labor only, but rather capital, labor, and information. And, within the general field of information, communication plays a vital role.

Communication

Communication is to the information business what transportation is to the industries dealing in goods and materials. Without good transportation, production would be scattered, decentralized, and inefficient. Transportation creates large markets and permits efficient production. But it does more — it has determined where and how we live. One only need consider the influence of rivers and harbors on population distribution to see this influence.

Resources

More and more of our national resources are engaged in the information business. Communications will be a major shaping force in this business. More and more it will determine where and how we live, how our businesses are organized, how large they become, and whom they serve. The impact goes beyond our economy. In our society, too, information technology in the forms of telephone and television have done much to change our social, political, and broad informational characteristics.

Regulation of Communications

We have learned from our experience in other fields that regulation of communications has a tremendous impact on the underlying information that is communicated. In broadcasting, for instance, regulatory policies regarding the number of television channels, programming requirements, and advertising support, have heavily directed television toward programming for mass audiences and mass tastes. As a result, regulatory policy has increasingly considered questions of content and quality of programs broadcast over the facilities. Why? Because regulation of transmission has shaped the economic incentives and disincentives involved in providing for the programs themselves, and because once regulation is established it tends to expand its purview.

Computer-Communications

In the common carrier field of communications, highly detailed regulation, oriented around public telephone service, has shaped and inhibited the growth of specialized communications services. Consider, for example, computer-communications services. At the present time, computers are available in a wide variety of configurations and prices. Raw computing power and associated equipment and software for these services are provided in a competitive environment that is quite responsive to social and individual consumer needs.

However, when information services draw on communications as well as computers, they must operate within an economic and technological framework that is oriented towards the more conventional forms of communications; and this makes carriage of data more expensive and more inflexible. Where we draw the regulatory boundary between computer services and communications will have a big influence on the services offered, the vitality and degree of innovation in the business, and whether the incentives are to suit the technology, the Government, or the user.

(Based on an address to The Conference Board, New York, N.Y., Feb. 15, 1972)

Effects on Evolution

So it is clear that government policies and regulatory concepts in the area of communications can have a profound effect on the evolution of the information business. Fortunately, much of the information industry is still young. If we are to guide this industry in a way that serves human ends, we must be prepared to back away from immediate problems and issues and to view things from their largest perspectives. We must trace our decisions back to fundamentals.

A Tool for Good or for Bad

Some of the fundamental considerations derive from cultural values, including such issues as access, privacy, and humanization. I express the last idea in the positive form: humanization, not dehumanization. While I do not believe that information technology will achieve the utopian ideal, neither do I believe that machines necessarily destroy basic human values. Information technology is a tool that we have put into our own hands. We can use it to enhance our own abilities and potentials, rather than degrade them. Our stress should be on developing the kind of institutions for the technology that serve this positive function, and not on creating defenses to meet a conjured-up parade of horrors.

It is difficult to predict with any certainty the rate of growth or the detailed composition of the information business of the future. But the basic direction is clear: More information, more highly organized, more dependent on technology, and more rapidly moved around. Who will have access to this emerging system of information — access as a provider as well as access as a receiver? Will these forms of access be widely diffused or highly centralized? How will information access affect our social and political institutions? What will be its impact on the free enterprise system?

Variety and Diversity

In seeking answers to these questions, we will have to recall the basic principles of variety and diversity that our society and our economy are founded upon. When we structure the information business, we structure the framework for the expression of ideas, for the exchange of information, and for the use of information in business. We need to think of:

- access that encourages diversity and quality in the sources of information, as well as in the way information is utilized;
- access that benefits individual human beings and small business, as well as large organizations and institutions;
- access that minimizes social polarization;
- access structured so as to avoid the development of a new class division — the information-poor and the information-rich — before that situation can arise.

Search for Public Policies

It is obvious that there are many uncertainties evaluating what is the best way of providing for access. The answers are neither easy nor readily available. Government cannot force people to be informed; it cannot ignore the realities and the freedoms of the marketplace; nor can it command the evolution of technology. Government can, however, search for the public policies that will foster an industry and a market structure that will encourage the applications

and the technology to grow naturally in the most desirable directions.

Privacy

Another important issue is privacy — in its widest sense — including related issues such as the integrity and autonomy of the individual. As our society grows more complex, and we become more independent, we are learning that privacy — or the capability of controlling who knows what about you, and why, — is fundamental to all human relations. There is a basic interest in society which society must not overlook.

Disclosure

However, it is also true that the individual's interest in privacy is frequently offset by his own interest in disclosure, since disclosure is often an indispensable means to achieving another desired good. Millions of consumers, for example, disclose personal information about themselves in order to obtain commercial credit. There is also a broader social interest in disclosure. There may be times when society must obtain some private information in order to act knowledgeably for the solution of social problems. If we absolutely prohibited all data acquisition, more would be lost in terms of foregone social capability than would be gained in terms of greater individual privacy.

Zones of Privacy

I do not think there can be monolithic principles to guide decision on privacy. There are certain kinds of information, or perhaps "zones" of privacy, which should be protected from all intrusion. Beyond that, individual choice should prevail. There is no single best resolution of the competing interests of privacy and disclosure that applies for each individual or situation. But, Government can assist in shaping utilization of information technology so that once an individual or societal decision is made, there is an effective mechanism for carrying it out.

Institutions

The new technologies and the new problems that come about will not necessarily require new institutions. Indeed, I think the basic objectives of diversity, choice, access, and privacy are likely to be more fully achieved in our system of private rights and legal procedures for enforcing them than through any new or expanded Federal bureaucracy.

Efficiency

In addition to considerations of access, privacy and humanization, the information business must be structured to achieve a degree of economic efficiency consistent with other goals. The question is how to do this. Much of our trouble in the present communications industry stems from two assumptions made years ago when we enacted the Communications Act of 1934: First, that a good part of the communications industry is characterized by natural monopoly; and secondly, that extensive regulation is necessary to prevent resulting monopolistic abuses. In many ways, the wheel is coming full circle.

Instead of natural monopoly, we find that more and more communications enterprises can be competitive in nature. And, in such an environment, we find that regulation affords not just consumer protection, but also uncertainty, delay and expense. What is the proper balance? Is the substitution of regulation for the marketplace really best — really justified

— or is it only due to the force of habit? Can the marketplace really be made to work effectively in such a complex and rapidly changing area?

New Mechanisms

There are no ready answers for these kinds of questions. We cannot afford to abandon the marketplace; we cannot afford to give up the choice, the diversity, and the freedom that it offers, nor can Government pretend that laissez-faire is an acceptable public policy. Rather, we will have to create new mechanisms and units of exchange which enable market inventives to operate.

The Mechanism of Copyright

To illustrate this point, consider the mechanism of copyright. Presently we rely on copyright laws both to give authors the incentive to produce and to establish a unit of exchange in the market system. Once an author copyrights a book, he obtains the exclusive right to sell, publish or copy it. From the proceeds of the sale or licensing of this right, the author is compensated for his labor.

How a Computer Affects This Mechanism

But what will happen if library services come to be provided by a computer-based network which feeds information right into the home? The computer permits easy change in the form of information. The computer provides the selection of parts of several original works to produce a wholly new product. Copyright laws pertaining only to the form in which an idea is expressed do not cover the situation I've described, where only the underlying information of the idea is used, and not the expression of the idea. Without a broadening of the copyright concept, our author would starve in his garret and the flow of new ideas would dry up. Those of you who have had experience with copyright can add to this list of problems — for example, the difficulties of adhering to the procedural requirements of our 63-year old copyright law, like affixing copyright notice to information inserted in a data base. You can ponder over whether an evanescent display of information on a CRT is a "copy" or not.

Change of Concepts

My point is this: We could strain present copyright laws to accommodate new information technology. But there is a limit to how effective present copyright concepts can be in an environment that is so foreign to it. For the most successful operation of the market, I believe we must find a new kind of property right in information. It should serve the same underlying purposes that present copyright does, but be suited to the use, value, and form of information in the newer systems of communication. This is only one example of the kind of changes we must be prepared to make to effectively utilize the marketplace to achieve our purposes.

In this field there are some complex issues that seem important for public policy. Government will have to deal with these problems. Though it is trite to assert that Government and industry must learn to work together more closely, this is nevertheless true. For, information is now a major factor in the growth of our economy, and policies for the exchange of information always have been a major concern of Government.

The importance of this field is matched only by its excitement. □

PICTORIAL REASONING TESTS — Part 5

Neil Macdonald
Assistant Editor, *Computers and Automation*

"There undoubtedly is a place for non-verbal, non-mathematical testing which is not culture-limited, not occupation-limited, and not background-limited ... and which would enable finding and employing many useful people — including programmers — who do not have American, middle-class backgrounds."

The pictorial reasoning tests which we have been publishing since October, 1971, continue to draw considerable response from our readers.

One reason probably is that the tests require observation, perception, comparison, recognition of shapes and designs, and reasoning. These operations are difficult for a computer program (except for the reasoning), yet stimulating to a human being. A second reason probably is that the techniques needed are those which we as human beings have had to use (and improve) all our lives — and it is fun to do something you're good at! A third reason, probably, is that the readers of "Computers and Automation" are a group of alert and intelligent people — so far as we can tell — and they seem to like contributing to the explorations we are making through these pictorial reasoning tests.

Prior articles on this subject in "Computers and Automation" are in the issues of: October, 1971 (No. 1); December (No. 2); February, 1972 (No. 3); and March (No. 4 — Analysis and Answers). In case any reader has missed these articles, we can supply back copies at moderate cost.

New Styles of Test

In this issue we publish a sample of a new style of test, Style 3. The first two frames in any item exhibit two samples of a relation between two objects. The question to be answered for each of the remaining 8 frames is "Is the same relation shown?" In the next issue (May) we plan to present a test in Style 4: the first three frames display three samples of a property; the question for each of the next seven frames is "Is the same property shown?"

Answers

The answers and comments that you, our readers, send us are very useful and give us much data to work from and think about. Our warm thanks to all of you. It is not easy to respond to individual persons who ask to know "the answers". But we have decided to publish the answers to all of our tests, usually from 3 to 6 months after the first printing of the test. The "correct" answers to CEA Reasoning Test No. 1 (which was printed in October 1971 and again in December 1971) were printed in the March 1972 issue. In many cases, it is impossible to prove that a certain answer is correct; accordingly, what we publish are so-called correct answers, denoted using quotation marks, as "correct" answers. □

"The figures have been drawn freehand and not too carefully. It is a myth that all figures should be drawn professionally; one can do a great deal with an author's free hand, approximate drawings, and the reader's eyes to interpret them; and such drawings make the gap between the author and the reader less formidable."

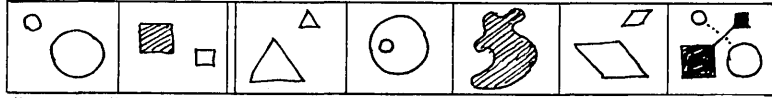
PICTORIAL REASONING TEST: C&A No. 6 - (may be copied on any piece of paper)

1. The following is a test to see how carefully you can observe and reason. It is not timed.

2. In each item the first two pictures A and B are samples that express a certain relation between objects or sets of objects. For each of the remaining eight pictures (C to J), consider the question "Does the picture express the same relation?". Then

write the code for your choice of answer in the cell provided. The codes are: V for "yes"; X for "no"; P for "logically, perhaps yes, perhaps no"; N for "not applicable"; and Z for "I am really puzzled and cannot reasonably choose".

3. For example: see the item below:



	A	B	C	D	E	F	G	H	I	J
1										
2										
3										
4										
5										
6										
7										
8										
9										
10										

Answer:

In each cell, insert the code for your choice of answer:

Item	C	D	E	F	G	H	I	J	Item	C	D	E	F	G	H	I	J
1									6								
2									7								
3									8								
4									9								
5									10								

Survey Data: 1. Name _____

2. Title _____

3. Organization _____

4. Address _____

5. In computer programming, are you: Average? Good? Excellent? Not your field? Other (please specify)

6. In systems analysis, are you: _____

7. In managing, are you: _____

8. What fields (not mentioned above) are you fairly good in (or even expert in)? _____

9. What other capacities do you have? (Please don't be bashful - but be objective) _____

10. Any remarks? _____

(attach paper if needed)

When completed, please send to: Neil Macdonald, Survey Editor, Computers and Automation, 815 Washington St., Newtonville, MA 02160

A reprint from
computers
and automation

● DO YOU LIKE
COMPUTERS AND AUTOMATION?

● DO YOU HAVE A FRIEND
WHO MIGHT LIKE IT?

● HOW ABOUT GIVING HIM
(OR YOURSELF) A GIFT
SUBSCRIPTION?

● Take advantage of our current offer:
a gift subscription to him (or you)
and for you —
a copy of our FOUR-STAR **** REPRINT

● ANY MORE FRIENDS OR ASSOCIATES
WHO MIGHT LIKE SAMPLE COPIES
OF C&A FREE? — just tell us
and we will send them a copy
— so they also may start
liking C&A

FOUR-STAR REPRINT

SCIENCE AND THE ADVANCED SOCIETY, by C. P. Snow,
Ministry of Technology, London, England (April, 1966)
THE INFORMATION REVOLUTION AND THE BILL OF RIGHTS,
by Dr. Jerome B. Wiesner, M. I. T. (May, 1971)
EMPLOYMENT, EDUCATION, AND THE INDUSTRIAL SYSTEM,
by Prof. John Kenneth Galbraith, Harvard Univ. (Aug. 1965)
COMPUTERS AND THE CONSUMER, by Ralph Nader,
Washington, D. C. (Oct. 1970)

cut here and tuck in flap

To: Computers and Automation

() Please enter a subscription for

Name _____

Address _____

City _____ State _____ Zip _____

() Send 13 issues including directory, \$18.50
in U.S.; add 50 cents for Canada, \$3.50 for
foreign postage

() Send 12 issues without directory, \$9.50 in
U.S.; add 50 cents for Canada, \$3.50 for
foreign postage

I enclose \$ _____ in full payment.

() Please send a FOUR STAR **** REPRINT to me:

Name _____

Address _____

City _____ State _____ Zip _____

Fold here — do not cut

**YES, start my subscription to COMPU-
TERS AND AUTOMATION according to the
instructions checked below.**

One Year (including the Computer Directory and Buyers'
Guide — 13 issues) U.S. only. \$18.50

One Year (excluding the Computer Directory and Buyers'
Guide — 12 issues) U.S. only. \$9.50

Name: _____ Title: _____

Organization: _____

Address: _____

City: _____ State: _____ Zip: _____

Country if not U.S.: _____

Signature: _____ P.O. No.: _____

Payment enclosed

Renewal

Bill me

New subscription

To SPEED the processing of your order, please check the one best
descriptor in each of the two categories below. (This information
will be used for statistical purposes only.)

