NBSIR 76-1189

Report of the Workshop on Estimation of Significant Advances in Computer Technology

Computer Systems Engineering Division
Institute for Computer Sciences and Technology
Washington, D. C. 20234

December 1976

U. S. DEPARTMENT OF COMMERCE
NATIONAL BUREAU OF STANDARDS

NBSIR 76-1189

REPORT OF THE WORKSHOP ON ESTIMATION OF SIGNIFICANT ADVANCES IN COMPUTER TECHNOLOGY

Edited by Paul Meissner

Computer Systems Engineering Division
Institute for Computer Sciences and Technology
Washington, D. C. 20234

December 1976

A Report of the Workshop on Estimation of Significant
Advances in Computer Technology
Held at the National Bureau of Standards
August 30-31, 1976

Edward Lohse, Chairman

U.S. DEPARTMENT OF COMMERCE, Elliot L. Richardson, *Secretary*
Edward O. Vetter, *Under Secretary*
Dr. Betsy Ancker-Johnson, *Assistant Secretary for Science and Technology*
NATIONAL BUREAU OF STANDARDS, Ernest Ambler, *Acting Director*

1976 WORKSHOP ON ESTIMATION OF SIGNIFICANT ADVANCES IN COMPUTER TECHNOLOGY

EXECUTIVE SUMMARY

The Institute for Computer Sciences and Technology has conducted a Workshop on Estimation of Significant Advances in Computer Technology. This Workshop was held at the National Bureau of Standards on August 30 - 31, 1976, and was attended by 20 representatives from industry, research organizations, universities, and other Government agencies, together with a number of ICST staff members.

The Workshop was intended to provide ICST with current scientific and technical information on advances in computer technology which could significantly impact the Federal Government's knowledge and use of computer technology developments in relation to computer security and export administration.

In order to focus the attention of the Workshop, a specific problem was chosen, namely the design of a large-scale digital machine which could be used for recovering the key used for encrypting data under the proposed NBS Data Encryption Standard (DES).

Presentations were made on the anticipated advances in computer architecture and in semiconductor technology. It was indicated that the present trends in component density for LSI, which has been increasing exponentially since the late 1960's, will continue in the same manner for at least the next five years. The density for logic circuitry is expected to grow from about 3000 gates per chip in 1975 to about 250,000 gates per chip in 1981; in memory chips the density will increase from about 25,000 bits per chip to about 1,000,000 bits per chip. The speed of logic circuitry has been increasing by about 1.5 megahertz per year for some ten years, which a speed of 30 megahertz being achievable at the present time. Speed-power ratios have been improving by a factor of 10 about every four years and a similar improvement appears likely in the next four years. The highest performance appears to be attainable with complementary metal-oxide-semiconductor, silicon-on-sapphire (CMOS-SOS) technology. This technology offers a speed-power product of one to two picojoules and a speed of 30 megahertz, and is expected to be reasonably available by 1981.

Semiconductor sources are presently concentrating on achieving high density at low cost, with less emphasis on extending high speed performance at the upper limits. Large production volumes are required in order to realize the most favorably prices, and this volume requirement is a barrier to many low-volume applications, including those of the military. A single order for one million chips would not be considered large.

Several designs were formulated for key-extraction machines for the data encrypted under the DES, and estimates were developed for the speed, size, development time, cost, and other factors. It is significant to note that while the technological factors for such a development are separately available (such as high density, high speed, low power, and low cost) these factors are not presently attainable in combined form as would be required for a successful key extraction machine. Rather, the various factors tend to be mutually exclusive, and extensive development effort and time will be required before all the factors become realizable in any one production device. To achieve a key exhaustion time on the order of one day, it was estimated that the cost would be several tens of millions of dollars, and that such a machine could not be placed in operation before 1990.

TABLE OF CONTENTS

APPENDICES

REPORT OF THE 1976 WORKSHOP ON ESTIMATION OF SIGNIFICANT ADVANCES IN COMPUTER TECHNOLOGY

1. Introduction

The Institute for Computer Sciences and Technology (ICST) of the National Bureau of Standards has responsibility under its basic charter, Public Law 89-306, to develop mandatory Federal Information Processing Standards, provide technical assistance and advice to Federal departments and agencies and conduct necessary research in computer sciences and technology. These objectives are accomplished through a comprehensive technical program that stresses high-priority national computer problems and issues. Specifically, ICST is responsible for monitoring advances in computer science and technology, assessing their technologically-derived impact and striving to promote their application and acceptance within the Federal Government.

1.1 Purpose of the Workshop

This Workshop was conducted at the National Bureau of Standards (NBS), Gaithersburg, Maryland, on August 30-31, 1976, to provide ICST with current scientific and technical information on advances in computer technology which could significantly impact the Federal Government's knowledge and use of these advances in relation to computer security and export administration.

The focus of the Workshop was on advances in the design, architecture and manufacturing of computer systems and related equipment which could be identified or estimated as characterizing the present state-of-the-art and the predictable future.

1.1.1 Computer Security

The subject areas of personal privacy, data confidentiality, and computer security are of the greatest National interest. The Privacy Act of 1974 (5 U.S.C. 552a) imposes numerous requirements upon Federal agencies to prevent the misuse of information about individuals and assure its integrity and security. ICST has been assigned certain responsibilities in the development of standards and guidelines for use by the Federal agencies in implementing the requirements of the Privacy Act and in complying with requirements for computer security and data integrity.

1.1.2 Export Administration

ICST has significant responsibilities in the area of export control to maintain an awareness of current and projected computer technology, production capability, and usage. This knowledge and expertise is made available for use within the Federal Government in the determination of export control criteria and parameters for various classes of ADP equipment.

1.2 Topic Selected as Computer Technology Vehicle

In order to achieve the objectives of the Workshop, a specific topic was addressed as a useful vehicle for examining current and projected capabilities for the design and manufacture of computer systems and related hardware. Consideration of this topic also provided direct and immediate assistance to NBS in the development of standards and guidelines, especially those related to computer security.

The selected topic was representative of a class of problems whose performance was not assumed to be constrained by traditional computer architectures and techniques. The topic involved the design and fabrication of a system to recover the key used to encrypt data under the NBS-proposed Data Encryption Standard (DES). (See Appendix B.)

1.3 Expected Significance of Results

ICST will use the information from the Workshop to (1) estimate the computer resources necessary to recover a key used in any particular instance by the proposed DES, (2) model advanced computer systems for which computer security safeguards must be emplaced to prevent computer fraud and to meet legislated privacy requirements, and (3) assess the potential technical significance associated with the export of computer-related products and technology.

1.3.1 Workshop Report

The product of the Workshop is this report containing technical information developed by the participants with regard to the topics considered. This report will serve as a significant element in the formulation of recommendations by NBS for use within the Executive Branch, and for submission to the Congress and to public groups for needed action pertaining to the subject areas of the Workshop. The report is intended as a factual summary of the Workshop for information purposes.

1.4 Organization of the Workshop

Technical experts representing a cross-section of the computer industry were brought together for the Workshop, representing the areas of semiconductor manufacturing, logic design, system architecture, and system fabrication. In preparation for the Workshop, announcements were sent to relevant associations and professional groups with the request that they identify suitable individuals who should be encouraged to attend the Workshop. The individuals so identified included representatives from industry, research laboratories, universities, consulting firms, and Government agencies. In addition, the Workshop was publicly announced to notify individuals wishing to contribute to the objectives of the Workshop. Several members of the ICST staff were present in order to contribute to the Workshop and to benefit from the available information. The Workshop was chaired by Mr. Edward Lohse, Director of Engineering - Operations, of the Burroughs Corporation.

1.5 Opening Remarks

Workshop participants were welcomed by the conference chairman. Mr. Lohse described the purpose of the Workshop and identified the topic selected as a vehicle for exploring advances in computer technology, namely the design of a machine for extracting the key used in encrypting data under the NBS-proposed Data Encryption Standard.

In opening remarks, Dr. Ruth M. Davis, Director of ICST outlined the responsibilities of ICST and the expectations for the Workshop. Mr. John Diebold was identified as Honorary Chairman for this Workshop and a second workshop to be held on the mathematical aspects of the proposed encryption algorithm. Dr. Davis identified three of the main responsibilities of ICST as (1) keeping abreast of advances in computer technology, (2) furnishing advice and guidance to the Federal Government on the effective management and utilization of ADP, and (3) performing gap-filling research and development on the basis of recognized needs.

The process of establishing standards was depicted as becoming more intricate as the art of data processing advances and relationships become more complex; this is particularly evident in the area of interface standards. ICST was identified as the champion of sometimes unpopular (but important!) causes, having a special regard for the often-overlooked and lonely user. Current efforts to develop communications protocols for the library community were mentioned. The development of safeguards for computer systems was described, the intent being to lower the vulnerability to risks to the same extent that the utility has been increased.

Dr. Davis expressed the hope that this Workshop might identify the limits which will be encountered by our present computer technology so developers might proceed consciously toward these limits rather than stumbling across them.

In the export area, ICST attempts to serve as a mediator between the business community and the security community. ADP is currently distinguished by exhibiting an increasing rate of increase in the international balance of trade.

Commenting on the scenario selected for the Workshop, Dr. Davis pointed out that the selected topic involved a standard of general interest, and that it provided a view toward the future. It also involved a problem having no analytic solution.

Dr. Davis announced that the second Workshop in this two-part series would deal with mathematical and statistical aspects of the selected topic and would be chaired by Mr. Julian Bigelow of the Institute for Advanced Study, Princeton, N.J.

2. Description of Topic Serving as Technology Case Study for the Workshop

The topic selected as a vehicle for consideration by the Workshop, namely a machine to extract the key used for encipering messages under the NBS-proposed Data Encryption Standard (DES), was put forth by Dr. Dennis Branstad of ICST. After describing the DES enciphering algorithm, he outlined the "worst-case" conditions for deriving a key using the known-plaintext threat. In this situation, it is assumed that an adversary has sufficient matching plaintext and cipertext, encrypted under a fixed, but unknown, key. He then presented an algorithm for extracting the key by exhaustion, first using a single machine, figure 1, and then using a parallel array of machines, figure 2. In the first case, figure 1, a block of plain text and a corresponding block of encrypted text are entered into an encryption test unit. The unit then encrypts the plain text under one key after another, each time comparing the result with the encrypted text input. If a match is obtained, the current value of the key is considered to be the desired answer and is printed out. If a match is not obtained, the value of the key is advanced by one and the process is repeated. The process would continue, if necessary, until all 2^{56} values had been tested. In the case of the parallel machine, figure 2, a set of encryption test units would be employed, each functioning in the manner described above. Each unit would be assigned a portion of the key space over which to perform its testing. The machine would be supplied with a pair of blocks, one being plain text and the other being the encrypted version. The machine would operate until a match was obtained, or until the entire key space (2^{56} values) was exhausted. By having n units operating in parallel, the search time can be reduced by a factor of n.

As to whether the correct key could always be extracted on the basis of a single pair of blocks, it was pointed out that the correctness of a tentative key could be quickly ascertained simply by testing it with another pair of blocks.

It was proposed that the Workshop participants use their specialized knowledge to devise implementations embodying this extraction algorithm, making maximum use of the advanced technology expected to be available as far into the future as this could reasonably be projected. Factors of interest would be the architectures of such machines, the type of circuitry, speed of operation, reliability and maintainability, size, power, and cooling requirements.

Dr. Branstad was followed by Dana Grubb of ICST who reviewed the NBS implementation of the DES using small and medium scale integration and TTL logic, in order to acquaint the participants with the computational details and circuit considerations (see Figure 3). The NBS implementation, designed for performing practical tests rather than maximum speed, performs the algorithm in 8 microseconds and requires an additional 26 microseconds to load and unload data, which is done in eight 8-bit bytes. The basic operations are performed with 181 ICs; additional test logic bring this to 205 ICs, representing about 5000 gates. PROMs are used to implement the functions of the S-boxes. The encryption time for the NBS equipment could be reduced to about 3.4 microseconds using special shift registers. The use of Schottky TTL could bring this down to about 1.7 microseconds. In answer to a question, the speed of MECL 10K logic was stated to be about 5 nanoseconds per stage and that of Schottky TTL as about 3 nanoseconds. As a point of reference, the time to exhaust all possible keys (2^{56}) with the NBS equipment would by about 17,000 years.