BUSINESS TYPE

- 01—Computer Manufacturer
- 02—Aerospace / Aircraft
Manufacturer
- 03—Other Manufacturing
- 04—Raw Materials Processing;
(chemical, primary metal,
petroleum, food, etc.)
- 05—Mining and Construction
- 06—Computing & Consulting
- 07—Finance, Insurance, Publ.,
and Service Organizations
- 08—Transportation Companies
- 09—Public Utilities
- 10—Research
- 11—Wholesale, Retail, Sales,
and Marketing Firms
- 12—Educational; (College,
University, or School)
- 13—Government and Military
- 14—Libraries

JOB FUNCTION

- 1—Technical Management; (computer
installation management, program
management, or engineering mgmt.)
- 2—Computer Center Personnel;
(methods & procedure analysts,
and operators)
- 3—Programming Personnel; (systems,
application & research programmers)
- 4—Professional; (systems analysts,
mathematicians, operations
researchers, and professors)
- 5—General Management Executives;
(corporate officers, owners, and
partners)
- 6—Engineering Personnel; (systems
engineers, research & development engineers)
- 7—Research Personnel
- 8—Students
- 9—Library Subscription
- 10—Subscription in Company Name
Only

FIRST CLASS

PERMIT NO. 33531
BOSTON, MASS.

BUSINESS REPLY MAIL

No postage stamp necessary if mailed in the United States

POSTAGE WILL BE PAID BY BERKELEY ENTERPRISES, INC.

COMPUTERS AND AUTOMATION

815 Washington Street

Newtonville, MA 02160

cut here

B - fasten to A

cut here

bend here and fold

4/72

A - fasten to B

cut here

The Bad Image That Computers Are Earning

"Shall we as computer professionals correct our programs, so that they function properly, or wait until we are kicked in the teeth by an enraged public?"

1. From Harold W. G. Gearing
Queenswood House
Stone Drive
Colwall
Malvern, Worcester
England

Many of us here are concerned with the bad image that computers are getting throughout the world, from bad data, bad programming, and inadequate training of data-preparation staff. I would suggest that you might open a corner of your magazine to hold bad examples. In your June issue, you commented: "Shall we as computer professionals correct our programs, so that they function properly, or wait until we are kicked in the teeth by an enraged public?"

Here are a few to be going on with:

1. A well-known British manufacturer of motor-car accessories put its accounts-payable onto a computer. The young girls punching the input cards from the supplier invoices were not properly trained, and did not appreciate how to distinguish goods value from returnable outer-packaging deposits. One supplier found that over a period of several months, items in the Company's details of payment forms bore little relationship to his statements for accounts receivable. A day trip of several hundred miles was necessary, to persuade the responsible accountant to examine his internal system.
2. A security-transport company computerised its sales invoices. They show only contract number and no narrative. Central offices of large users have to examine contracts each time invoice batches arrive and manually allocate the invoices by writing on them the source and destination of each service. The invoicing system appears to be geared to holding a weekly service charge only; hence when the service is rendered only monthly, the contract monthly charge is divided by 4.33, rounded for entry in the master record; subsequent multiplication by 4.33 by the standard monthly invoicing program results in an invoice which differs by pennies from the contractual figure, which in many cases is also being prepaid by a banker's standing order.
3. A London west-end outfitting company decided to save money on its sales-ledger system by notifying all its account holders that they were being transferred to Barclay-card. Many English people dislike credit cards, and future business is probably being lost, particularly postal order business.

In this country the Inland Revenue is modifying its former ambitions to centralize all income tax records in a few computer centres. British obsti-

nacy, in continuing to prefer to deal with a local tax inspector, may be winning the day against the Big-Brother Computer!

2. From *The South Middlesex News*, Jan. 18, 1972
Framingham, Mass.

In this age of mushrooming automation, man has scored a rare victory over a computer — in this case a \$1.5 million machine described as a "good worker" which "just couldn't compete with people."

In Sacramento, Calif., in a move that cut teacher credential processing time by 900 per cent, George Gustafson fired the machine and switched to human beings.

"We got rid of a million and a half dollars worth of computer," said Gustafson, executive secretary of the State Teacher Preparation and Licensing Commission. "We pulled the plug and sent it back to IBM."

Gustafson Monday described his action as "converting credential processing from a complex and costly automated system to a streamlined, fully manual operation."

"It was easier to do it by hand," said Gustafson, who gave this assessment of the departed computer: "It was a good worker; it just couldn't compete with people."

This giant step backwards, Gustafson said, resulted in cutting the credential period from an average of 95 days down to the current average of 10.

Gustafson said that as a result of the change he was able to reduce the staff from 240 persons to 106. Since August, the department has cut 80 employees but all but three were given jobs with other state agencies.

A side benefit of the switch came during the summer, when the commission hired more than 50 poor and minority students to help make the change to manual processing.

("Man Beats the Machine", by United Press International)

3. From *New York Daily News*, Jan. 23, 1972
New York, N.Y.

More than 100 state senators and assemblymen joined Sen. John D. Caemmerer (R-Nassau) yesterday in sponsoring two bills to curb the power of the Parking Violations Bureau, which has harassed and dunned thousands of innocent motorists to pay for undeserved tickets.

Caemmerer, chairman of the Joint Legislative Committee on Transportation, said passage of the

bills would "prevent another PVB nightmare ... in New York City—or any other city."

The antics of the bureau and its computer, Super Sleuth, were detailed in a News series after thousands of readers pleaded for help by writing Action Line, a reader service feature that runs in the Long Island edition.

Motorists who never had driven in New York City were being plagued by Super Sleuth to pay parking tickets. Letters to the bureau, at 475 Park Ave., South, brought no reply—only higher fines and stepped-up threats.

The protests resulted in public hearings by Caemmerer Dec. 2 at the State Office Building, at which exasperated motorists told of widespread bureaucratic bungling and arrogant disinterest by the bureau.

Caemmerer's bills would require the violations bureau to provide transcripts of all hearings, require police witnesses if requested and allow defendants to be present at appeals.

Most important—at least to the innocent who are being victimized—the bills would require more careful vehicle identification and would require the bureau to answer its mail.

"We must deal with the PVB's preposterous attitude toward answering legitimate mailed-in questions," Caemmerer said.

The most maddening situation facing many motorists was that a parking ticket would be sent to them in Nassau County, although they had never driven in New York City. Not only that, it was marked "second notice."

In a typical example, a man with a blue Rambler, license plate XYZ-1234, would get a "second notice" to pay a ticket issued in the Bronx—where he had never been—on a yellow Ford with a different plate number.

He then would write a letter—registered—to explain the goof. A month later, he would get a more threatening letter demanding a higher fine. This would continue implacably, with higher fines and threats to withhold auto registration renewal.

So the motorist was forced to pay up—although innocent—or take a day off from work and drive 50 or 60 miles to straighten it out. In many cases, the motorist would drive in, be told: "Don't worry about it," and the next week receive another threatening letter.

Caemmerer's bill would require the cop or meter maid to put more information on the parking ticket. In addition to the make of the vehicle, the bill would call for its color, model, body type, plate number and registration tag number, with its expiration date, according to the Senator.

This should help the Motor Vehicle Department in Albany identify more carefully the owner of the car and make sure the ticket reaches the person who deserved it.

The legislation also would require that all certified mail to the bureau from motorists must be answered within 30 days or the case must be dismissed.

The bureau had never bothered to answer mail. Letters were stacked up by the thousands.

Bureau Director Anthony Atlas has often declared that the abuses of the bureau were being corrected, but letters to The News from harassed and distressed motorists did not diminish.

"My mail is worse than ever," Caemmerer said.

At The News, the rate of complaints also is higher than ever.

("Aim Monkeywrench at Super Sleuth", by Donald Weinbrenner)

4. From *The New York Times*, Feb. 20, 1972 New York, N.Y.

In the two weeks since 155,000 maximum base rent orders have gone out to tenants living in rent-controlled apartments, 17,379 landlords and tenants have visited or telephoned the city Office of Rent Control to protest or challenge the new rents fixed in the orders.

One was an owner who had carefully reported on the proper form when he increased the rent on an apartment that had become vacated, only to have it ignored when the city's computer figured the maximum rent he could collect from it.

Robert C. Rosenberg, the city official in charge of the office's computer, traced the error and partly calmed the landlord.

It turned out that the owner had listed the apartment as "4S" on one form and "4-S" on another.

Computer Confused

Mr. Rosenberg, assistant administrator of the Housing and Development Administration's maximum base rent system, said his computer had a one-track mind and did not realize that "4S" was "4-S" as well as—on some occasions in some landlords' minds—"S4."

"The computer isn't able to match the listings," Mr. Rosenberg said. "A special unit—of people, not computer sections—is resolving these matching problems. As soon as a problem is resolved, the computer is notified and a corrected order issued."

Mr. Rosenberg said landlords and tenants who discovered apparent errors should file protests at once. A tally Friday, however, showed that the 17,379 persons, who own or rent 21,250 apartments, did not wait for urging and have filed protests already. More will be coming in next week, for 102,000 orders are to go out tomorrow.

In all, more than 1.1 million orders are to go out.

One set of problems that is giving the computer pause arises from inconsistent financial data. When data are not consistent, the computer does not attempt to reconcile the conflict. It just omits the apartments to which they refer.

Until it gets a correction, the computer solves its problems by tapping out a message on the order: "Controlled apartments for which you have not been notified require further research. You will receive notification on these apartments shortly."

("17,379 Protest New Rent Orders; Inconsistent Form Entries and Computer Blamed", by Will Lissner)

Do You Want To Stop Crime?

William P. Wood, III
Dept. of Information Systems
Virginia Commonwealth Univ.
800 W. Franklin St.
Richmond, Va. 23220

"The last time the three fugitives were seen after blowing up the University laboratory, they were driving north towards Canada."

"The robbers jumped into a waiting car and fled into the night."

Automobiles Used in Crime

Such are typical daily news reports. What do all of these reports have in common? Almost every criminal MUST USE AN AUTOMOBILE SHORTLY BEFORE AND/OR AFTER HIS CRIME.

Automatic Car Identification

Such a fact might be used to great advantage in law enforcement. A system that would utilize this fact is as follows:

The principle used is borrowed from the railroad industry. The railroads use a system named ACI (Automatic Car Identification) to daily track and locate railroad cars. A problem the railroads have had until ACI is the losing of railroad cars. It is not unusual for a boxcar to be hooked up to the wrong train, sent across the country, and sidetracked on some remote spur. To remedy this problem, the railroads set up a system of photoelectric sensing devices along their tracks. These devices have the ability to read color coded plaques placed on the side of the cars. These sensing stations are connected, via telecommunications, to a central computer complex. This complex stores the location of the industry's two million cars.

License Plates Read by Sensing Stations

Using a similar system the nation's automobiles could be kept track of for the purpose of law enforcement. License plates would be required by law to conform to specifications which would allow them to be read by the sensing stations. These stations would be set up at strategic locations along our nation's highways. They would be tied via telecommunications equipment to centrally located computers manned by law enforcement personnel.

Suggested Systems to Track Criminals

This system could be constructed for either of two levels of capability. The more limited level would be that used for only tracking specific vehicles. For example, this would track known criminals. The more capable, and thus more expensive system, would sense and keep in memory for short periods, perhaps a few days, the location of all vehicles on U. S. roads with license plates. Information concerning cars of special interest could be kept in memory as long as necessary.

Such a system would provide the following advantages:

1. All cars within the area of a crime before and immediately after could be identified and their license numbers checked against suspect's license numbers.

2. Getaway cars could be traced throughout the country.
3. Suspects and witnesses would have their stories verified or discounted.
4. Such a system would be a great deterrent to crime.
5. Stolen cars could be traced almost immediately.
6. Drug traffic could be traced.
7. Such a system would cut into virtually every kind of crime: murder, robbery, rape, drug, arson, kidnappings, bombings, vandalism.

Cost of Tracking System and Cost of Crime

The cost of such a system might climb above one billion dollars, just for the setup cost. The cost of crime, though, is well in excess of twenty-one billion dollars per year. Even if the system did not pay for itself in the dollars and cents terms of cutting the cost of crime by as much as its own cost, how can one put a price tag on the misery and fear generated by this plague on society? Citizens, fearing for the safety of their families and homes, flee to the relative safety of the suburbs. Parents pray that their children will not fall prey to the evils of drugs and juvenile delinquency. Not only would this system be a boon to rid our society of those sinister doers of evil, but it would act as a tremendous before-the-act deterrent to those realizing the probability of apprehension.

Cost to Our Personal Privacy

There is one final cost that remains to be considered. This is the cost to our personal privacy generated by the ever encroaching inroads of computers and electronic gadgetry. Would such a system shorten the time between now and 1984?

IBM'S POWERFUL PARTNER: The Accounting Principles Board

(Editorial, reprinted with permission from "Samson Technology Trends", Dec. 1971, copyright 1971 by and published by Quantum Science Corporation, 851 Welch Road, Palo Alto, Calif. 94304)

More than the increased competition from IBM, the recent ruling from the Accounting Principles Board (APB), threatens to decimate the ranks of independent computer companies that supply plug-compatible peripherals to the end user. The high principled accounting rules are forcing all companies, large or small, to suddenly be super-honest and as a result, the APB has forced the majority of the small and medium sized independent computer companies to their knees, and sometimes into bankruptcy.

The ruling, instituted last year, requires that a conditional sale to a third party lessor be treated on a standard rental accounting basis rather than as a sale. This ruling has drastically reduced the reported earning of all peripheral suppliers who lease the majority of their equipment and has made the financing of rental inventory almost totally impossible for most. In fact, no company which does not have a sizeable two to four year-old base of rental equip-

ment in the field can report profit. Worst of all, the fastest growing companies are penalized most.

Before this ruling, most peripheral equipment suppliers relied on third party leasing to finance their sales. Moreover, the third party transactions provided the independents with an excellent profit record as long as their sales base continued to grow. Third party sales were recorded as revenue at the full sales price of the leased equipment rather than only the rental revenue accruing to the leasing company.