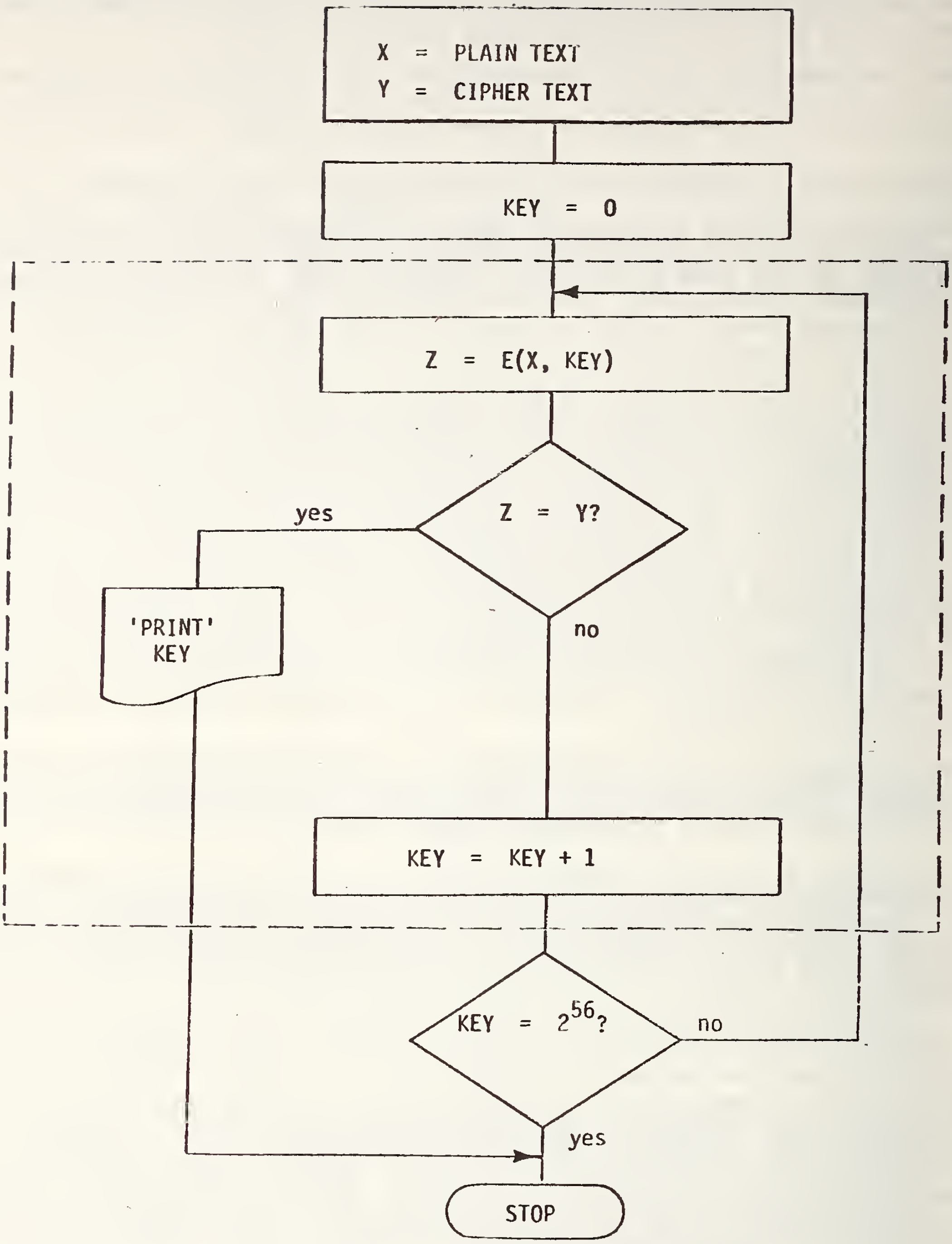


FIGURE 1. KEY EXTRACTION ALGORITHM

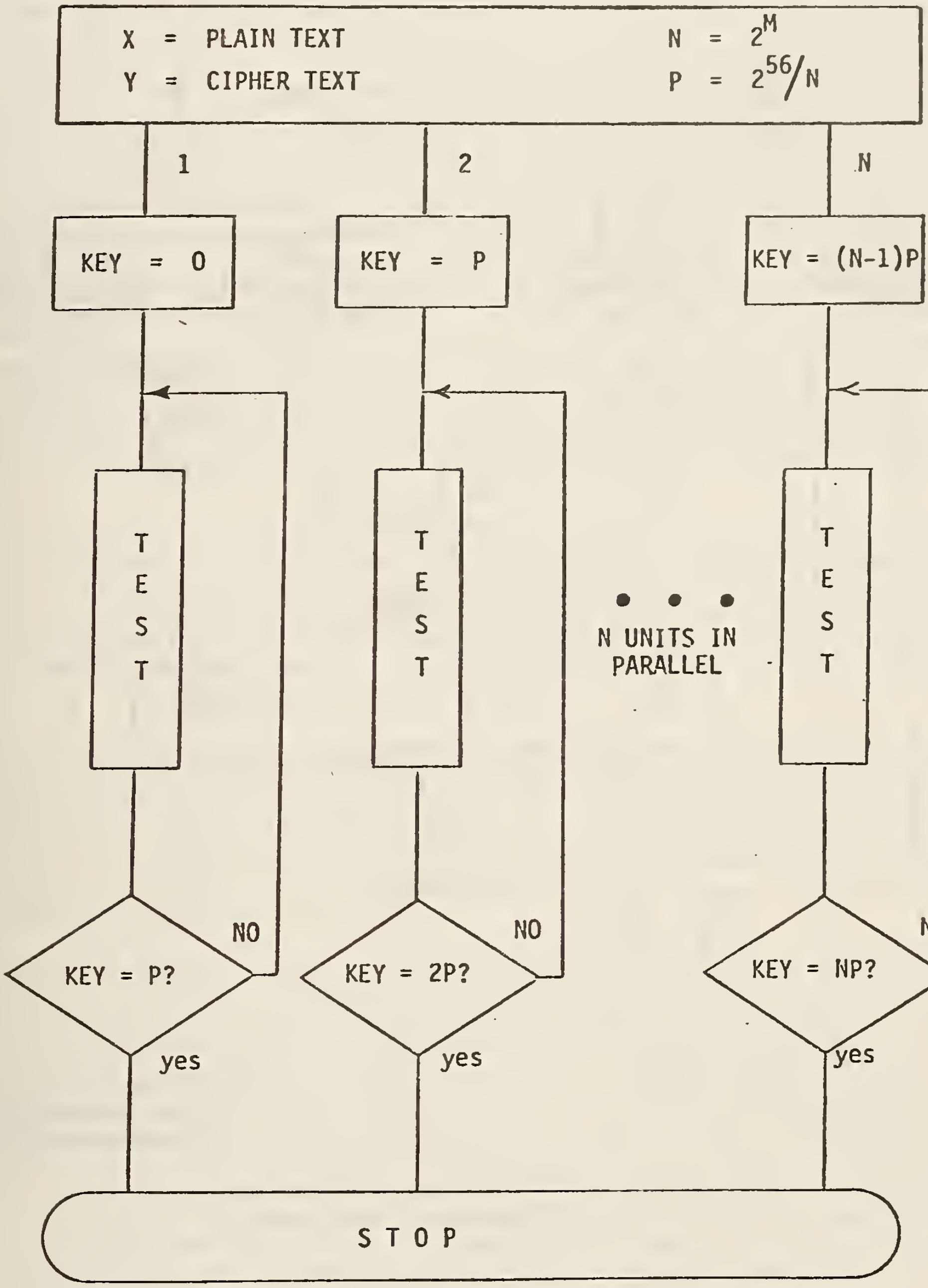


FIGURE 2. PARALLEL VERSION OF KEY EXTRACTION ALGORITHM

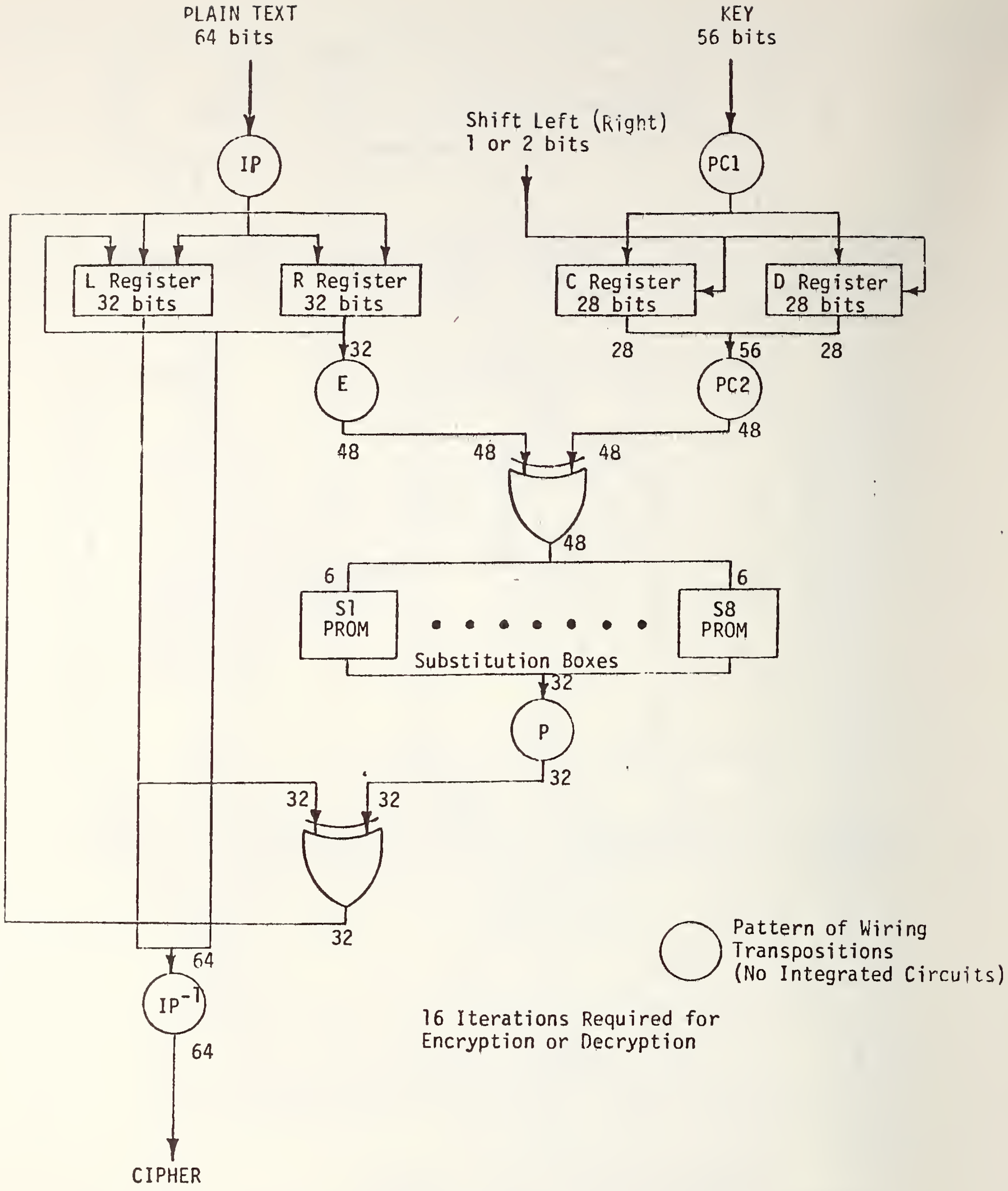


Figure 3. Schematic Diagram of NBS Integrated Circuit Version of DES Encryption Algorithm

3. Summaries of Current and Projected Computer Technology

3.1 Computer Architecture

An overview of computer architecture was presented by Mr. Jack Lynch, Director of Advanced Development of the Burroughs Corporation. He illustrated the dramatic growth in component density of LSI logic chips using the chart shown in figure 4. At the present time, the CPU for a small business computer could be completely fabricated on a single chip (about 3000 logic gates). According to the projection, one of the largest CPUs could be fabricated on a chip by 1981 (about 250,000 logic gates.) Mr. Lynch pointed out that a logic gate is comprised of several devices, typically about 10. The high-yield chips involved are about 200 by 200 mils, or about 1/2 cm by 1/2 cm. This poses an interesting question for management: what would be the source of corporate income when the largest machine they make can be fitted onto a $10 chip? The answer is felt to lie in the development of comprehensive business systems designed to enable businesses to increase the efficiency of tneir overall operations.

Growth in density of memory chips is illustrated by the chart shown in figure 5. In 1975 the density was about 25,000 bits per chip; it is estimated that this will become about one million bits per chip by 1981. Such densities, while theoretically possible, will require additional research in techniques such as electron-beam lithography in order to be realized.

Mr. Bigelow asked about the connectivity problem as more components are squeezed onto a chip. Mr. Lynch responded that this did not appear to be an insurmountable problem and offered as evidence the fact that intricate products are currently being fabricated successfully. Mr. Bigelow further asked how many layers of metal could be emplaced for achieving interconnections. This question was answered by Mr. Hillis of Motorola who stated that two layers were generally available in production, but these could be supplemented by using elements as interconnections.

Initial impetus for LSI development was attributed to the military which provided the resources at first; later on, the commercial and business interests became involved. The comment was made that the volumes required for economic production are becoming so great that potential small users including the Military are being shut out to an increasing degree. Mr. Hillis commented that semiconductor sources are emphasizing low-cost devices, while the drive for higher-speed logic families is losing steam. The commercial thrust is on achieving high density at low cost.