Admittedly, the old treatment unfairly favored the peripheral equipment supplier because it did not fully allow for the potential risks and write-offs resulting from the return of obsolete equipment. It was nevertheless approved of and certified by the accounting profession for several years. The ethics of such misguided support of a false business practice must seriously be questioned, as well as the sudden application of new principles of accounting that reversed prior certified profits into losses. The APB, in an attempt to place the profitability of the independents in proper perspective, has now created a situation that makes sales growth of computer products to the end user nearly impossible except for large companies that can finance their own leases.

Many small companies that based their business plans on old accounting rules have already or will soon cease existence as independent entities. The APB now has on its conscience not only dozens of bankruptcies, but also large losses of hundreds of thousands of stockholders who had accepted their views and relied on them to make investment decisions. What can we look forward to from the accounting profession in 1972 after the pooling-of-assets ruling in 1970 and third party lease accounting in 1971? Happy New Year!

CDC VS IBM — CORRECTION

*I. From Frederic O. Parlova
169 West 88 St.
New York, N.Y. 10024*

I read with interest the article on the IBM/CDC/Greyhound Litigation (C&A, Feb. '72).

In your introductory remarks you state, "...and there is apparently nothing in the court order(s) which enables the plaintiff, CDC, to obtain access to the information....." May I call your attention to page 49? "Examination and evaluation by expert IBM, Greyhound, and Control Data personnel is necessary if the data is to have any meaningful significance to counsel in preparing their defense." Also, "IBM shall make the said answers available only to its counsel and to not more than 15 of its non-clerical personnel....CDC and Greyhound shall comply with this paragraph but with a limitation of 10 non-clerical employees...."

II. From the Editor

We regret the error, and appreciate very much your correction.

CORRECTION

In the March 1972 issue of Computers and Automation, the following correction should be made: page 27, "Pictorial Reasoning Test: C&A No. 5" — in the first paragraph under Figure 2, replace the words "include OK or X as appropriate" by "include V, X, or Z as appropriate."

REDUCING AND DISMANTLING SCIENCE AND RESEARCH INSTITUTIONS, AND SOCIAL RESPONSIBILITY

*Andrew G. Michalitsanos
University of Cambridge
Cambridge, England*

The disillusionment with science in the United States is clearly evident in the continuing decline in the number of private and industrial research positions and the systematic reduction of research funds in both governmental and nongovernmental sectors.

The attitude of the Nixon Administration and the U. S. Congress has been aimed at drastically reducing the volume of scientific research in the United States, a nation whose growth and prosperity is almost totally dependent on the inventiveness of its scientists, who can provide new ideas and techniques for industry.

The Government's reason for this policy is based on public clamor against "non-relevant science."

It would be interesting indeed to find a person who could define "relevant scientific research." Many areas of scientific endeavor were at one time or another considered not directly applicable to public needs, but have become almost guiding centers of industrial applicability many years later. For example, solid state physics, at one time only of academic interest, today occupies an important place in electronic applications of all types. The telephone on the President's desk was constructed with the aid of "non-relevant scientific research."

The U. S. Government's attitude has a much deeper psychological effect on the American public in general. The cutting of research funds fosters the belief held by many young citizens today that science lies at the roots of the country's dilemma since it has brought the problems as well as the advantages.

The new generation appears to have replaced scientific logic with mysticism, clearly a step backward into the caves.

Pure science has not created the problems, but rather society's inability to apply scientific discoveries in a resourceful and meaningful manner. We should recognize that pure scientific research provides an intellectual store from which we may extract ideas and apply them to our needs. Reducing funds and decreasing the amount of pure scientific research simply makes the available store of information smaller.

I am not advocating indiscriminate spending for relatively obscure areas of science. However, I can see little use in dismantling the research institutions that have taken decades to establish.

The Nixon Administration should reassess its actions and consider what sad effects their decisions will have on the United States and the rest of the world for decades to come.

(Based on a letter published in the New York Times, Sept. 24, 1971)

A Concerted Campaign To Deny The American People Essential Knowledge About The Operation of Their Government

*Prof. Henry Steele Commager
Amherst College
Amherst, Mass. 01002*

The Nixon Administration is at it again. First it tried to intimidate the television networks. In vain. Next it attempted, for the first time in our history, to silence the press by the threat of prior censorship. Again in vain.

Now the Justice Department has launched an attack on the constitutional privileges of a co-ordinate branch of the Government — the Congress of the United States and, by implication, every legislature in the United States.

The issue is once again the Pentagon Papers. We might have supposed that with its defeat in The New York Times case the Government would drop this shabby prosecution. Not at all.

At the instigation of the internal security division of the Justice Department, a Federal grand jury in Boston has now subpoenaed Dr. Rodberg, legislative assistant to Senator Gravel, to appear before it. The Government's brief acknowledges that the thrust of the subpoena is to prepare the ground for an inquiry into "acts done by Senator Gravel in reading and inserting into the record the Pentagon Papers."

This may seem like a tempest in a teacup — especially as the Government has by its decision to publish the Pentagon Papers in toto abandoned its argument that their publication would do "irreparable injury" to the "security" of the United States — an argument palpably absurd at the time. But in fact three major principles of our constitutional system are at stake in this new Justice Department caper.

First is the hard-won principle of the immunity of any legislator from just this sort of harassment. Second is the principle of the separation and the equality of powers of the three departments of government. Third is the principle of freedom of speech and of the press.

The Constitution provides (Art. I, sec. 6) that "for any speech or debate in either House, they [Congressmen] shall not be questioned in any other place." Neither the purpose nor the meaning of this clause is obscure. The purpose was to make it forever impossible for any executive authority to punish or intimidate any legislator for what he might say in the legislative chambers.

These interpretations are now challenged by the Government brief which asserts that Congressional immunity from "question or debate" does not cover committee reports, and that it is wholly personal and cannot be enlarged to embrace legislative staff.

The first of these assertions was disposed of as recently as 1969 when Chief Justice Warren reiterated the principle that the speech clause covered committee reports, resolutions, "and such things as are generally done in a session of the House in relation to the business before it."

The second assertion raises the larger issue of the separation and equality of powers in our Government. But the principle laid down in Jefferson's Manual of Parliamentary Practice and formally adopted by both houses of Congress, has never been successfully challenged, namely that "Congressmen are at all times exempted from question elsewhere, for anything said in their own House; that during the time of privilege neither a member himself, nor his wife, nor his servants, may be arrested, cited, or subpoenaed in any court."

The logic of these constitutional and legal immunities is obvious. It is not to confer special privileges on legislators — or on judges or Presidents — but to protect them against harassment and intimidation which, as Justice Harlan put it, might "inhibit and dampen the ardor of all but the most resolute, or the most irresponsible, in the unflinching discharge of their duties."

The attack on Senator Gravel's immunity is pernicious — not only constitutionally and politically, but philosophically. It is part and parcel of what can only be described as a concerted campaign to deny the American people that knowledge about the operation of their Government so essential to the sound functioning of democracy.

It is a direct assault on the Constitution and the separation of powers; it is an indirect assault on the principles which the Constitution was designed to preserve and advance, above all the principle of freedom of speech and of the press. In this matter what the father of the Constitution, James Madison, said in 1794, is still relevant: "If we advert to the nature of Republican government, we shall find that the censorial power is in the people over the Government, not in the Government over the people."

(Based on a report "A Senator's Immunity" by Henry Steele Commager published in The New York Times, October 15, 1971)

FALL JOINT COMPUTER CONFERENCE: TOPICS

From the Editor

The Fall Joint Computer Conference in its call for papers has listed the topics which it seeks or hopes to cover in the program of papers:

- User Applications and Requirements
- Architecture Trends and Limitations
- Terminals
- Communications
- Complete Systems and Networks
- Hardware Advances
- Software Development
- Measurements, Analysis, and Evaluation
- Reliability
- Social Issues
- New Ideas — Try Us

Some of the most important topics in the computer field are left out of this list:

- Computers and Privacy
- Should IBM be Broken Up as a Monopoly?
- The Distrust of Computerized Systems by the Public
- The Use of Computers in Dictatorships
- Should Computer People Develop into Information Engineers?

Perhaps all these topics are included silently in the topic "Social Issues".

Internal Revenue Service: USE OF COMPUTERS

William H. Stewart, Jr.
Asst. Prof. of Political Science
Bureau of Public Administration
Univ. of Alabama
University, Alabama

(Excerpt from "Computers and Government", Citizens Information Report No. 7, published by Bureau of Public Administration, University of Alabama, 1972, 54 pp. "The material in this publication is not copyrighted in the hope that its use without restriction will be more widespread.")

Perhaps the most comprehensive use of computers in American government at any level is that made by the federal Internal Revenue Service. Automatic data processing in this agency has resulted in more accurate identification of potential and delinquent taxpayers, prevention of duplicate refunding of taxes, verification of tax computation, billing of outstanding taxes, tax audit, development of statistical information for proposed legislation, and tax administration controls. These improvements are not simply to the government's benefit. They help ensure that the tax burden will be borne equitably and that some do not escape paying legally owed taxes while others pay more than they are obliged to pay.

Approximately 76.8 million individual income tax returns were filed during the 1970 filing period. The role of computers in the processing of these returns is substantial. The central automatic data processing installation of the Internal Revenue Service is located at Martinsburg, West Virginia. The system is so massive that it requires 275 technicians to feed in the data received from district computer centers, which handle initial processing and verification of tax returns. Returns are transmitted to Martinsburg for more extensive analysis and consolidation into the master magnetic tape files. One-half inch of tape contains a complete three-year running tax account for each return filer.

The automatic data processing system utilized by the Internal Revenue Service has been programmed to look for the most common types of taxpayer "mistakes" and the classifications of taxpayers who are most likely to make these errors. The agency's experience is that the higher the individual or corporate income the greater is the chance of error. Its data system program includes a special check for returns over a certain secret figure. The computer will note and flag returns which depart markedly from expectations. An audit may be indicated for taxpayers who list substantially more in the areas of charitable contributions, interest payments, and medical expenses than they have in previous years and/or exceed the normal figures expected for individuals in their income bracket. A combination of incongruencies will increase greatly the likelihood of an audit by mail or through a personal interview.

At the present time approximately one in 44 returns is audited. This the computer does not do. It verifies arithmetic, prepares tax bills, and indicates which returns should be audited. The auditing process itself, however, is not automated. Based on the number of revenue agents it has, a district Internal Revenue Service office advises the Martinsburg computer system of the number of returns it has the manpower to audit. Given a figure of, for example, 75,000, the data processing center supplies the office with the names of the 75,000 "best" candidates for

further examination based on how far these people depart from the standard categories.

Federal officials feel that automatic data processing is geared to improving accuracy and equity in tax collecting. The efficiency of the system makes possible the collection of greater revenue at smaller cost. During the initial year in which computerized tax collection procedures were in operation in the Southeast, many tax delinquents paid taxes owed without governmental prodding in the belief that these omissions would be discovered by the government's computers. Computers have had, therefore, not only a technological but a psychological effect on tax collection procedures. Officials of the Internal Revenue Service also report that embezzling by agency employees has become harder since the processing of income tax returns was made the assignment of giant computers.

SOME RESPONSIBILITY FOR OUR CHAOTIC SOCIETY

S. R. Harrison, Ph.D.
The Norwegian Institute of Technology
Trondheim, Norway

Good for you and your articles on President Kennedy's assassination. Our country needs people like you and your staff who are willing to take a stand and fight for what they believe to be true.

The time is long overdue that our profession had some life injected into it and begins to accept some responsibility for our chaotic society. I find too many highly specialized journals "doing their jobs" in presenting only restrictive technical publications.

I applaud your efforts.

Unsettling, Disturbing, Critical . . .

Computers and Automation, established 1951 and therefore the oldest magazine in the field of computers and data processing, believes that the profession of information engineer includes not only competence in handling information using computers and other means, but also a broad responsibility, in a professional and engineering sense, for:

- The reliability and social significance of pertinent input data;
- The social value and truth of the output results.

In the same way, a bridge engineer takes a professional responsibility for the reliability and significance of the data he uses, and the safety and efficiency of the bridge he builds, for human beings to risk their lives on.

Accordingly, Computers and Automation publishes from time to time articles and other information related to socially useful input and output of data systems in a broad sense. To this end we seek to publish what is unsettling, disturbing, critical — but productive of thought and an improved and safer "house" for all humanity, an earth in which our children and later generations may have a future, instead of facing extinction.

The professional information engineer needs to relate his engineering to the most important and most serious problems in the world today: war, nuclear weapons, pollution, the population explosion, and many more.

RTR
CGO
NFH
WSW
PGZ
QGO
GVR
MFD
TKF
MTP

The Meaning of an Integrated Data System

W. R. Larson
Western Electric
Corporate Education Center
P.O. Box 900
Princeton, N.J. 08540

"If an enterprise ever achieves an optimum position of having its data so structured that it is suitable and available to all concerned in order to make the most effective decisions with the most efficient information, then the enterprise can be said to have a complete integrated system."

PRO
YTH
LDE
OFF
NEW
TTH
ETO
ESW
GIC

A socio-economic enterprise, whether it is a corporation, a government, a university, etc., should have the same underlying goal: to improve the environment of the society. There are many different approaches as to how society can be improved but it is not my intent to discuss or judge whether all of the different means are justified if they all reach their desired end. However, no matter what approach an enterprise takes, the internal activities of the enterprise can be structured in such a fashion as to achieve their goal, if they remember that they are also a part of the society. As to the internal activities of the enterprise, they are, or usually should be, structured in some systematic convention normally called a System.

Three Definitions of a System

A System has been called, "a whole that is more than the sum of its parts", e.g., a car is more valuable as a whole than all of the sub units (transmission, electrical system, etc.) added together as individual components. Another concept of a system is that it is the sum of its parts interrelated in such a fashion as to achieve some particular objective. A third, somewhat paradoxical, definition of a system is that a system is a method of attaining some desired position but delimiting the chance of optimizing that position.

There are many other definitions of the term System and they are probably all as valid as the ones mentioned above. It will be advantageous to remember at least these three definitions as we progress through the concepts of an integrated system.

Concepts of Integrated Data Processing Systems

Before we see what might be considered as a complete integrated system, let's take a look at the concepts of integrated systems as they exist today. Generally speaking, an integrated data processing system is one in which data can be inputted to a central computer from any outlying area by the use of some type of data transmission device and the output from the computer can be sent back to the locations in the same way. The areas or locations can be within the same building as the computer or miles away from it.