Mr. lynch presented a chart prepared by Booz, Allen & Hamilton showing the distribution of costs incurred by U.S. businesses on information resources, figure 6. Costs for 1975 are shown as $150 billion and are estimated to grow to $350 billion in 1985. From the standpoint of the outside supplier, the greatest potential is in the areas of telecommunications and word processing which greatly outweigh the outlays for EDP. The solution to large-scale business systems, according to Mr. Lynch, involves partitioning the systems into manageable segments. This has three aspects: how to achieve the partitioning, how to implement the segments, and how to create an Operating System which can coordinate the operation of the segments and "avoid chaos". The solution is felt to lie in the use of networks of processors whose operation is properly coordinated. The major unsolved problem is felt to be in the area of software management and the survivability of systems. He conjectured that the necessary techniques might first emerge in dealing with large structured problems such as weather analysis for which large processing arrays were assembled.

As to the role of fiber optics, it was stated that these are being more actively pursued for use in communications, rather than in computers.

3.2 Semiconductor Technology

An overview of semiconductor technology was presented by Mr. Howard Wright of Collins Radio Company. He alluded to the fact that Collins is working on implementations of the DES but placed those efforts outside the scope of his presentation to the Workshop. He expressed the view that density increases of 4 to 1 should not be difficult to achieve. Among the promising new technologies is VLSI (Very Large Scale Integration). He felt that

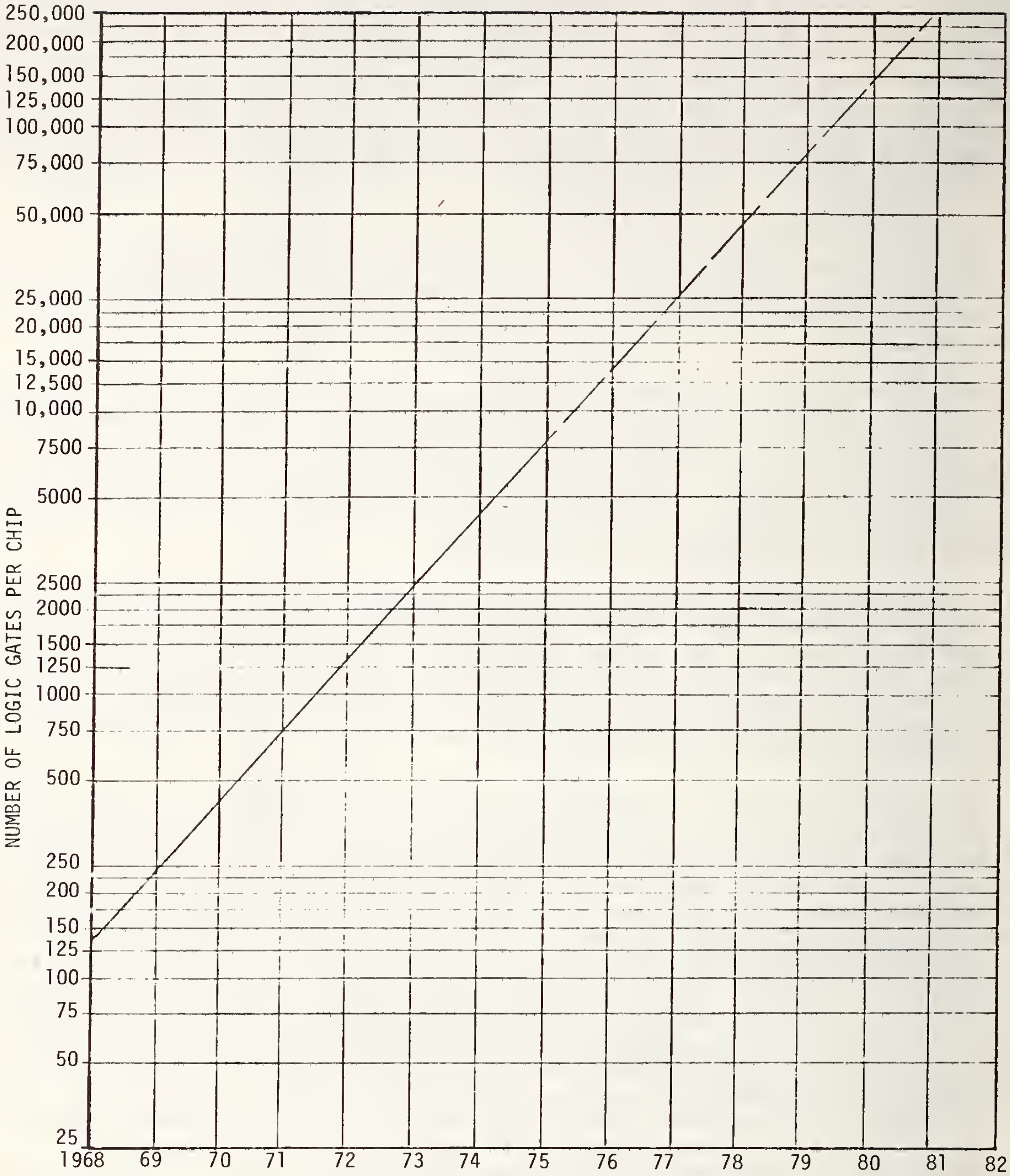


FIGURE 4. NUMBER OF LOGIC GATES PER CHIP AS A FUNCTION OF TIME.
(CHIP COST IN $10 RANGE FOR MASS-PRODUCED CHIPS.)

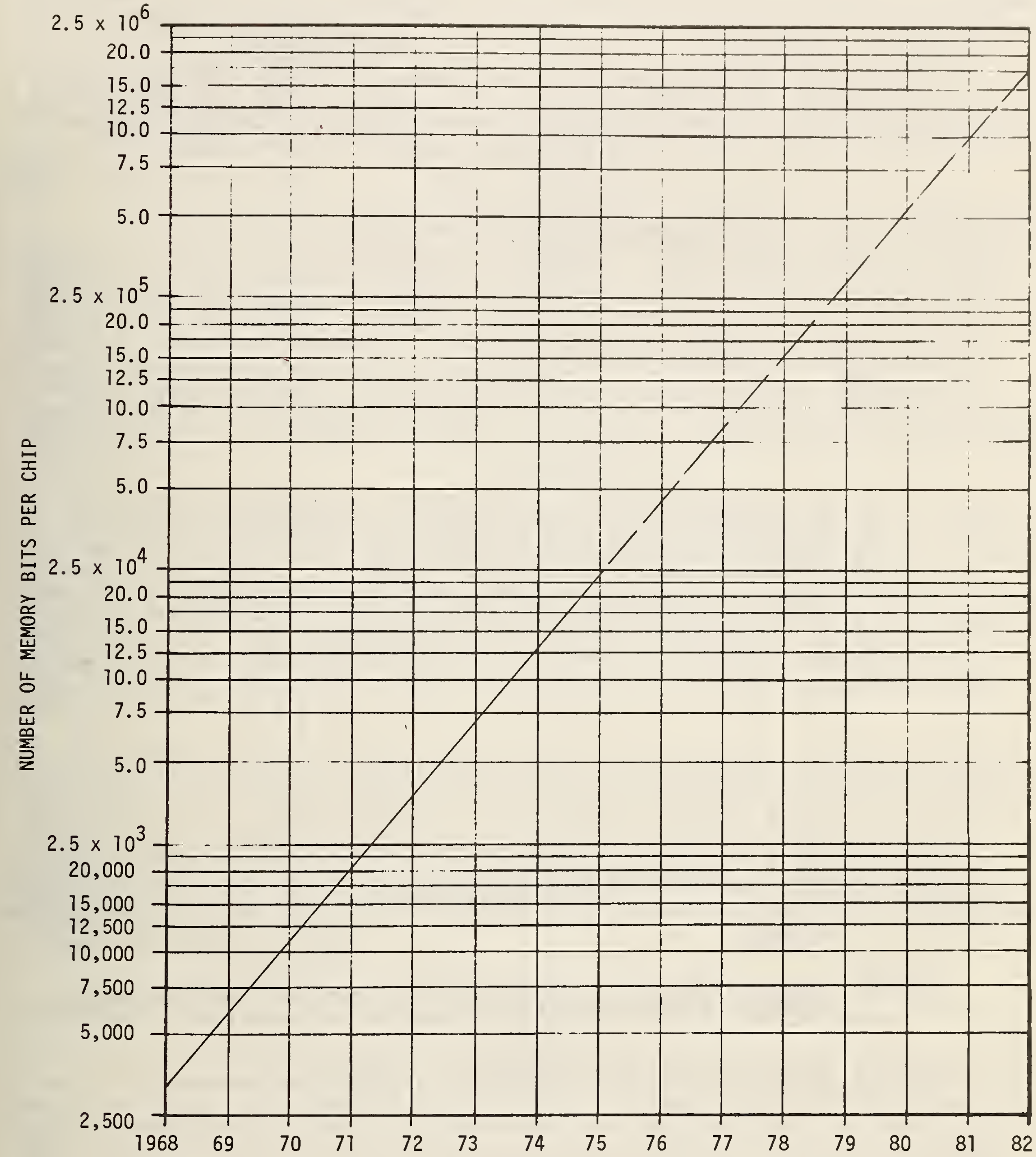
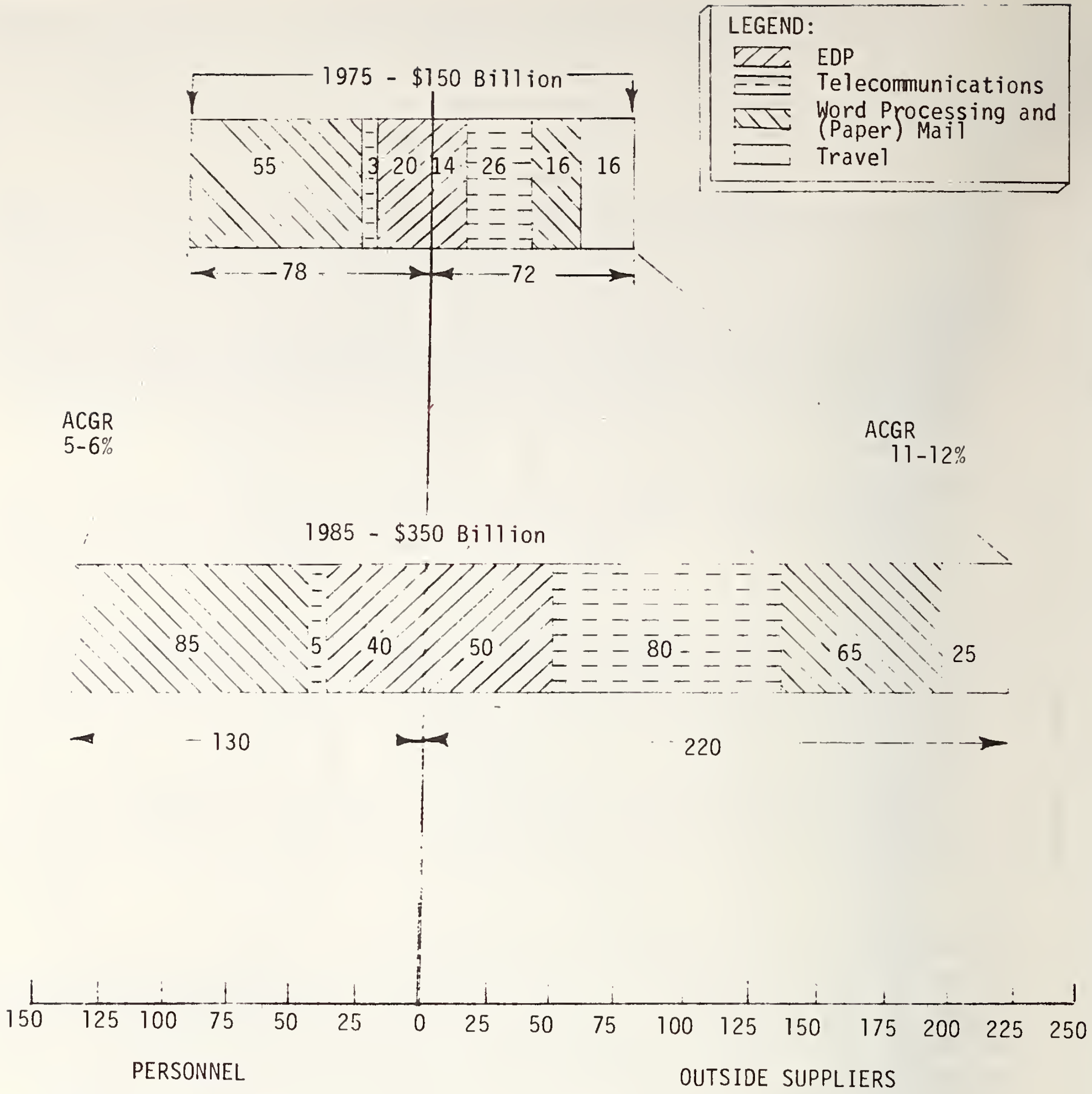


Figure 5. Number of Memory Bits per Chip as a Function of Time. (Chip Cost in $10 Range for Mass-Produced Chips.)



SOURCES: Booz, Allen & Hamilton, annual reports of major suppliers, FCC reports, Department of Labor (Assuming 5% annual rate of inflation).

Figure 6. Expenditures by U. S. Organizations on Information Resources

energy density would be kept at present levels by reducing voltages as devices get smaller. Speed increases of about 1.5 megahertz per year have prevailed over about a 10-year period, and he felt that this trend would continue. Speeds of about 30 megahertz, he said, are achievable today. He noted that the speed of a system must be held down to about 1/2 or 1/3 of the maximum speed of the devices, to allow for statistical variations and safe operating margins under worst-case conditions. Power consumption is decreasing; this tends to keep heating problems within bounds, and has also made battery operation more feasible. Complementary Metal-Oxide-Semiconductor (CMOS) circuitry offers very low power levels in the standby mode.

Reliability tends to decrease as density goes up, but this is offset by improvements in design. Mr. Wright felt that the emphasis for the Workshop was more properly on maximum performance, rather than maximum density or low power. CMOS circuitry using Silicon-on-Sapphire (SOS) was suggested as probably offering the highest performance if other factors are considered less important. A chart was presented comparing several of the current MOS/LSI processes, figure 7. CMOS-SOS offers a speed of 30 megahertz, which is several times that of the other processes. It has a very low power consumption for its speed, namely a speed-power product of 1 to 2 pico-joules, as compared to 8 to 20 for the other processes. It is presently the most expensive of the current processes, being some 6 times as much as the least expensive process. Mr. Wright pointed out that a new undertaking has associated with it a higher risk factor, and that this further increases the price, at least initially.

Reliability figures were given for various grades of production devices, see figure 8. A military grade chip containing perhaps 500 transistors might be expected to exhibit a reliability of 0.01% failures per 1000 hours, after undergoing a burn-in period. A good grade chip, also burned in, might have a reliability of about 0.03% per 1000 hours. Commercial grade chips, containing 6000 or more transistors, and without burn-in, might be about 0.3% per 1000 hours. These figures refer to hard (permanent) failures. The comment was offered by Mr. Lynch that there may be 20 to 30 soft failures per hard failure. A soft failure may be anything from a momentary transient to a prolonged intermittent condition. For this reason, critical applications should incorporate failure detection and automatic restart provisions.

In answer to a question by Mr. Bigelow as to how the failure rate varies with time, it was stated that there is a higher infant mortality rate, after which a stable rate prevails. Mr. Hillis noted that the failure rates vary significantly, depending upon the type of circuitry, as for example whether it is dynamic or static, ROMs or RAMs. Dr. Pirtle offered the observation that if ICs were viewed as analog devices rather than digital devices, a great deal more variation would be noted. In practice, digital circuits are exposed to substantial variations arising from a variety of factors. Mr. Hillis observed that while the refresh times for dynamic memory elements theoretically could be in the range of seconds, they were customarily refreshed in milliseconds to achieve a wide margin for reliable operation.

Semiconductor advancement is currently emphasizing higher density, lower cost, higher speed, lower power, and increased reliability, as illustrated in figure 9.

Mr. Bigelow asked what would be considered a good initial quantity to start with for a new item. According to Mr. Wright, this could be 1000 parts if the purchaser would pay all of the start-up costs. Mr. Hillis offered the comment that this could be influenced by the potential to the vendor for additional sales of the same product. In answer to a question by Mr. Lohse on start-up times, it was stated that a new product or a new source for a product would take a period of time, but not as long as was required for the initial effort.

With regard to the achievement of higher densities, Mr. McDonald of Bell Telephone Laboratories stated that various problems might be encountered as wire paths become exceedingly small, one of these being metal migration. He referred to work being done by IBM in this area and referenced a paper by Keyes.*

*"Physical Limits in Digital Electronics," Robert W. Keyes, Proc. IEEE, May 1975, Vol. 63, No. 5, pp. 740-767.