An expansion of this concept can lead us into what we might call an integrated computer system. The

word common is very significant to this type of system: a common data area of storage, a common way of storing data, a common way of retrieving data, and probably most important, having common data. The following discussion of these ideas is brief but hopefully thorough enough to give one an appreciation for these ideas.

A Common Data Area of Storage

The ultimate of this idea might be to have a central storage area for the entire enterprise where all the relevant data pertaining to any location is available to one or all who have the need to know what is happening throughout the enterprise. All of the advantages and disadvantages of the Principles of Centralization would apply in this situation.

The anticipated implementation of this idea would be to have all the location's data centralized at least within the location and available to all within the location. In a technical sense, all the data, as economically feasible, would be common to one computer structure.

A Common Way of Storing Data

We're not interested as much in the input media as we are in the form in which the data is actually stored in the storage area. All the data should be in such a form (not meaning binary, octal, etc.) that it can be processed in a standard method regardless of the purpose for storing the data. The editing, initializing, and updating procedures should generally be the same whether the data pertains to personnel, items, organizations, etc. And the logical way of actually storing the data (structuring the records, files, data sets, etc.) should be the same regardless of the storage device or program innuendos.

A Common Way of Retrieving Data

The method of accessing data within a computer environment should be the same whether the data is for program usage or report outputting. The data, having been stored in a common fashion, should be available to any type of program in its present structure. In other words, all algorithmic programs and report generators should be able to retrieve data in a common way.

Having Common Data

As was mentioned previously, common data is probably the most important aspect of integrated computer systems. Speaking in a broad sense, this means that our stored data is common (if applicable) to any or all usages. The data can be used in many different applications without having need for any redundant appearance of the data. Common data, pertaining to say employees, can be used for payroll, planning, personnel, control, or other purposes.

An Integrated System

Given what we called an integrated computer system, with a few additional concepts we can expand this into what is normally thought of as an Integrated System.

More Value From the Total Operation

Activities of an enterprise are represented by what we might call programs, computer type or otherwise. If these programs can be so designed that they can be linked together to facilitate the passage of data from one to another without any external changes, then we are receiving more value from the total operation than the sum of the individual programs gives us. More value not only in an economic sense, but the timeliness and completeness of the data enhances the chance of putting the information to more effective use.

Standardization

However, to achieve an integrated system there must be many standards on both a location and enterprise basis. Even the smallest sub-components of a system are so large in scope that they tend to become unruly and are usually standardized to some degree. In order to achieve the desired position of having an integrated system, standardization may tend to dampen a true envision of the activities of the enterprise: not so much how to unite them, but how to improve them should be the task. Creativity (if discernable) and good analysis tend to drown in a pool of standards. To pass data from one program to another in the most efficient manner so that the most effective use of that information can be made does not mean that the data itself is the most useful. Financial or management accounting activities of an enterprise are of this nature.

Changes in an enterprise's activities in its approach to reaching its goal should be conducted whenever it can be shown to be advantageous, not just necessary, and the changes should not just be mechanization.

Achieving a Complete Integrated System

If an enterprise ever achieves an optimum position of having its data so structured that it is suitable and available to all concerned in order to make the most effective decisions with the most efficient information, then the enterprise can be said to have a complete integrated system.

All of the activities of the enterprise must always be subject to improvement; moreover, the personnel and technical components of the enterprise must be flexible and dynamic enough to handle any possible changes. To state that we have optimized our position within a given set of constraints should never infer that the constraints that exist can not be reduced. □

C.a

NUMBLES

Neil Macdonald
Assistant Editor
Computers and Automation

A "numble" is an arithmetical problem in which: digits have been replaced by capital letters; and there are two messages, one which can be read right away and a second one in the digit cipher. The problem is to solve for the digits.

Each capital letter in the arithmetical problem stands for just one digit 0 to 9. A digit may be represented by more than one letter. The second message, which is expressed in numerical digits, is to be translated (using the same key) into letters so that it may be read; but the spelling uses puns or is otherwise irregular, to discourage cryptanalytic methods of deciphering.

We invite our readers to send us solutions, together with human programs or computer programs which will produce the solutions. This month's Numble was contributed by:

Andrew M. Langer
Newton High School
Newton, Mass.

NUMBLE 724

```
L U C K
+ I S
-----
L I U D
× T H E
-----
S K F E D
T K S H D
O L K T D
-----
U E H S L E D
```

UC = OF

2015 1837 9205 9

Solution to Numble 723

In Numble 723 in the March issue, the digits 0 through 9 are represented by letters as follows:

T = 0	O,W = 5
R = 1	Y = 6
V = 2	E = 7
I = 3	M,N = 8
L = 4	S = 9

The message is: Every mile is two in winter.

Our thanks to the following individuals for submitting their solutions — to **Numble 722**: Marijoe Bestgen, Shawnee Mission, Kans.; Ed Blake, Bellwood, Ill.; Wylie Crawford, Chicago, Ill.; and Walter Wesley Johnston, Springfield, Ill.

DALLAS: WHO, HOW, WHY? Part II

Mikhail Sagatelyan
Moscow, USSR

"Within a few days after the commission was formed, Earl Warren made a sensational and enigmatic announcement: he said that a number of facts and circumstances connected with the assassination of President Kennedy would possibly not be made public during the lifetime of the present generation. ... Today when most of the conclusions presented in the report of the Warren Commission have been disproved and it is not accepted in America nor anywhere else, Warren's statement becomes much more comprehensible."

Kennedy and Johnson

The day when the President-elect of the United States officially assumes his duties is precisely determined by law. This event always takes place on the 20th of January of the new year following Presidential elections. On that day the newly-elected President and Vice-President take their oath of office, subsequently review a military parade, and in the evening attend a traditional ball complete with film stars, waiters in tuxedos and champagne galore.

Usually, well ahead of the occasion, a colourful programme goes on sale in Washington which describes the ceremonies and gives the biographies of the President and Vice-President.

The custom was observed on January 20, 1961, when John Kennedy officially became President, and Lyndon Johnson Vice-President, of the United States. Leafing through the thick, glossy pages of the programme, I ran into the following paragraph in Johnson's biography:

So "Jack" and "Lyndon" — as they were so long known in the Senate, which as of now will begin to call them "Mr. President" and "Mr. Vice-President" — made many common causes, and also one rival cause. They both honourably and candidly sought the highest honour, the nomination for President. It was a good fight. For neither of those contestants was made of sugar candy; and neither was without weapons of skill and power which flash so gleamingly in the hands of that artist in public affairs, the truly professional politician.

But of course, somebody had to lose. The man who had won was big enough to turn at once to his fallen antagonist to permit him to keep his sword and to enlist that sword in what was now to be common cause again between the two. And the man who had lost was big enough to accept. The old Senior had become the new Junior; and both had reason to be glad.

Even discounting the sugary-pompous nature of the piece, inevitable in all official biographies published on such occasions, the description of the interrelationships between Kennedy and Johnson and the reasons given for their coming together, are flagrantly false. The single truth in the cited passage lies in one fact: Johnson was now in a subordinate position to Kennedy.

Kennedy and Johnson. "Jack" and "Lyndon" ...

They met for the first time many years before they found themselves in harness in the two top gov-

(Part 1 was published in the March issue of *Computers and Automation* March, 1971, pp 28-36. — Reprinted from *Sputnik*, published by Novosti Press Agency, Moscow, USSR.)

ernment posts in America. It happened in 1952, on the eve of Lyndon Johnson's election as Democratic Party Senate Leader, a position he had long coveted and fought for. Two days before the elections were to take place and in which all Democratic senators were to participate, the newly-elected Senator from Massachusetts, John F. Kennedy, walked into Johnson's office. The junior Senator did not much resemble the dignified image cultivated on Capitol Hill — he was wearing a loose sweater over casual slacks. After announcing that he intended to vote for Johnson's candidacy, Kennedy said good-bye and left.

"Seems like a nice kid," Lyndon Johnson said then, speaking from the heights of his Senatorial position. "Probably has a good future ahead of him."

That was the first encounter between the 35th and the 36th Presidents of the United States. However, their personal political fortunes and biographies crossed only in 1960, when both decided to seek the Presidential chair in the White House. The most obvious and intense area of struggle was the Democratic Party Convention in Los Angeles where in July the battle for who was going to be Democratic nominee unfolded.

The contest between Kennedy and Johnson was a routine one and was described by the American press no more sensationally than the rivalry between Kennedy and the rest of his opponents — Adlai Stevenson, Hubert Humphrey and Stuart Symington. There was nothing "fateful" about Los Angeles. That much I can vouch for since I was present at the Convention together with the TASS correspondents Harry Freeman and the late Ivan Beglov. It seems to me that the first overt clash between Kennedy and Johnson should be described the way it was seen at the time, when no one, obviously, could imagine that the road begun in Los Angeles would end in Dallas.

American party conventions could be compared to a chess tournament camouflaged as a circus performance. This is the way it was.

The Convention of the Democratic Party of the USA was held July 11 to 15 in an indoor sports arena capable of seating 20,000. The hall was filled with noise and excitement. Few of the 4,500 delegates present actually listened to whoever was speaking from the high and seemingly inaccessible rostrum. Participants freely wandered about the convention hall, smoked, and exchanged comments in loud voices.

In spite of the effectiveness and picturesqueness of the proceedings (which were televised), important decisions were not reached there, only announced with the bombast of a circus act introduction. In this respect the convention hall resembled a chess board. The "delegate-pawns", drawn up in invisible battle order, were ordered about by the leaders of

the state delegations — the "knights" and "bishops" of the Democratic Party who were right in the main body of the hall. On the platform were more important figures — leaders of the National Committee of the Party. They moved up and down the long rows of the platform like "castles" without ever descending to the floor.

The most important people were not there at all. They controlled their cohorts from a distance. They appeared in the hall only when the outcome of the tournament was clear to them and when only two or three foreordained moves were left to be played. So the real clashes took place across town, in the huge, old-fashioned Biltmore Hotel where the headquarters of the various contenders for the nomination had established themselves. And although on the surface everything appeared to be much more dignified and seemly than on the "chess board" of the convention hall, it was precisely in the suites of the Biltmore that the deals and intrigues took place, each contender having the sole aim of emerging victor-king, in order to do battle with the other victor-king — the winner on the Republican side of the national chess board.

John Kennedy and the chief organizer of his election campaign — his brother Robert — were not particularly worried by the insistent chanting from the galleries of the sports arena: "We want Stevenson! We want Stevenson!" They knew very well that the two-time loser in his bid for the White House was not their main opponent. A more dangerous man was Lyndon Johnson, Majority Leader of the Senate for many years. This was confirmed by the balloting: Johnson was runner-up to Kennedy.

Even before the Convention started, the Kennedy brothers knew they controlled the votes of 600 delegates — 161 fewer than they needed to win. These votes were obtained by Kennedy in a pre-convention effort in two ways: first through deals made with party bosses in big cities and secondly through an active campaign featuring personal appearances in many states of the Union. On the other hand, in accordance with agreements reached, a significant number of the votes were his only on the first ballot or at most, the second. If Kennedy had not achieved the required majority on the first count, he would have lost the votes of many states to other contenders. Therefore, the Kennedy strategy at the convention amounted to one thing — to win at all costs on the first ballot. The entire activities of their headquarters on the eighth floor of the Biltmore Hotel were directed to this end.

In this situation, Lyndon Johnson's main aim also came down to one thing — to prevent a Kennedy victory on the first count. Only then could Johnson hope to gather the necessary majority on subsequent ballots. So, no less actively than Kennedy, he appeared before unpledged delegations, trying to woo and win them. Johnson even agreed to a face-to-face confrontation with his adversary in front of a joint meeting of the New York and Massachusetts delegations. However, Kennedy — a brilliant and erudite speaker — had no great difficulty in demolishing Johnson, a pastmaster of back-room intrigues but not of open debate.

The last-ditch, desperate attempt made by Johnson's headquarters to stem the triumphant tide of the Kennedy forces was the assertion that Kennedy had an incurable disease — Addison's — that his days were numbered, and that therefore he should not be elected. This statement was made in Los Angeles by John Connally, Lyndon Johnson's campaign manager.

Such an attack, even by the low standards of American politics, was considered "below the belt".

But as a matter of fact the Kennedys were not left wanting. Their headquarters promptly published a medical report on Kennedy's health which quickly neutralised whatever potential harm the circulating rumours concerning "an incurable and fatal disease"¹ threatened. On July 13, John Kennedy was elected Democratic candidate for the Presidency by 806 votes. Lyndon Johnson received 409.

The press corps, both American and foreign, had become firmly convinced of a Kennedy sweep some 24 hours before the event and had predicted it in their despatches. There is no doubt that Johnson knew of his defeat even earlier. In any case, even before the convention began, he and his supporters behaved in such a way so as to ensure that Johnson would be Kennedy's running mate in the forthcoming elections. Phil Graham, publisher of the Washington Post and a trusted friend of Johnson's, first broached the subject to John Kennedy on the eve of the convention. Later, the "Great Texan" — Sam Rayburn, Speaker of the House of Representatives — had a conversation with Kennedy which Johnson thought settled the matter of his candidacy for the Vice-Presidency.

Therefore, when Kennedy met Johnson in the latter's suite in the Biltmore on the morning following Kennedy's victory, Johnson was quite sure what the topic of discussion was going to be. Later he described his conversation with the future President:

He told me that he had said many times that he thought I was the best qualified for the Presidency by experience, but that as a Southerner I could not be nominated. He said he felt that I should be the one who should succeed if anything happened to him.

Such is Lyndon Johnson's version. However, judging by what John Kennedy said, it went differently:

I didn't offer the Vice-Presidency to him, I just held it out like this [here he simulated taking an object out of his pocket and holding it close to his body] — and he grabbed at it.

The talk ended with a firm commitment from Kennedy on only one point: he would get in touch with Johnson within two or three hours.

On returning to his own headquarters, Kennedy announced to his aides: "You wouldn't believe it ... he's agreeable! He wants it!"

The reason for Kennedy's evident astonishment was revealed by a Kennedy staffer that evening to Theodore White, a journalist close to Johnson:

It was always anticipated that we would offer Lyndon the nomination; what we never anticipated was that he would accept.

And so the question was decided. Submissive to the will of the leadership, the convention declared Lyndon Baines Johnson Democratic candidate for the Vice-Presidency. The chess game in Los Angeles was over.