PROCESS	Relative Size	Speed MHZ	Relative Complexity to Fabricate	PWR x Delay Pico-Joule	Order of Cost	Maturity Years
P-MOS, METAL GATE, LOW V_T, I^2	1.0	1.5	1.0	20	1	4
P-MOS, DEPLETION	.62	1.5	1.2	16	2	3
P-MOS, SILICON GATE, DEPLETION	.43	2.0	1.4	14	3	2½
N-MOS, Silicon Gate	.45	5.0	1.4	12	4	3
CMOS BULK	2.0	5.0	2.0	8	4	3
CMOS SOS	1.4	30.0	1.5	1-2	6	1
I^2 L	.45	8.0	1.5	8	5	1
VLSI (Very Large Scale Integration)	¼(same)	Same	Same	Same	Large	In develooment

FIGURE 7. COMPARISON OF CURRENT MOS/LSI PROCESSES

	FAILURE RATE
● MILITARY GRADE	0.01% / 1000 HRS
● GOOD GRADE	0.03% / 1000 HRS
● COMMERCIAL GRADE	0.3% / 1000 HRS

FIGURE 8. RELIABILITY LEVELS FOR VARIOUS GRADES OF LSI CHIPS

- HIGHER DENSITY
- LOWER COST
- HIGHER SPEED
- LOWER POWER
- INCREASE RELIABILITY

FIGURE 9. DIRECTION OF SEMICONDUCTOR TECHNOLOGY ADVANCEMENT

Regarding density, it was stated that interconnections can cut the density in half, while with silicon there may be a further reduction of 20%.

Mr. Hillis directed attention to an article in the February issue of Computer Design, "Trends in Computer Hardware Technology," by David A. Hodges (pp. 77-85), which he felt represented an accurate summary of present and emerging technology. Mr. Hillis particularly noted the dramatic price discontinuity on the chart depicting costs per million instructions per second (MIPS) versus time, in the case of a 3-MIPS microprocessor. This component was displaced below the curve by orders of magnitude, indicating the radical price drop achievable through LSI with high-volume production.

4. Technology Aspects of Exhaustive Key Recovery

4.1 Suggested Design for a Key Extraction Machine

The Workshop was addressed by Mr. Whitfield Diffie of Stanford University who distributed a paper entitled, "Cryptanalysis of the NBS Data Encryption Standard," coauthored by Mr. Diffie and Dr. Martin E. Hellman of the Department of Electrical Engineering, Stanford University. The paper advances the hypothesis that a machine could be built using current technology for extracting keys used with the DES by exhaustion in an average of 10 hours of computation time (20 hours maximum) and that the prorated cost per key extracted would be about $5,000 with a machine whose cost is $20 million. Of greater concern is that the decreasing cost of computation would bring the cost per solution down to perhaps $50 within 10 years. Mr. Diffie stressed that the primary focus of the paper was on the speed and cost of the suggested machine.

Mr. Diffie then reviewed a series of questions which had been posed when they first raised the possibility of building the suggested key extraction machine.

With regard to the design and control costs for such a machine, Mr. Diffie pointed out that it is not comparable in difficulty to large parallel array-type machines with multiple connections among computing elements. It uses a simple tree structure and each element need only communicate upward to its supervisory element; no sideways paths are involved. Thus, the control problems and design complexity do not escalate with size.

As to reliability, the computational elements would operate essentially independently, so that continued machine operation is not dependent on all elements working continuously. While the probability of one or more elements failing per day may be high, it is necessary to factor in the probability that the failed element(s) also happen to be assigned the desired key. The joint probability thus becomes exceedingly small. Provision was made in the suggested design for self-testing circuitry and spare components, and allowance was made in the time estimates for diagnostic and repair times. Mr. Bigelow commented that there could be other types of errors, such as the failure to enter the clear text correctly into all of the chips.

An objection to the suggested machine was that a single $10 chip could not be used to solve for the key, and that it would take 40 microseconds per key rather than 1 microsecond. As to the required computational speed, Mr. Diffie stated that CMOS-SOS would be capable of meeting this requirement. Mr. Diffie contrasted the design of a chip for their suggested machine with the NBS implementation of the algorithm. In the NBS equipment, most of the time is consumed in I/O operations, while these would be minimal in the suggested machine.

Mr. Diffie was asked whether he considered it possible to carry out a task of the magnitude involved in building the suggested machine in a clandestine manner. He responded that they were not so concerned with this aspect of the problem; they were more concerned with the fact that, for example, NSA would have the means to carry out such a task through its available channels. Mr. Hillis offered the opinion that RCA would be the only source that could provide such a quantity of SOS chips over a span of a year or two, and that such a capability would be perhaps 4 to 5 years away. Regarding the charts shown in earlier presentations, the comment was made that they apply only to everday applications and do not represent exotic devices (figs. 4 and 5).

In answer to a question by Mr. Lynch on the number of CMOS-SOS gates that would be needed, Dr. Diffie said that about 5000 would be required. To achieve the fast solution time, a 30 megahertz clock would be required, although there was some conjecture that this speed might have to be doubled.

As to the size of the suggested machine, they had used an estimate on the order of 10,000 chips per cabinet, and 1,000,000-chip machine would require 100 cabinets. Power consumption was estimated at 400 kw, which, while large, would not be insurmountable. Mr. Diffie asked the participants whether they might know of comparable-sized machines. Mr. McDonald suggested that it would be 250 times the size of a large computer memory. Power consumption of the STAR computer was stated to be 250 kw. The Illiac IV was described as occupying 8 cabinets and drawing 250 kw.

Mr. Diffie noted that for purposes of extracting the key, the initial permutations would not be significant, since the transformed version of the key would be the new key for the solution. He suggested the use of read-only memory for the S-boxes. Dr. Pirtle noted that the main source of delay was in the memory references, since all other processing was simply logic gating.

Mr. Diffie saw another threat in that at some point in time a machine capable of breaking the algorithm might become available as the result of some legitimate endeavor, such as a large-scale array processor. This might then be diverted to the task of code breaking. While he saw this as unlikely in the next 10 years, he felt that such a machine might certainly become available in less than 25 years and this possibility should be a source of concern.

Mr. Diffie posed the question as to what might be expected to become available in terms of standard (or slightly modifiable) chips that might be used in a key-extraction machine, or in terms of parallel processors, considering their growth and the research using large arrays of processors.

Mr. Hillis pointed out that there is no such thing as easily producing a slightly modified version of an existing chip. Any modification is equivalent to starting over again.

4.2 Formation of Workshop Subgroups

In order to conduct more detailed explorations, the Workshop participants were divided into two subgroups, one on anticipated advances in technology and one on architectures for a key-extraction machine. The subgroup on technology was chaired by Mr. Weiselman and the subgroup on architecture was chaired by Mr. McDonald. These subgroups deliberated for the balance of Monday afternoon and Tuesday morning.

The Workshop reconvened at 11:00 a.m. on Tuesday, and summaries were presented by the respective subgroup chairmen.

4.2.1 Summary of Subgroup on Architectures for Key-Extraction Machine

The subgroup summary was presented by Mr. McDonald. Several candidate architectures were offered, together with estimates of cost, speed, development time, and probability of success. These are summarized below:

(1) Acquire large-scale, high-speed machine which could be modified for key extraction:

Buy a STAR computer, Est. Cost: $8-10 million, or buy a CRAY 1, Est. Cost $7 million.

Special hardware for functions not readily programmable:
Hardware cost: $400K
Development cost: $400K
System Integration: $1 million, plus 2 years.
Solution rate: 10-40 nanoseconds.
Maximum time to exhaust all possible keys: 23-91 years.
Start 1976, Finish 1978.

(2) Acquire future large machine:

Buy "SUPER STAR", Est. Cost $8-10 million.
Build special hardware and add special instructions.
Permutation hardware (2 sets)
Functions (2 sets) } Est. Cost: $2 million, plus 2 years.
Special instructions
Start 1981, Finish 1982.

(3) Build Pipelined Special Processor:

ECL logic, 20 nanosecond clock, 1000 chips for one solution unit.
Est. development cost: $1 million.
Solution rate: 20 nanoseconds, 50 keys per microsecond.
Exhaustion time for one solution unit: 46 years.
Build machine with 10 solution units:
Exhaustion time: 4.6 years
Est. cost: $1.6 million
Start 1976, Finish 1979.
Build 20 machines:
Exhaustion time: 3 months
Est. cost: $13.5 million
Start 1976, Finish 1982.
Estimated certainty: 60%.

(4) Employing exotic technology, e.g., Josephson junction:

50 picosecond clock
Solution rate: 1 nanosecond per solution per substrate.
1000 substrates.
Exhaustion time: 19.8 hours.
Est. cost to develop and fabricate: $50 million.
Start 1985, Finish 1990
Estimated certainty: 10%.