There was an undercurrent to the determination displayed by Lyndon Johnson and Democratic leaders from the South, West and certain other areas of the country to make sure he was Kennedy's running mate. But I learned of it only after the convention in Los Angeles. On the flight back to Washington, an American reporter I knew who had spent many years covering Congress said to me:

The Kennedys are dangerous to the oil industry. Whatever else they do, they'll try to put the squeeze on the oil people. Why? Because oil prices haven't suited old Joe for a long time. His main money is in real estate, in buildings which, as it happens, have to be heated. So if they can swing it ... But the Texan oil billionaires aren't out of their minds yet. Their man is right there, sitting on Kennedy's neck. What? You didn't know Johnson was their man? How long have you been over here? Almost a year? Then consider that half your time's been wasted if you don't realize things like that ...

My companion told another story. It seems that when Johnson's friends told him that the Vice-President has less power than the Majority Leader of the Senate, he replied with confidence: "Power is where power goes."

"Power is where power goes." His meaning became clear shortly after John Kennedy became President of the United States.

The structure of political power in America is such that the role of Vice-President in affairs of state is negligible. The only precisely defined responsibility he bears is to preside over the Senate: according to the American Constitution, the Vice-President is also President of the Senate. John Quincy Adams, the first Vice-President of the United States, made the following remarks concerning this oddity of American politics:

My country has, in its wisdom, contrived for me the most insignificant office that ever the invention of man contrived or his imagination conceived. I am Vice-President. In this I am nothing. But I may be everything.

Throughout the history of the United States all Vice-Presidents have had to reconcile themselves in one way or another to this interpretation of their position. At the beginning of Kennedy's Presidency, American history was enriched by a curious precedent. In February 1961 the following news spread through the White House: Johnson had prepared and sent to Kennedy a draft executive order according to which a number of Presidential functions would be handed over to the Vice-President. To this day the document has never been published although no one denies its existence. Therefore one is, of necessity, limited to the information that circulated among White House reporters at the time. Johnson was reported to have requested jurisdiction over the space programme, the Department of the Interior² and the Department of Justice (which meant including the FBI).

The story of the memo was taken as one more proof of Johnson's inordinate ambitions and lust for power, already well known in Washington. For a period of time the memo became a target of jokes in Washington political salons and Johnson was compared to William Seward.³ The Vice-President was infuriated when he learned he was the object of ridicule and he complained to the President, maintaining he had been "misunderstood". The tales ceased after that conversation and, luckily for Johnson, never appeared in the press.

Shortly afterwards, at a regular White House press conference, Kennedy announced that he was assigning an independent field of work to Johnson — the over-all leadership of the US space programme. There was nothing about transferring any other duties to Johnson. For that matter, the memorandum itself was never mentioned, even though the announcement was obviously the response to it. Power over departments having the most direct bearing on

Negro civil rights and control over exploitation of oil resources, Lyndon Johnson did not obtain.

In the first two-and-a-half years of his Presidency, Kennedy, as did most of his predecessors, punctiliously tried to ensure that the Vice-President enjoyed the respect without power due him according to the Constitution. Johnson wanted more, much more. But he preferred to suffer what he considered slights, in silence. Later, Johnson's biographer, Theodore H. White, was to write of that period:

Chafing in inaction when his nature yearned to act, conscious of indignities, real and imagined, Johnson went through three years of slow burn.

By 1963 Johnson had almost given up appearing at sessions of the Cabinet, official ceremonies, receptions and balls at the White House.

Johnson's absence was, of course, noted. The ubiquitous press began to seek an explanation. At a dinner in the Washington home of a prominent lobbyist, in early summer 1963, I first heard that Kennedy supposedly was going to refuse to have Johnson as his running mate in the Presidential elections scheduled for the fall of 1964. The thinking, as it was then outlined, ran: after the position taken by Kennedy on Negro civil rights⁴ there was no use counting on the white Southern vote anyhow, so Johnson in the next election campaign would be mere dead-weight.

At first these rumours did not receive even indirect confirmation. But at the beginning of September 1963, the Washington press blew up a story of financial manipulations by one Bobby Baker, the Secretary of the Democratic Majority of the Senate. To be honest, these manipulations were not all that scandalous or untypical. There were far worse goings-on in Washington and involving far more important figures at that. Nevertheless, the papers dug their claws into Bobby Baker and hung on.

As the scandal mounted, the real reasons for its exposure became clear: the Vice-President himself was involved! In 1955 Bobby Baker was appointed Secretary of the Democratic Majority of the Senate. Lyndon Johnson was Senate leader and the man who had given him the job. Baker was among the most trusted of Johnson's lieutenants. In 1957 he said of Baker that he was a man who truly served his country and Johnson considered him to be one of his most loyal, faithful and competent friends. Bobby Baker worked hard to get the support of a number of influential senators for his chief's bid to become the Democratic candidate for President in 1960. During the convention in Los Angeles, Johnson said Baker was his right arm; the man whom he consulted last at night and the man he saw first in the morning. Now the Washington press, and, following their lead, most of the newspapers in the country, emphasized that particular aspect — Bobby Baker's closeness to Lyndon Johnson and his personal financial affairs. Reporters even recalled the fact that Baker had named his son Lyndon Baines Johnson Baker. Baker himself had long been known in Congress as "Little Lyndon".

At first Bobby Baker was only accused of using his position in Congress for "shameless influence peddling" that netted him considerable income. Between 1955 and 1963, with an annual salary of \$19,600, he managed to "make" \$2,226,000, practically tax-free at that. Baker's main method of making money was extremely simple: by way of his people in the Senate and Government, he pushed through large-scale military orders to defence companies and received direct bribes or more often, indirect. Thus:

after securing a good government contract for North American Aviation Co., Baker was rewarded with exclusive rights for his company (legally in the name of a front man) to sell hot lunches, beverages, sandwiches, etc., at the multitude of plants run by the corporation.

It was because of this deal that the scandal came to light. Baker, it seems, had intended to share the catering franchise with another Washington wheel-dealer named Hill but later changed his mind. The incensed Hill went to court and began to tell all he knew of his former pal's activities — and he knew quite a bit. By October articles were appearing that suggested that Baker, under Johnson's direction, was the man who personally handled the large cash campaign donations that flowed in during the 1960 elections. Citing the names of witnesses, Hill maintained that a considerable share of the cash donations did not reach campaign coffers.

The "Baker Affair" immediately drew the attention of the Departments concerned. The Department of Justice played an active role in the investigation and as became known, already after John Kennedy's death, Robert Kennedy, the Attorney General, gave orders to use electronic listening devices in order to establish what relationship, if any, Johnson had to Bobby Baker's manipulations.

When the Washington newspapers The Evening Star and The Daily News first published the scandalous tidings, Johnson was in Western Europe. When he heard the news, Johnson curtailed his trip (even though according to the programme it was already coming to an end) and returned to Washington. The American correspondents who accompanied him maintained that his hurry was definitely caused by the unfolding scandal.

In Washington one of the Kennedy brothers (exactly which one has not been established) curtly informed Johnson that the FBI would carry out a full investigation of the Baker business. The Vice-President was not even asked his attitude to such an investigation. He was told and that was that. Later, at a regular White House briefing, President Kennedy promised that the nation would learn "the whole truth about Bobby Baker". Each new story published on the subject was like a hammer-blow to Johnson, causing irreparable political damage. On November 8, 1963, Life magazine printed a detailed story of the scandal. On one side of a two-page spread, the pictures of two of Baker's mistresses who were mixed up in the unsavoury business were published; facing them (full page) was a picture of Lyndon Johnson embracing Bobby Baker.

In spite of all this, Johnson did not make a single public statement on the subject. The Vice-President preferred to keep his own counsel.

Talk that Kennedy intended to "dump Johnson" was renewed with vigour. By then almost no one doubted its authenticity. The very fact that the President had promised the "whole truth" about Bobby Baker spoke volumes. The danger of being irretrievably politically compromised hung over Johnson.

On October 31, 1963, at a routine press conference, the President was asked a direct question: would he like to have Johnson as his running mate in the next elections and if so would Johnson's name go forward as a candidate for the Vice-Presidential post in the voting at the Democratic Party's next convention?

Kennedy answered both questions affirmatively. But he did so in such a way that his hands were not tied. The President's assertion met with disbelief: within a few days of the briefing the "Bobby Baker

Affair" had swollen with new details constituting an open threat to Johnson's reputation. The impression was created that the Kennedy brothers were leading up to a situation where the pressure of circumstances would force Johnson on his own initiative to refuse to stand for the post.

On November 12, 1963, President Kennedy called the first strategy meeting on the 1964 election campaign. However, neither Johnson nor his people attended. This fact, which became known almost right away to the White House press corps, was the last straw that convinced many that the Kennedys were, indeed, intending to "dump Lyndon".

Johnson himself, undoubtedly, had long known of these intentions. He and his circle could not help but see that events were moving in such a way that his whole future political career was under threat, the worst and most serious that the "Great Son of Texas", who had inherited the title after the death of "Mr. Oil" — Sam Rayburn — had ever faced in his whole life.

Besides this menace, there was another: the possibility that he would lose power even in his native state of Texas.

The Democratic machine in Texas was riddled with internal contradictions and in this respect the situation was very similar to the one that existed in the New York Democratic Party machine in 1959 and '60.5 Among the "liberal Democrats" in Texas, as the American press called them, dissatisfaction had grown with the men who represented the big oil interests — Johnson and his right-hand man John Connally who had resigned his post as Secretary of the Navy in order to be elected Governor of the State of Texas in 1962. Leaders of the Democratic Party organisations in Negro communities in Texas (the most politically active, by the way, of Negro communities in the South), trade union leaders, small businessmen, were all among the discontented. The owners of small and medium-sized oil companies, feeling the squeeze of the oil giants of Texas and other areas of the United States, formed the backbone of the movement. In the elections of 1956, Ralph Yarborough obtained the support of all these disaffected elements and was elected Senator from Texas in spite of the all-powerful Johnson and Connally. In order to characterise Yarborough politically, it is enough to say that at the Los Angeles Convention, Yarborough was the only Texan delegate to vote for Kennedy. The next three years showed that Senator Yarborough enjoyed Kennedy's unfailing support.

By the fall of 1963, Yarborough had good reason to think that as a result of the active campaign carried out in the rank and file of the Democratic Party in Texas, he and his supporters could hope to wrest control of the organisation from Johnson and Connally at the forthcoming 1964 convention of the Democratic Party of Texas. In 1964, with Kennedy's behind-the-scenes support, Yarborough intended to run against Connally whom he had almost defeated in 1962, for Governor of the State of Texas. On November 22, 1963, The Houston Chronicle, whose editor and owner was a Kennedy supporter, published the results of a poll conducted by its reporters which showed that 57 per cent of Texan voters were for Ralph Yarborough.

On October 4, 1963 (the Bobby Baker affair had been in the headlines for a month already) John Connally, Governor of the State of Texas, placed before the White House the question of Kennedy and Johnson making a trip together to Texas in order to "reconcile the local warring factions of Democrats before the elections". At first Kennedy did not agree to the suggestion: it would be better, he said, if Lyn-

don Johnson, the head of the Democratic Party machine in Texas, handled it himself. Kennedy also used the excuse of pressing government business.

Then Lyndon Johnson, in a private conversation with Kennedy supported Connally's proposal. Later, weighing each word carefully, Johnson admitted that they had, in fact, "discussed the political situation in Texas". After that talk Kennedy agreed to make the trip. But this decision did not lessen his reluctance to go, of which he spoke frankly to Pierre Salinger, his Press Secretary ("I wish I didn't have to go to Texas") and to Secretary of the Treasury, Douglas Dillon, who was scheduled to fly to Japan at the same time ("You're off to Japan and I've got to go to Texas. God, how I wish we could change places!")

It is not difficult to understand that the President's initial refusal to make the trip was dictated by his relations with both Johnson and Texas. Once he had decided that Johnson would not be his running mate in the next elections and believed that his stand on the Negro question had lost him the white Southern vote anyhow, what was the point of going to Texas? In addition, the object of the trip, dreamed up and organised by Johnson and Connally, was to strengthen their political hold on the state at the expense of their rival — Senator Yarborough whom the Kennedys supported.

Nevertheless, after the talk with Johnson, Kennedy agreed to go. To refuse would have meant that he openly repudiated Johnson. This the President was not yet prepared to do. Of all methods of fighting, the Kennedy brothers preferred the "double-game". One of the two participants in that conversation is dead. As for the other, whatever his version, let us be frank: neither America nor the world would ever take his word for granted, even if Johnson chose to speak some day. They wouldn't because too many of Johnson's reconstructions of talks with others (including people alive today) have turned out to be, to put it mildly, edited in Johnson's favour and the version contradicted by the other party.

This is really unfortunate. In the final count the riddle of Dallas would be more than half-solved if the world could learn the Vice-President's true motives when he insisted on "his" President travelling to Texas and particularly Dallas.

In truth, doesn't it become obvious after examining the host of serious political difficulties that Johnson fould himself in by October 1963, that he could disentangle himself only by a miracle or an accident? Miracles don't happen. Accidents, including planned accidents, including accidents to Presidents, do happen. In the circumstances, it is not surprising that even in America the Johnsons have been compared to the Macbeths.

As a matter of fact, at the end of 1969 the silence on this ticklish subject was broken — not by Johnson himself, but by his younger brother, Sam Houston Johnson. He wrote a book entitled My Brother Lyndon.

On the third or fourth day after the assassination in Dallas (for some reason the younger Johnson does not specify the exact date) when Sam Houston was in San Antonio, staying in the El Tropicano Motel (in order to escape hordes of reporters), Lyndon, by then President of the United States, telephoned him. The ensuing conversation took place as described by Sam Houston Johnson:

"I imagine you're pretty busy," I said.

"Never been busier," he said. "But I've been waiting for the chance to talk with you and to let you know how much I appreciate all you've done for

me, Sam Houston. I wouldn't be here if it hadn't been for you."

"Lyndon, I had nothing to do with Oswald."

"He gasped, sputtered and then exploded. My God, what an explosion! I have never heard him so angry. 'Goddamit, Sam!' he shouted. 'What the hell kind of a remark is that? Here I come all the way home to have a serious talk with you, and you come out with a damned stupid horrible crack like that! Why in hell can't you ever be serious, you crazy ass? You make your lousy sick jokes about everything ...' He went on like that, getting angrier and angrier, for about 20 minutes. I kept expecting him to slam the phone down. Finally, in a tired, somewhat despairing voice, he said, 'I'll call you some other time.'"