(5) Million-chip parallel machine:

One million chips:

Est. development cost: $1 million.
Est. cost per chip: $50.
Make and test 10^4 cards: $20 million.
System development cost: $2 million.
Production: 300 man years.
Size: 64 bays.
Total cost: $72 million.
Power: 3 megawatts; cooling power, 9 Mw., total 12 Mw.
Exhaustion time: 19.8 hours.
Start 1983, Finish 1990
Estimated certainty: 10-20%

(6) Special low-cost parallel machine (suggested by Mr. McDonald):

Fabricate cards with 70 T^{2}LS chips.
100 cards per bay, 10 bays = 1000 cards.
Solution time per card: 4 microseconds.
Effective solution time for complete machine: 4 nanoseconds per key.
Exhaustion time: 9.14 years.
Est. development cost: $2 million.
Est. total cost: $4 million.
Start 1977, Finish 1979.
Estimated certainty: 70%.

(Note: In 1980 - 1982, speed should be ten times as fast.)

Mr. McDonald offered some observations with regard to the above design. He visualized 1000 devices occupying some 10 bays of equipment at a total cost of about one million dollars and having a solution time of 4 microseconds. This would take about 9 years for exhaustion, which would be 4000 times longer than required. But the processing speed/power ratio has been increasing at the rate of about a factor of 10 every 4 years. At this rate, in about 8 years such a machine would have a solution time of about one month. He felt that with a little ingenuity this might rapidly be enhanced.

The various machine architectures are contrasted in the following chart, figure 10.

4.2.2 Summary of Subgroup on Technology

The subgroup summary was presented by Mr. Wieselman.

Implementation of DES chip using today's technology: NMOS Depletion Load, 50 nanosecond gate delay:

Solution time of 40 microseconds and
160 microseconds for two different manufacturers.

Typical cost figures for quantities, based on standard parts, not custom parts assuming about 4 years of production:

NMOS Technology:
0-100K chips per year, $100 per chip;
100K chips per year, $25 per chip;
1 million chips per year, $10 per chip (for 4 years of production).
Confidence level in the above figures is 80%.

Future technology, CMOS SOS:

1 microsecond solution time
In quantities of 1 million per year (for 4 years of production):
$50 - 100 per chip for high reliability grade;
$20 per chip for commercial grade.

Circa 1986:

High speed version: 1/2 microseconds solution time.
Gate delay 1 nanosecond.
3K-30K gates per chip.
3 Watts per chip (practical limit).
0.1 - 1.0 picojoule operating range.
Quantity price $10.
Confidence level in the above figures is 80%.

High density version:

Gate delay 10 nanoseconds.
100K gates per chip.
0.1 picojoule
Solution time 1/4 microsecond using pipeline approach.
Quantity price $50 - 100 per chip for high reliability grade;
$10 per chip for commercial grade.

Development costs, system costs, and cost of accompanying chips would have to be factored into the above figures.

Confidence level in the above figures is 30%.

By 1986, chip sizes would be larger. Greater reliability would be achieved through redundancy. Other technologies such as optics might be expected to appear.

4.3 General Comments

Dr. Pirtle noted that machines with instruction cycles of 20 nanoseconds exist today, and that a solution time of 4 microseconds would be very conservative for a high-speed processor. Some representative arithmetic times were quoted for reference purposes. A floating-point addition for two 32-bit operands was given as 20 nanoseconds. For two 64-bit operands the add time was twice as long, while the multiplication time was four times as long.

With regard to the number of chips that would be required for a key extraction machine, Mr. Hillis noted that an order for one million chips of a given design would not be considered exceptionally large. Memory chip production is several million per year. The Rockwell calculator chips are being produced at the rate of 2 to 3 million per month. An order for one million chips for a key extraction machine would probably result in a cost closer to $100 than $10. In order to achieve a lower price, one would have to consider a non-American, captive source under control of an adversary. The necessary technology would be a further requirement, and this would take some period of time to achieve.

Mr. Hillis stated that the life cycle of commercial chips is about 5 years. He pointed out that it takes a production of about 1 million chips to stabilize the yield, and that the price can be reduced 20% for the second million. For a large order, a customer would probably not go to a sole source, and this could double the cost.

Mr. McDonald wondered whether it might be possible to use arrays of commercial DES chips for building a key extraction machine. He noted, however, that the commercial chips would probably be rather low speed in performance, since they are intended mainly for communications applications, with the data transfer rates being limited by the line speeds. The emphasis in the commercial DES chips will be on moderate speed at low cost.

Mr. Thorpe offered the marketing observation that implementations embodying a component are turning out to add more to the cost of the product than the cost of the component itself.

The comment was offered that encryption procedures could quickly be changed and this would obsolete a key-extraction machine.

5. Computer Security Requirements and the DES

For the purposes of the Workshop, the DES was selected as a vehicle for exploring significant advances in computer technology, as described in the preceding sections of this report.

Numerous comments arose during the Workshop regarding the proposed DES as related to computer security requirements, and these comments are summarized in this section.

With regard to the lifetime of the data to be protected by the DES, Mr. Lohse commented that some records would be encrypted for permanent storage, while others would be encrypted only for transmission. Consideration was given to the question of what would constitute a good time frame for the life of the standard. Mr. Secretan of Collins pointed out that the technology is changing too fast to enable projections to be made for more than a few years into the future.

Mr. Maczko of the Incoterm Corporation observed that there seems to be a range of values to be protected, yet the Workshop appeared to be looking at a single solution to protect all values.

The feeling was expressed among the participants that the DES could be used in various ways to achieve higher levels of security; however, the question was raised as to whether this would fall within the definition of this standard.

With regard to the purpose of the Workshop, Mr. Diffie offered the opinion that the interests of the organizers might not correspond to the interests of the participants. He felt it would be helpful to consider what would properly constitute a good standard.

SYSTEM	START	FINISH	COST ($ MILLIONS)	KEY EXHAUSTION TIME	SUCCESS PROBABILITY
MODIFIED STAR COMPUTER	1976	1978	9-11	23-91 YRS	--
MODIFIED PROJECTED SUPERCOMPUTER	1981	1982	10-12	5-12 YRS	0.6-0.7
PARALLEL MSI	1977	1979	4	9 YRS	0.7
PIPELINE ECL	1976	1982	13.5	3 MONTHS	0.6
JOSEPHSON JUNCTION	1985	1990	50	1 DAY	0.1-0.2
PARALLEL LSI	1983	1990	72	1 DAY	0.1-0.2

Figure 10. Summary of Characteristics of Key Extraction Machines Using Various Architectures

Mr. Bright expressed confidence in the DES as a component, but added that a component by itself isn't an encryption system. He offered the opinion that the standard should be suggestive rather than restrictive for maximum usefulness. He recalled that with the 64-bit key there had originally been discussion over the 8 bits which were not used in the encryption process.

Mr. Diffie saw the DES chip as a good component, as far as it goes, but not as a finished product, that is, additional measures should be used to achieve greater security. One technique would be the use of multiple encryption, and he felt that the proposed standard should include such provisions. There was some debate as to how the strength of the algorithm might increase under multiple encryptions. In some systems, encryption under multiple keys is simply equivalent to encryption under some other single key, though this was not felt to be the case with the DES.

Mr. McDonald noted that the existence of a component for performing encryption would strongly influence any actual system. He added that the software people have expressed a desire for "more handles". Mr. James Nelson of Univac expressed the need for an algorithm that was capable of enhancement, but that systems shouldn't be burdened with more than the applications could support.

Mr. Lohse cited the SWIFT monetary transfer in which link encryption is used together with end-to-end message authentication. Protection is achieved through key management plus an algorithm plus management of personnel plus the protection of records. There is a need to keep the various aspects in balance. He visualizes a spectrum of protection as being achievable with the DES. It was pointed out that the Gretag equipment used in SWIFT employs a 2000-bit key.

In their paper, "Cryptanalysis of the NBS Data Encryption Standard", Dr. Hellman and Mr. Diffie argue that an algorithm having a longer key should be used, in the range of 128 to 256 bits. The paper further argues that a key of this length would not unduly complicate the design of the algorithm nor encumber the user, yet it could increase the security beyond any foreseeable possibility of key extraction by exhaustion. Mr. Diffie was questioned as to how the DES might be expanded to use a key of, say, 112 bits. He pointed out that 768 bits are involved in the 16 rounds which are carried out by the algorithm, and that these iterations would provide an opportunity to introduce additional key bits, rather than depending only on the original 56 bits.

With regard to the use of a longer key, Mr. Diffie pointed out that only about 20% of the gates required to implement the DES are key-dependent. Most of the gates are in the substitution boxes, and these could be implemented with a PROM. There was some debate as to whether the algorithm could be partitioned without requiring excessive pin connections; it would also cost more to implement if it required more than one chip. The Collins representatives noted that the present algorithm is close to the maximum that could be implemented on a chip with present technology; a more complex algorithm might not be realizable for perhaps another two years. Mr. Hillis supported the view that the present key length is about the limit for produceability and that a delay of one to two years might be encountered if a longer key were required.