According to Sam Houston, Lyndon never referred to that telephone call ever.

It seems to me that the most interesting and indicative factor in this story is not so much that Johnson flew into a towering rage, but rather that his brother, who was privy to many of his political machinations in the past, should have said what he did. And it was no joke at all. The quick-witted Lyndon turned it into a joke to which he did not dare refer.

'What a Commission, Oh Lord!'

On the evening of November 25, 1963, after Kennedy's funeral, I learned the following:

Firstly, the same day, following the assassination, Lyndon Johnson decided that the investigating commission that had to be formed should be composed solely of Texans! The new President 'did not wish to include a single representative of the Federal Government.'

Secondly, he wanted to publish the FBI's initial report on the crime without first showing it to the Attorney General, Robert Kennedy.

How did all this become known to a few White House reporters? I think the former aides of the assassinated President made sure we knew. They did so with a definite aim in mind: the Kennedy clan wanted to prevent Johnson from succeeding in his plan to localise the investigation to Texas where he was all-powerful.

Unfortunately, even though there was no doubt of their authenticity, I could not report those sensational facts at the time. For one thing, by their very nature, they suggested that the new President had an odd desire to avoid a broad, full-scale investigation of the murder. Secondly, without naming sources, the story would have sounded flimsy and could easily have been denied and the author accused of "slanderous insinuations directed at the President of the United States". But the story was given to us with the understanding that the source would remain unnamed.

So the first time those two facts were published along with concrete names involved was in William Manchester's book Death of A President. According to Manchester, the Deputy Attorney General, Nicholas Katzenbach, who in the days following the assassination fulfilled the duties of the Attorney General as Robert Kennedy was tied up with "clan" affairs and the organisation of the funeral, learned of Johnson's decision on the make-up of the investigating commission. He immediately went to see Abe Fortas, a Washington lawyer and lobbyist close to the new President. Through Fortas, Katzenbach managed to dissuade Johnson from his original idea. From Fortas, Manchester writes, Katzenbach learned of Johnson's intention to publish the FBI report without

showing it to Robert Kennedy. The forceful and insistent Katzenbach was successful in persuading Johnson to change his mind on this as well. Since Manchester's book came out, none of the people involved by name has denied the story ...

Yes, Johnson's abortive attempt to establish a "Texan Commission" spoke of much and above all, perhaps, indicated that during Johnson's tenure of the Presidency, hopes for uncovering true reasons, motives and participants in the crime, were slim or non-existent.

Within a few days after the funeral of John Kennedy I also learned that the New York banker, John McCloy, who in the past had carried out delicate foreign assignments for the government, had, in confidential discussions with representatives of a number of European states who had arrived for the funeral, bluntly demanded that the press in their countries cease raising a fuss around the assassination, and desist from making insinuations regarding a "conspiracy". If they did not, McCloy threatened, United States relations with these countries would deteriorate drastically.

Such an appeal was revealing in itself: it meant that certain circles in America desired as little talk as possible of a conspiracy. Johnson has to be included in those "certain circles". It is impossible to imagine that McCloy could have conducted such talks without the knowledge and blessing of the new President.

The rest of the proceedings of the official investigation of the assassination showed that it was directed by a hand accustomed to the cowboy traditions of breaking in a horse.

On November 29, 1963, it was officially announced that President Johnson had set up a special commission to investigate the crime in Dallas. After several categorical refusals, Earl Warren, Chief Justice of the Supreme Court finally agreed to head it.

This is how Warren himself later described the talk which took place in the White House on November 29, 1963:

"I saw McGeorge Bundy first. He took me in, and the President told me how serious the situation was. He said there had been wild rumours, and that there was the international situation to think of. He said he had just talked to Dean Rusk, who was concerned, and he also mentioned the head of the Atomic Energy Commission, who had told him how many millions of people would be killed in an atomic war. The only way to dispel these rumours, he said, was to have an independent and responsible commission, and that there was no one to head it except the highest judicial officer in the country. I told him how I felt. He said that if the public became aroused against Castro and Khrushchev there might be war.

"'You've been in uniform before,' he said, 'and if I asked you, you would put on the uniform again for your country.'

"I said, 'Of course.'

"'This is more important than that,' he said.

"'If you're putting it like that,' I said, 'I can't say no.'"

In spite of Warren's chary and careful account (when it was published, Johnson was still President),

quite a few interesting features emerge. An analysis of the conversation (unfortunately Johnson has not published his version), bearing in mind what we already know of the new President's attitude to the Dallas killing, is of considerable importance.

Let us begin with Warren's initial refusal to take part in the commission. In a conversation with Nicholas Katzenbach which preceded Warren's interview with the new President, the Chief Justice explained his refusal thus: he had always believed that members of the Supreme Court should not be asked to take on responsibilities outside the framework of their direct duties. Such an explanation strongly suggests an excuse concealing weightier motives. After all, the country was rocked by the murder of its President; then, before the eyes of America, the alleged assassin was killed; the authorities in Dallas, violating every principle of law, utilized the mass media in order to convince the people of Oswald's guilt before any investigation was carried out and permitted flagrant violations of law that were in themselves highly suspicious.

So in his own way Johnson was quite right (when speaking of establishing "an independent and authoritative commission") that there was only one man in the country who could head it: the highest representative of the judiciary in the United States of America.

Earl Warren must have been perfectly aware of that himself. And still he tried to get out of it with an unconvincing excuse. Perhaps because Warren, along with many other prominent Washington figures, already suspected that in the prevailing situation the commission would not be allowed to get at the truth and he did not wish to become an associate in protecting those truly responsible for the crime.

Such a construction is not mere supposition, as may be thought at first glance. Within a few days after the commission was formed, Earl Warren made a sensational and enigmatic announcement: he said that a number of facts and circumstances connected with the assassination of President Kennedy would possibly not be made public during the lifetime of the present generation.

Reporters pressed for an explanation but Warren did not have another word to say. Today, when most of the conclusions presented in the report of the Warren Commission have been disproved and it is not accepted in America or anywhere else, Warren's statement becomes much more comprehensible.

But to return to the conversation between Lyndon Johnson and Earl Warren on November 29, 1963. The Dallas police announcement that "Oswald was a communist", Johnson called "wild rumours" and even expressed the anxiety that "if the public became aroused" it could come to war. It is not hard to see from Warren's writings that precisely these arguments convinced the Chief Justice to change his mind and accept.

"How is this?" the reader may well wonder. The same Johnson who was the first and only member of the Kennedy cabinet to put forward the "communist plot" theory after the murder, now, only a week later calls it "wild rumour". It would seem that on mature consideration the new President had rejected his own idea as nonsense. No. Johnson was not about to repudiate his initial interpretation. Let us remember that after his talk with Warren he repeated it in a written document to the Commission and, dis-

dainig the truth, attempted to enlist Robert Kennedy as one sharing his views.

What is the explanation? Johnson was maneuvering. When it was reported to him that Warren had refused to participate in the investigating commission and he learned the excuse, the new President must have guessed the true reason for the refusal ("this business stinks ..."). But now, when Johnson had failed in his attempt to set up an all-Texan investigation, he needed the Chief Justice of the Supreme Court with his prestige and reputation of being an honourable man, to head the commission. Johnson, a past-master of political mimicry, caught Warren, putting it crudely, on the hook of patriotism.

The Warren Commission began its work early in December 1963. The White House spared no efforts to force the American press to write nothing but eulogies of the Commission. "Our arms are being twisted," the franker reporters complained. But here and there discordant notes were sounded. The New York World Telegram and Sun wrote that great expectations should not be placed on the Commission as the conclusions it reached would depend wholly on the information placed at its disposal by the FBI and the Dallas police authorities.

Nevertheless, Americans continued to hope that in the course of its investigations the Commission would reveal the background and mechanics of the assassination.

As far as I and the rest of the Soviet newsmen stationed in Washington were concerned, naturally, above all we wondered how the "communist conspiracy" theory would fare in the hands of the Warren Commission.

* * *

Footnotes

1. The Kennedys got their own back, even though within the accepted framework. Their people spread rumours of Johnson's financial manipulations and connections with the oil kings. The candidate limited himself to a scornful reference to Johnson as "Colonel Cornpone." (Texans are fond of corn.)
2. In the USA the Department of the Interior handles natural resources among other matters and makes recommendations concerning laws governing the relations between the Federal Government and the oil industry.
3. Seward was Secretary of State under the Lincoln Administration and shortly after being appointed he demanded that Lincoln transfer a number of vital Presidential responsibilities to his jurisdiction.
4. Even the limited Civil Rights bill proposed met with sharp Congressional opposition and was not approved during Kennedy's lifetime.
5. The party apparatus in the State of New York was supposedly controlled by Carmine de Sapio and Michael Prendergast, two gangster-types. In fact, it was split by internecine warfare into several hostile groups and by the spring of 1960 the party bosses had full control of only a few areas in New York City itself. This fact did not escape the notice of the Kennedys. Their political allies under the leadership of old Joe Kennedy, began to quietly establish relations with the leaders of Democratic Party machines in various New York counties and with promises and when necessary, bribes and threats of exposure and scandal, began to weld together the antagonistic groupings of New York Democrats. Shortly before the Los Angeles Convention, de Sapio and Prendergast discovered

to their surprise that they were faced with two alternatives: either they came out against Kennedy and revealed that they had in fact lost control over the party apparatus, or they preserved the trappings of power and promised to support Kennedy. Even though the two bosses were furious and in any other circumstances would not have supported Kennedy, they were forced to capitulate. "Those Kennedys, they stole our State," Prendergast complained to close friends.

(To be continued in the next issue.)

C.a

ADVANCED NUMBLES

Neil Macdonald
Assistant Editor
Computers and Automation

An "advanced numble" is an arithmetical problem in which: digits have been replaced by capital letters; and the numbers are ordinary words. Each capital letter in the arithmetical problem stands for just one digit 0 to 9. Each digit is represented by just one letter (unless an equation, such as $M = K$, is also given). No easy clues (such as partial products in a multiplication) are ordinarily given. There may be more than one solution.

ADVANCED NUMBLE NO. 72401

Find one solution to: ONE X ONE = SEVEN

ADVANCED NUMBLE NO. 72402

Find one solution to: TWO X TWO = THREE

Solutions to Advanced Numble No. 72031

In Advanced Numble No. 72031 in the March issue, the letters stand for the following digits:

Solution 1:

Y = 0	C = 4	BON X BON = CANDY
O = 1	A = 5	213 X 213 = 45369
B = 2	D = 6	
N = 3		

Solution 2:

O = 0	N = 4	BON X BON = CANDY
D = 1	Y = 6	304 X 304 = 92416
A = 2	C = 9	
B = 3		

Solution to Advanced Numble No. 72032

In Advanced Numble No. 72032 in the March issue, the letters stand for the following digits:

T = 1	G = 6	ONE X TWO = EIGHT
I = 2	E = 7	397 X 183 = 72651
O = 3	W = 8	
H = 5	N = 9	

We invite our readers to send us solutions, together with human programs or a computer program which will produce the solution.

Political Lies: An Acceptable Level?

by Richard M. Nixon, President, U.S.A., the White House, Washington, D.C. — and 'The New York Times', General David M. Shoup, Senator J. William Fulbright, Senator Gaylord Nelson, the American Friends Service Committee, 'The San Francisco Chronicle', and others

"A responsible government has a duty to be prudent when it spends the people's money."

Outline

1. The F-111 Plane
2. The Department of Defense
3. How to be Prudent with Defense Budgets
4. The End of the War in Vietnam
5. American Combat Forces in Laos
6. American Combat Forces in Cambodia
7. The Army of South Vietnam
8. 'Peace' vs. Destruction

1. The F-111 Plane

The F-111 in a Nixon Administration will be made into one of the foundations of our air supremacy.

Richard M. Nixon
El Paso, Texas
November 2, 1968

MISSING F-111A IS HUNTED IN UTAH AND NEVADA WILDS

New York Times
February 14, 1969

F-111 ENCOUNTERS ANOTHER "WING BOX" PROBLEM AS CRACK DEVELOPS

New York Times
February 18, 1969

NELLIS A.F.B., Nev., March 4 (UPI)—An F-111A fighter-bomber crashed today. . . . The plane was the 2nd F-111A to crash in less than three weeks and the 13th to crash since the flight test program began.

New York Times
March 5, 1969

(Excerpted with permission from 'The Unholy Hymnal: Falsities and Delusions' compiled by Albert E. Kahn, published and copyright © 1971 by Simon and Schuster, 660 Fifth Ave., New York, N.Y., 1971, paperbound, 159 pp)

The Senate Permanent Subcommittee on Investigations issued a report in Washington yesterday calling the multibillion-dollar F-111 fighter-bomber program a "fiscal blunder of the worst magnitude."

Of the 500 [planes] to be built, the subcommittee said, fewer than 100 will "come reasonably close" to performing as originally intended. . . .

Among the contentions the report made were the following:

Roswell L. Gilpatrick, Deputy Secretary of Defense under Mr. McNamara, "was guilty of a flagrant conflict of interest" in the awarding of the F-111 airframe contract to the General Dynamics Corporation. He was "top level policy counselor" to the company for two and a half years before going to the Pentagon. . . .

Testimony given by [Secretary of Defense] McNamara was termed at various points "obviously intentionally deceptive," . . . and "an obvious and artful attempt to avoid telling the truth."

Richard Witkin
New York Times
December 19, 1970

2. The Department of Defense

I consider the Department of Defense to be a Department of Peace.

President Nixon
Washington, D.C.
February 6, 1969

America has become a militaristic and aggressive nation. . . . We maintain more than 1,517,000 Americans in uniform overseas in 119 countries. . . . We have an immense and expensive military establishment fueled by a gigantic defense industry. . . . Today the active armed forces contain over 3.4 million men and women. . . .

For far too many senior professional officers, war and combat are an exciting adventure. . . . It is this influential nucleus of aggressive, ambitious professional military leaders who are at the root of America's evolving militarism.

. . . Standing closely behind these leaders, encouraging and prompting them, are the rich and powerful defense industries. . . .

Militarism in America is in full bloom . . .

General David M. Shoup
Former Commandant U.S. Marine Corps
Article in *The Atlantic*
April 1969

. . . Since World War II we have spent roughly 10 times as much on warfare and its attendant requirements as we have on the welfare of our people.

Senator Fulbright
Washington, D.C.
June 4, 1969

3. How to be Prudent with Defense Budgets

A responsible government has a duty to be prudent when it spends the people's money. There is no more justification for wasting money on unnecessary military hardware than there is for wasting it on unwarranted social programs.

President Nixon
Colorado Springs, Colorado
June 4, 1969

According to Senate Majority Leader Mike Mansfield, the U.S. has spent \$23 billion on missile systems that either were never deployed or were abandoned. In a paranoid system, waste is a way of life.

. . . If one rationale for building a new weapons system is exposed as nonsense, others spring up to take its place.

. . . Virtually the only people making decisions as to whether new weapons systems are needed, whether they cost too much, and who should make them, are men who directly and personally stand to benefit from big defense budgets.

Richard J. Barnet
The Economy of Death, 1969

Quite simply the MIC [Military-Industrial Complex] consists of the sprawling Pentagon and its network of defense suppliers and research facilities that together produce America's armed might. During the course of the cold war it has grown into an \$80 billion-a-year juggernaut consuming a tenth of the nation's giant-sized gross national product. . . .

Sen. Gaylord Nelson of Wisconsin says: "The whole economy is infiltrated. We are a warfare state."

Newsweek
June 9, 1969

4. The End of the War in Vietnam

I pledge you tonight that the first priority foreign policy objective of our next Administration will be to bring an honorable end to the war in Vietnam. . . . My fellow Americans, the dark long night for America is about to end.

Former Vice President Richard M. Nixon
Presidential Nomination acceptance speech
Republican National Convention
Miami, Florida
August 8, 1968

5. American Combat Forces in Laos

QUESTION: Mr. President, there's been growing concern, sir, about deepening U.S. involvement in Laos. If you could confirm that, would you also say whether this runs counter to your new Asian policy?

PRESIDENT NIXON: There are no American combat forces in Laos. . . .

QUESTION: Mr. President, you say there are no combat forces in Laos. How do you regard the airmen who bomb the Ho Chi Minh trail from bases in Thailand and Vietnam? Would you regard those as combat forces?

PRESIDENT NIXON: . . . we do have aerial reconnaissance, we do have, perhaps, some other activities.

News Conference
Washington, D.C.
September 26, 1969

There are no American combat troops in Laos.

President Richard M. Nixon
Washington, D.C.
March 7, 1970

WASHINGTON (CDN)—Tens of thousands of Americans have engaged in combat activities in the secret war in Laos. . . .

The United States has spent more than a billion dollars on the war—almost all of it in secret.

These are some of the key facts to emerge with the publication of the Senate Foreign Relations Committee testimony taken at closed hearings on Laos. . . .

Essentially, testimony shows, the Nixon administration has concealed the dimensions of the aerial war by emphasizing the relatively small number of U.S. personnel actually based in Laos. This figure is no more than 2000. Yet this 2000 represents only a tiny fraction of those involved in combat activities in Laos, because most of those engaged in combat haven't been stationed in the country.

James McCartney
San Francisco Sunday Examiner & Chronicle
April 26, 1970

LAIRD ADMITS GI'S DO GO INTO LAOS

San Francisco Chronicle
May 19, 1970

6. American Combat Forces in Cambodia

Officials in the White House, the Pentagon and the State Department . . . strongly reaffirmed the United States policy of not widening the war in Vietnam. They said the rules of engagement had not been changed to allow American forces to penetrate Cambodia.

New York Times
March 28, 1970

We finally have in sight the just peace we are seeking.

President Nixon
San Clemente, California
April 20, 1970

This is not an invasion of Cambodia. . . . We take this action not for the purpose of expanding the war into Cambodia but for the purpose of ending the war in Vietnam, and winning the just peace we all desire.

President Nixon
Washington, D.C.
April 30, 1970

NIXON SENDS COMBAT UNITS INTO CAMBODIA TO ATTACK COMMUNIST STAGING AREA

New York Times
May 1, 1970

In terms of military objectives, the main points made by the President in his speech of April 30 announcing the action were two: that the enemy was "concentrating his main forces in the sanctuaries where they are building up to launch massive attacks on our forces," and that in the eastern border areas of Cambodia there was "the headquarters for the entire Communist military operation in South Vietnam."

The headquarters has not been found; hardly anyone believes any more that it existed. Nor did our invading armies find the slightest evidence of Communist troop concentrations prepared for a "massive" attack on South Vietnam; virtually no enemy troops were in the border areas.

Anthony Lewis
New York Times
June 6, 1970

(please turn to page 50)

NEW CONTRACTS

TO	FROM	FOR	AMOUNT
National Cash Register Co. of Canada, Ltd., Toronto, Canada	Canadian Department of Industry, Trade and Commerce, Ottawa, Canada	A research and development program over the next five years; project involves development of new types of equipment for the banking industry	\$16.6 million
Honeywell, Inc., Tampa, Fla.	U.S. Air Force Rome Air Development Center, Rome, N.Y.	Development and installation of an automated technical control (ATEC) system for Defense Communications System (DCS); system will automate many of the technical control functions now performed manually throughout the DCS	\$6.9 million
Honeywell Aerospace Division, St. Petersburg, Fla.	Martin-Marietta	Building the Guidance Control and Sequencing Computer (GCSC) for the Viking Mars lander; computer will direct descent and landing of capsule to the Mars surface; control a number of instruments designed to perform scientific analyses and obtain surface photographs	\$6.3 million
Computer Sciences Corp., Los Angeles, Calif.	Atomic Energy Commission, Nevada Operations Office	A three-year contract extension for continued facility management services at the AEC's Nevada Operations Office	\$3.5+ million
PRC Information Sciences Co., Los Angeles, Calif.	Air Force Systems Command's Rome Air Development Center, Rome, N.Y.	Developing a microform system (for Air Force Military Personnel Center, Randolph Air Force Base, Texas) by converting master personnel records of active duty officers to a microfiche file; will lead to a complete automated system for conversion, maintenance, use and retirement of all Air Force master personnel records including Air Force Reserve and Air National Guard	\$3.5 million
Sanders Associates, Inc., Nashua, N.H.	Cunadata Corp., Madison, Wisc.	Sander's "Can Do" programmable computer terminals to be incorporated into a nationwide data processing network for credit unions; comprised of a video display, keyboard, magnetic tape cassette and hardcopy printers	\$3.4 million
Control Data Corp., Minneapolis, Minn.	University of Montreal, Montreal, Quebec, Canada	Expanding computer complex; major users will be departments of mathematics, nuclear physics lab, computer sciences, school of architecture and school of law	\$3.1 million
Ampex Corp., Marina del Rey, Calif.	Raytheon Co., Equipment Div., Sudbury, Mass.	Model 1885 core memory system for data processing and air traffic control equipment for FAA	\$2+ million
Datacraft Corp., Ft. Lauderdale, Fla.	Greyhound Leasing Corp.	Magnetic core memory systems, plug-to-plug compatible with IBM System/360 Series computers; will be used for add-on or replacement applications	\$2+ million
International Computers (South Africa) (Pty.) Ltd.	South Africa Department of Statistics, Pretoria	Large-scale ICL System 4-72; equipment is specifically designed for on-line processing and communications based systems	\$1.6+ million
Hazeltine Corp., Greenlawn, N.Y.	Boeing Co., Seattle, Wash.	Developing and supplying Airborne Computer-Driven Display System for AWACS (U.S. Air Force Airborne Warning and Control System)	\$1 million
Mine Safety Appliances, Co., Pittsburgh, Pa.	U.S. Bureau of Mines	Design, manufacture and installation of a mine air surveillance and monitoring system; intended to bring a new level of safety to coal mining operations	\$606,000
Rapidata, Inc., Fairfield, N.J.	New Jersey Bell Telephone Co.	Providing dedicated computer services	\$230,000+
Goodyear Aerospace Corp., Akron, Ohio	U.S. Air Force, Air Force Human Resources Laboratory, Williams AFB, Phoenix, Ariz.	A prototype of a flight formation simulator which should reduce the time and costs of teaching student pilots formation flying	\$200,000 (approximate)
Kustom Electronics, Inc., Chanute, Kans.	New York State Police, Albany, N.Y.	Four Mobile Communications Terminals (MCT-10) for communication between squad cars and a central police control computer; to be installed in patrol cars in the Albany area	\$65,000 (approximate)
Ampex Corp., Redwood City, Calif.	Modular Computer Corp., Fort Lauderdale, Fla.	Core memory stacks which will provide mainframe memory for a new series of Modular computer systems	\$400,000+
Corporation S, Dallas, Texas	Republic Money Orders, Inc.	Automated system for reading and recording on magnetic tape selected information from the register copy of money orders	—
Incotel, Ltd., New York, N.Y.	Kansas City International Airport, Kans.	Supplying software programs which control computerized information systems being installed by TWA and Braniff	—
Memory Technology, Inc., Sudbury, Mass.	Memorex Corp., Santa Clara, Calif.	Over 100 READ-Only Memory Systems used to provide control storage for Memorex's 660 Disc Controller	—
Univac Division of Sperry Rand Austria	Grosseinkaufsgenossenschaft Österreichischer Consumvereine (GÖC), Vienna, Austria	A UNIVAC 9700 system; applications will include billing, preparation of delivery notes, sales statistics, inventory status, general accounting and payroll processing	—

NEW INSTALLATIONS

OF	AT	FOR
Burroughs 3500 system	Federal Reserve Bank, Richmond, Va. (2 systems)	Processing bank checks, government checks, and United States postal money orders (systems valued at \$1.5 million)
Control Data CYBER 70 Model 72	Free University of Berlin, Germany	Research, teaching and administration; will be connected to a CDC 6500 at Berlin Technical University to provide a dual system for both schools for scientific problems requiring massive calculations (replaces a CDC 3300) (system valued at \$951,000)
Control Data 3170 system	Wyoming Employment Security Commission (ESC), Casper, Wyo.	Job matching, processing statewide employment records and unemployment insurance claims
Control Data 3200 system	Consolidated Forwarding Co., St. Louis, Mo.	Business data processing, e.g., payrolls, general and revenue accounting, statistics and freight billing (system valued at \$362,000)
Control Data 6400 system	University of Virginia, Charlottesville, Va.	Handling academic instruction, student and faculty research projects, and support data processing and consulting services for 20 colleges and universities in northern Virginia (system valued at \$2 million)
Control Data 6500 system 6600 system	United Computing Systems, Inc., Kansas City, Mo.	Expanding nationwide remote computing services (systems valued at about \$5 million)
EMR 6050 system	Institute of Applied Geophysics, Brno, Czechoslovakia	Handling data for programs aimed at increasing the country's national petroleum and gas production (system valued at \$600,000)
Honeywell Model 58 system	The Canadian National Institute for the Blind, Toronto, Canada	Expanding and improving services to Canada's 27,000 registered blind persons; initial use is administrative; future plans include on-the-job programmer training, a job matching service, use as a research tool for ophthalmologists, and as a data bank of information to agencies sharing service to the blind
Honeywell Model 115 system	Rand Whitney Co., Worcester, Mass. Risdon Manufacturing Co., Naugatuck, Conn.	Machine utilization, production costing, revenue reporting and payroll applications Production scheduling, inventory reporting and control, inventory simulation and forecasting and other manufacturing-related applications
Honeywell Model 115/2 system	Wean United Incorporated, Pittsburgh, Pa.	Numerical control, engineering and accounting applications
IBM System/3	Ratrie, Robbins and Schweizer, Inc., Baltimore, Md.	A job costing system that indicates, on a daily basis, profit or loss on each project under construction
IBM System/3 Model 6	U.S. Cold Storage Corp., Philadelphia, Pa.	Tracking exact location of 11 million pounds of frozen food moving in and out of USCS's freezers and coolers each month; computer-produced reports also pinpoint, well in advance, shipment, delivery and removal dates for each lot
ICL 1904A system	British Aircraft Corp., Fairford, Glos., England	All work connected with flight testing of Britain's Concorde prototype and production models capable of processing several flights simultaneously (system valued at over \$2 million)
UNIVAC 1106 system	Commonwealth Associates, Inc., (CAI) Jackson, Mich.	A UNIVAC 1106 time-sharing operation concerning engineering design applications; batch mode of operation will be concerned with various accounting and administrative tasks (system valued at \$1 million)
UNIVAC 9200 system	Express Freight Lines, Milwaukee, Wis.	A number of operations to improve efficiency and service to customers
UNIVAC 9200 II system	The Kellogg Company, Battle Creek, Mich. Nikkan Sports News, Tokyo, Japan Tokyo Malt Clothing Co., Tokyo, Japan	Inventory and production control, cost accounting and payroll processing; also, computers are linked to an 1106 at headquarters to that data can be interchanged between the facilities in Nebraska, Tennessee and California Serving as the heart of an automated editing and printing system Inventory control
UNIVAC 9400 system	Clapper Publishing Co., Park Ridge, Ill. Coutts and Company, London, England Ontario Hospital Association, Toronto, Canada Washington State Community College District 17, Spokane, Wash.	Order entry, customer list maintenance and mail order processing First step in the establishment of real-time banking system; system, which supersedes one of two UNIVAC 9300 computers, will be linked to 33 UNIVAC DCT-1000 Data Communication Terminals Processing of all types of medical information; preparation of costing statistics for 300 hospitals; and keeping track of all Ontario hospital employees pension contributions Vocational and technical training of students in all phases of data processing, including training in hospital computer programs for health occupation students, student services, financial and personnel services; eventually to serve all community colleges in North-eastern Washington State

NAME OF MANUFACTURER	NAME OF COMPUTER	DATE OF FIRST INSTALLATION	AVERAGE OR RANGE OF MONTHLY RENTAL \$(000)	NUMBER OF INSTALLATIONS		NUMBER OF UNFILLED ORDERS
				In U.S.A.	Outside U.S.A.	
Siemens	301	11/68	0.75	-	-	82 C
Munich, Germany	302	9/67	1.3	-	-	28 C
(A)	303	4/65	2.0	-	-	70 C
(July, 1971)	304	5/68	2.8	-	-	63 C
	305	11/67	4.5	-	-	93 C
	306	-	6.5	-	-	- C
	2002	6/59	13.5	-	-	39 C
	3003	12/63	13.0	-	-	32 C
	4004/15/16	10/65	5.0	-	-	99 C
	4004/25/26	1/66	8.3	-	-	54 C
	4004/35	2/67	11.8	-	-	185 C
	4004/135	-	17.1	-	-	- C
	4004/45	7/66	22.5	-	-	248 C
	4004/46	4/69	34.0	-	-	10 C
	4004/55	12/66	31.3	-	-	22 C
	4004/150	-	41.0	-	-	10 C
	4004/151	-	51.5	-	-	22 C
	404/3	-	1.9	-	-	- C
	404/6	-	-	-	-	10 C
						Total: 298
USSR	BESM 4	-	-	-	-	C C
(N)	BESM 6	-	-	-	-	C C
(May 1969)	MINSK 2	-	-	-	-	C C
	MINSK 22	-	-	-	-	C C
	MIE	-	-	-	-	C C
	NAIR 1	-	-	-	-	C C
	ONEGA 1	-	-	-	-	C C
	URAL 11/14/16	-	-	-	-	C C
	and others	-	-	-	-	C C
						Total: 6000 E
						Total: 6000 E



PROBLEM CORNER

Walter Penney, CDP
Problem Editor
Computers and Automation

PROBLEM 724: CHAFING AT THE BIT

"Pete," said the boss, "I've been looking over our telephone charges. They've been increasing pretty rapidly and I thought we might be able to cut down somewhere. The biggest item seems to be our field station."

"Yes, there's a lot of data being sent in connection with that Delphide experiment."

"What does that involve?"

"You know how the experiment is set up. Well, seven trials are made simultaneously and the number of successes is sent back here. Since there are eight possible outcomes three bits are used. The data are concentrated and sent as a solid stream of bits. I don't think you can beat that."

"I'm not so sure. How are these numbers of successes distributed? Normally?"

"More like Poisson. Zero successes is the most common outcome; about a third of the experiments have no successes. Then they tail off so that seven successes is very rare, occurring only about 1.4% of the time."

"If there's that much variation we ought to be able to effect some economies. It might pay to use more than three bits for some of these rare values and fewer than three for the ones that occur often."

"But," said Pete, "One of the advantages of using three bits is that we don't need spaces. If you use variable length equivalents, wouldn't you need a space to show where one ends and the next begins?"

"No, not if the equivalents are properly chosen. Have you any figures on the frequencies of these outcomes?"

Pete fumbled through a folder. "Here's a sheet with the latest figures. On the average 0 to 7 successes occur respectively 120, 72, 60, 45, 30, 18, 10 and 5 times out of 360."

"O.K. Let's see whether we can work out a system of equivalents averaging less than three bits and still separable without ambiguity."

Solution to Problem 723: Behind the Eight Ball

The fifteenth number on the list will be 8 018 018 088. After this we must use digits other than 8 (4, 5, 9, 1 and 7 in order), so that the twentieth number will be EIGHT-BILLIONEIGHTEENMILLIONEIGHTEENTHOUSAND-EIGHTHUNDREDEIGHTYSEVEN.

Readers are invited to submit problems (and their solutions) for publication in this column to: Problem Editor, Computers and Automation, 815 Washington St., Newtonville, Mass. 02160.

ADVERTISING INDEX

Following is the index of advertisements. Each item contains: name and address of the advertiser / name of the agency, if any / page number where the advertisement appears

- ACM, 1133 Ave. of Americas, New York, N.Y. 10036 / Corporate Presence, Inc. / Page 51
- COMPUTERS AND AUTOMATION, 815 Washington St., Newtonville, Mass. 02160 / Pages 2, 3
- GML CORPORATION, 594 Marrett Rd., Lexington, Mass. 02173 / Page 52
- MICROFILM PRODUCTS, INC., 40 West 15 St., New York, N.Y. 10011 / S. Frederic Auerbach Co., Inc. / Page 27
- SIMON AND SCHUSTER, 630 Fifth Ave., New York, N.Y. 10020 / Page 50

7. The Army of South Vietnam

The morale and self-confidence of the Army of South Vietnam is higher than ever before.

President Nixon
Washington, D.C.
June 30, 1970

... tonight I can report that Vietnamization has succeeded.

President Nixon
Washington, D.C.
April 7, 1971

SAIGON DESERTIONS UP NEARLY 50% IN SPRING*

New York Times
July 27, 1970

* The average monthly desertion rate from the South Vietnamese Army, reported this dispatch from Saigon, was about 8,000 in 1969; the number of deserters had risen to more than 11,000 in May 1970 and to nearly 12,000 in June.

The Central Intelligence Agency has told President Nixon that the Vietnamese Communists have infiltrated more than 30,000 agents into the South Vietnamese Government in an apparatus that has been virtually impossible to destroy.

Neil Sheehan
New York Times
October 19, 1970

8. 'Peace' vs. Destruction

The peace we seek ... is not victory over any other people, but the peace that comes with healing on its wings, with compassion for those who have suffered, with understanding for those who have opposed us ...

President Nixon
Washington, D.C.
January 20, 1969

It has been more than a year since the rhetoric of peace began in Vietnam. During this time scores of thousands of men, women and children have died in the fighting. . . .

The human situation today in Vietnam is worse than it has ever been. An entire nation is being destroyed and the tempo of destruction has increased. One third of the rural people of this rural nation have become refugees. Hundreds of thousands of acres have been defoliated, countless villages have been razed. . . . The American Friends Service Committee, which has been involved in the relief of war suffering for more than half a century, has rarely encountered such misery as in Vietnam today.

From a White Paper on Vietnam
issued by the American Friends Service Committee,
inserted in the *Congressional Record*
May 7, 1969

There were about forty or forty-five people that we gathered in the center of the village . . . men, women, children . . . babies. . . . Lieutenant Calley . . . started shooting them. And he told me to start shooting. I poured about four clips into the group . . . I fired them on automatic . . . I might have killed ten or fifteen of them. . . . So we started to gather them up, more people . . . we put them in the hootch, and we dropped a hand grenade in there with them . . . they had about seventy or seventy-five people all gathered up. So we threw ours in with them and Lieutenant Calley . . . started pushing them off . . . into the ravine . . . and just started using automatics on them . . . men, women, children . . . and babies. . . . It just seemed like it was the natural thing to do at the time.

Paul Meadlo,
Former U.S. Army private, American Division,
describing the massacre at My Lai, South Vietnam
Interview on CBS-TV
November 24, 1969

In his book *Militarism, U.S.A.*, Colonel James A. Donovan writes: ". . . at the end of October, 1968, when bombing of the North halted, the total bomb tonnage dropped in both North and South Vietnam was given as 2,948,057 tons. (Total tonnage dropped by U.S. aircraft in World War II, in both European and Asiatic theaters, was 2,057,244.) So we dropped almost 50 percent more bombs on Vietnam than in both Europe and the Pacific."

WOULD YOU BELIEVE

- Richard M. Nixon
- Spiro T. Agnew
- Lyndon B. Johnson
- Hubert H. Humphrey
- Robert S. McNamara
- Melvin R. Laird
- Dean Rusk
- William P. Rogers
- Maxwell Taylor
- William C. Westmoreland
- John N. Mitchell
- J. Edgar Hoover

YOU WOULD! THEN READ

The Unholy Hymnal

Falsities and Delusions
Rendered by the Foregoing
and
Other Choir Boys of the Credibility Gap

Compiled by
Albert E. Kahn

Simon and Schuster Cloth: \$4.95
630 Fifth Ave. Paper: \$2.95, a Touchstone Book
New York, N.Y.





**Adrian Ruyle's
committee wants
you in Boston
August 14-16.**

For a no-tea-party ACM 72.

Adrian Ruyle, recently of MIT's Lincoln Laboratory and now head of ARS Training Systems, is our Northeast Regional Representative. He's no stranger to ACM annual technical conferences—having attended each one since ACM 65. Over the years, he's formed some strong opinions on how they should be run.

Now he's doing something about them. As General Chairman of ACM 72 to be held in Boston August 14-16, Adrian is helping his committee cook up a thoroughly professional program.

"It'll be no Boston 'tea party'," says Adrian. "We're cutting out the frills. ACM 72 will stand or fall on its service to our members. We want people to know what's going on in every major field of computing—and then to get more involved in their areas of interest at ACM.

"Our call for papers has produced a phenomenal response. Each Special Interest Group and Committee will showcase new developments in its own area. There will be challenges for the experts—and special tutorial

sessions for anyone who wants background on a particular topic. Overall it will be an excellent chance for members to renew or enlarge their ties with ACM. Or for non-members to join."

Plan now to join us at ACM 72. If you are not a member, part of your admission fee can be converted to annual dues—saving you \$25. Send in the coupon today!

ACM 72 Committee:
Walter Abrams
Jack Crowley
Jeffrey DeVeber
James Donohue
John Donovan
Carol Giltner
Elden Levine
Adrian Ruyle
Kenneth Scott
Rosemary Shields
Richard Waterhouse
Gunars Zagars

Association for Computing Machinery
1133 Avenue of the Americas
New York, New York 10036

I am interested in ACM and ACM 72.
Please send more information.

Name _____

Position _____

Address _____

City _____ State _____ Zip _____

acm

**Association
for Computing
Machinery**

THE COMPUTER DISPLAY REVIEW

**DON'T LET A
CONSULTANT SNOW YOU!**

*Can he analyze, evaluate and
review every available display for you?*

And cost compare them?

The CDR does!

Here's the list . . .

ALPHANUMERIC DISPLAY EQUIPMENT

Aids Mark Series
Alphacom Model DW-33
American Data Systems 760 Video Terminal
Applied Digital Data Systems Consul
Applied Digital Data Systems Envoy
Atlantic Technology 2000 Series Data Display Terminal
Beehive Medical Electronics Models I, II, III
Bendix Interactive Terminal Logiport/1
Bunker-Ramo 700 Information System
Bunker-Ramo 2222 Control Unit
Bunker-Ramo 2223 and 2225 Control Units
Burroughs B9352 Input and Display Terminal
Burroughs B9351 Input and Display Terminal
Communitytype 1000 Series
CII 6100 Display System
CII 6300 Display System
Comutek Series 100 Terminal
CC-30 Communications Station
Computer Communications Totelcom (CC-335)
Computer Optics CO: 70
Computer Terminal Datapoint 2200
Computer Terminal Datapoint 3300
Computer Terminal Datapoint 3360
Conrac 201 Data Display Terminal
Conrac Contractor 401
Control Data 210 Series Display System
Courier Executerm I
Courier Executerm 60 and 65 and
Executerm 260 and 265
Data Disc 6200 Television Display System
Data Disc 6500 Graphic Display System
Data Dynamics Model 5000
Data 100 Model 73
Delta Data Systems Delta 1
Delta Data Systems Telterm 1, 2, 3
Elliott Series 20 CRT Display System

Ferranti 50/60 Display System
Ferranti TDM 1000/2000 Display System
Foto-Mem Foto-Vision
Four-Phase Systems: System IV/70
Honeywell Datanet 760 System
Hazeltine 2000
Hendrix Series 5100 Display Terminal
Hughes HDC/HDM Digital-Video Data Display
Incoterm SPD 10/20
Infoterm VISTA Series
IBM 2260/2848 Display System
IBM 2265/2845 Display System
IBM 3270 Information Display System
ITT 3100 Alphascope
Lear Siegler Interactive Display Terminal
Marconi Series X4000
Mark Computer Systems DD-70
Megadata S/R 900 and 1000 Series System
Mitsubishi Character Display System
Monitor Systems 8200
NV Philips Character Display Unit P1088
Omera/Segid Datascope 500
Omera/Segid Datascope 800
Philco-Ford CUE
Philco-Ford Alphanumeric Color Display Unit
Model D-20
Philco-Ford Alphanumeric Display Unit
Model D-21
Photophysics '45' Series
Plessey Series 100
RCA DIVCON
RCA 70/752 Video Data Terminal
Raytheon DIDS-400 Display System
Raytheon DIDS-500 Digital Information Display
Raytheon Data Systems PTS 100
Sanders 720 Data Display System
Sanders 620 Data Display System
SEFAC Mark II Display System

SE Laboratories Video Display
SINTRA TE 1000 Display System
SINTRA TE 4000
Spiras Systems IRASCOPE
Stromberg DatagraphiX 1110 Display System
Toshiba DDS-110 and DDS-120
Toshiba DDS-140 Color Display
TEC Series 400 Data Screen Terminal
Trivex 40/80
Ultronic Videomaster 7000 Series
Univac Uniscope 100
Univac Uniscope 300
Video Systems VST Series
Wyle Computerminal Model 600
Xerox BC100/BC200 Display System

LINE-DRAWING DISPLAY EQUIPMENT

Adage Graphics Terminal
AEG Telefunken SAP 200
AEG Telefunken SAP 300
AEG Telefunken SIG 100 Data Display Unit
Control Data 250 Digital Data Display
Control Data Grid Display Subsystem
Control Data 1744/274 System
Control Data 3344/274 System
Control Data Variable Intensity Display
DEC 338/339 Program Buffered Displays
DEC 340 Precision Incremental CRT Display
DEC Graphic 15
Evans & Sutherland Model I
Ferranti Argus Display Systems 30 and 40
Graphic Displays ETOM 2000
Imlac PDS-1 Display Computer
IDI IDI10M/II
IDI Model E1
IDIGraf Display Terminal
III 1060 Graphical Display
IBM 2250 Model I Display Unit
IBM 2250 Model III Display Unit
IBM 2250 Model IV Display Unit
ICL 928 Graphical Display System
ICL 1830 Graphical Display
ICL 4280 Graphical Display System
ITT Modular Alter and Compose Console
ITT Operations Planning System Console
Lundy System 32 Display
Marconi Series X2000 Display System
Monitor Display 8100
Philco-Ford READ Model 512
RCA 6320 Integrated Display Console
Sanders ADDS/900 Advanced Data Display
System
SEL 816A Computer Graphics System
SINTRA GIDI Terminal
SINTRA VU 2000 Graphical Display System
Stanford Radio & Telefon ITT Grafoskop
Stromberg DatagraphiX 1090 Direct View
Display
Tasker Display Consoles Models 9100 and
9110
Tasker Display Consoles Models 9200 and
9210
Toshiba DDS 300 Graphic Display Unit
UNIVAC 1557/1558 Graphic Display
Subsystem
Vector General Graphic Display System
XDS Model 7580 CRT Display System

Storage Tube Display Systems

Comutek Series 400 Display System
Conograph Conographic/10
Corning 904 Display Terminal
DEC KV Graphics System
Princeton 801
Tektronix T4002 and T4002A Terminals

• This list will be out-of-date tomorrow. But you won't be. The CDR will keep you current.

GML CORPORATION 594 Marrett Road • Lexington, Massachusetts 02173
Publishers of Computer Characteristics Review

(617) 861-0515