Mr. Diffie felt that the speed of encryption using a 128-bit key could be comparable to that for the 64-bit key by using more parallelism, but this point was debated. Mr. Bigelow expressed the intuitive feeling that the computation time would necessarily have to be increased for a larger key, in order to realize a more rigorous encryption. He felt that it would not be possible to get adequate mixing by means of parallel processes; at some point it would be necessary to employ serial processes to achieve this.

One way of obtaining greater security with a shorter key is simply to change the key more frequently, but it was pointed out that it is not always convenient to do this. Mr. Hillis wondered whether a satisfactory solution might be to change the key more frequently in proportion to the value of the information being protected. Mr. Diffie called attention to the fact that key generation is fundamental to the encryption process and must be comparably rigorous.

With regard to the utilization of the key bits, it was noted that the DES uses the bits quite uniformly. Each of the 56 bits in the key used by the algorithm is used from 12 to 15 times during the 16 rounds.

Mr. Bright noted that the NBS effort is oriented toward hardware. However, he has produced a software version which is available on the NBS 1108. He quoted figures for software execution of the algorithm for a 370/155 and an 1108. These were about 7 milliseconds after the key schedule was generated.

Mr. Bright made the observation that the ADP marketplace is seeing for the first time products (i.e., encryption devices employing non-DES algorithms) which are unknown in functions (and dubious, he added). He characterized these as "snake oil" or "unlabelled merchandise" and claimed that with other products from EDP suppliers the customers at least know what they've got. He wondered whether others at the Workshop shared his concern. Mr. Jeffery noted that when a customer purchases a UART* he doesn't ask what is inside. Mr. Bright expressed concern about a product for which the typical customer would have no way to measure the effectiveness of what he was getting.

Mr. Lohse observed that the DES would be an improvement over the unknown, and often chaotic, situation which is present in the market today.

6. Concluding Discussion

Upon completion of the summaries presented by the subgroup chairmen, Ed Lohse called upon the Workshop participants for comments. Mr. Bigelow requested that confidence levels be assigned to the projected figures given in the summaries and this was done.

The implications of a single order for 1 million chips were discussed. The cost per chip for such an order was estimated at $50 - $100. It was noted, however, that a supplier probably would not accept a single order for 1 million chips on a one-time basis. Mr. Bigelow asked whether a customer might negoitate on the basis of a larger order, say 5 million chips, then take the first million and disappear. Mr. Hillis pointed out that this was very unlikely, since the supplier would investigate the source of such an order very carefully.

Mr. Lohse enquired as to whether everyone was in agreement that the trends put forward in the summaries were factual. He asked if there were any diverging opinions. None were offered.

Mr. Pyke announced to the Workshop that NBS is establishing a validation service for the DES. He solicited the assistance of the participants in helping NBS to verify the correct operation of the test-bed and to determine how it interfaces to the actual equipment that might be brought in. Participants wishing to pursue this further should contact Dr. Branstad.

Mr. Jeffery pointed out that the NBS standard refers only to hardware or firmware implementations not changeable by a typical user, as in the case of a microprocessor where the program is contained in a PROM. Mr. Diffie asked whether ROMs would be considered as hardware and Mr. Jeffery responded that these were included in his definition.

The Workshop was concluded with expressions of appreciation to the participants from Dr. Ruth M. Davis, Mr. Lohse, and Mr. Pyke.

*UART -- Universal Asynchronous Receiver-Transmitter, an LSI component widely used for communications applications, such as remote terminals.

Appendix A

Attendee List
1976 Workshop on Estimation of Significant Advances in Computer Technology
August 30 - 31, 1976

Mr. Jogindra M. Bakshi
National Bureau of Standards

Mr. Julian Bigelow
Institute for Advanced Study

Mr. Robert P. Blanc
National Bureau of Standards

Dr. Dennis K. Branstad
National Bureau of Standards

Dr. Herbert S. Bright
Computation Planning, Inc.

Dr. Ruth M. Davis
National Bureau of Standards

Mr. Whitfield Diffie
Stanford University

Mr. Joseph K. Everton
Sperry Rand Corporation

Dr. Jason Gait
National Bureau of Standards

Mrs. Martha M. Gray
National Bureau of Standards

Mr. Dana S. Grubb
National Bureau of Standards

Mr. Durrell W. Hillis
Motorola, Inc.

Mr. Seymour Jeffery
National Bureau of Standards

Mr. George E. Lindamood
National Bureau of Standards

Mr. Edward Lohse
Burroughs Corporation

Mr. John T. Lynch
Burroughs Corporation

Mr. Bill Maczko
Incoterm Corporation

Mr. Henry S. McDonald
Bell Telephone Laboratories

Mr. John J. McDonnell
Electronic Funds Transfer Commission

Mr. Paul Meissner
National Bureau of Standards

Mr. Jeremiah J. Murray
U. S. Army Electronics Command

Mr. James C. Nelson
Sperry Rand Corporation

Mr. Frank F. Oettinger
National Bureau of Standards

Mr. R. A. Pagan
Federal Aviation Administration

Dr. Mel Pirtle
NASA Ames Research Center

Mr. Thomas N. Pyke, Jr.
National Bureau of Standards

Mr. Robert Robke
NCR Corporation

Mr. Steven Schieltz
Dataproducts Corporation

Mr. Frank Secretan
Collins Radio Group

Mr. Bud Studley
U. S. House of Representatives

Mr. Rod Thorpe
Collins Radio Group

Mr. Doland Toth
Control Data Corporation

Mr. Christopher Van Wyk
National Bureau of Standards

Mr. Irving Wieselman
Dataproducts Corporation

Mr. Howard Wright
Collins Radio Group

APPENDIX B. WORKSHOP BACKGROUND INFORMATION

1976 WORKSHOP ON ESTIMATION OF SIGNIFICANT ADVANCES IN COMPUTER TECHNOLOGY

I. PURPOSE

The Institute for Computer Sciences and Technology (ICST) of the National Bureau of Standards has, under Public Law 89-306, certain resoonsibilities for the management of computer technology in the Federal Government. Specifically, it strives to monitor and understand advances in computer sciences and technology, assess their technologically-derived impact and attempt as appropriate to help in their application and acceptance within the Federal Government.

This Workshop is intended to provide ICST with current scientific and technical information on advances in computer technology which could significantly impact the Federal Government's knowledge and use of computer technology developments in relation to computer security and export administration.

The focus of the Workshop is to be on advances in the design, architecture and manufacturing of computer systems and related equipment which can be identified or estimated as characterizing the present state-of-the-art and the predictable future.

II. SPECIFIC OBJECTIVES

NBS will use this information to (1) estimate the availability of computer resources necessary to recover the key employed in the NBS-proposed Data Encryption Standard, (2) model advanced computer systems for which computer security safeguards must be emplaced to prevent computer fraud and to meet legislated privacy requirements, and (3) assess the potential technical significance of the proposed export of computer-related products and technology.

III. SPECIFIC PROBLEM

So as to achieve these objectives, the Workshop will address a specific problem as a useful vehicle for examining current and projected capabilities for the design and manufacture of computer systems and related hardware which address specific computational applications. Attention to this particular problem will also be of direct and immediate assistance to NBS in the development of standards and guidelines, especially those related to computer security.

The problem which has been selected is representative of a class of problems whose performance is not assumed to be constrained by traditional computer architectures and techniques. It involves the design and fabrication of a system to perform the algorithm specified in Attachment A. Note that embedded in this algorithm is a function "g", which is the data encryption algorithm recently proposed as a Federal standard by NBS. Attachment B describes this algorithm.

IV. QUESTIONS TO BE AOORESSEO

Among the questions to be considered by the Workshop in addressing this problem are:

1. What are the candidate system architectures for implementing this algorithm?
2. What are the basic performance and ccst characteristics of current and projected electronic devices suitable for use in implementations of these architectures, e.g., semiconductor devices, Josephson effect devices, . . .?
3. What system designs appear most effective in terms of execution time, error performance, power dissipation, and physical space?
4. What component and system manufacturing limitations may be involved in the implementation?
5. What are the inter-relationships among the basic overall engineering parameters, such as time to successful algorithm execution; cost to design, fabricate, test, operate and maintain; and elapsed time between initiation of design and system operation?
6. What is the projected effect on the considerations above of the time of initiation of the effort, e.g., now, twu years from now, five years from now, . . .?
7. What additional physical limits or technical resource constraints are applicable?

It is hoped that the answers to these questions will be addressed in quantitative terms and, as applicable, through graphical representations of parametric tradeoffs.

V. QUALIFICATIONS OF PARTICIPANTS

The participants should be recognized experts on capabilities and techniques in one or more of the following areas:

- semiconductor manufacturing
- logic design
- system architecture
- system fabrication

Participants should be able to address the above in terms of the current state-of-the-art as well as near future capabilities and techniques.

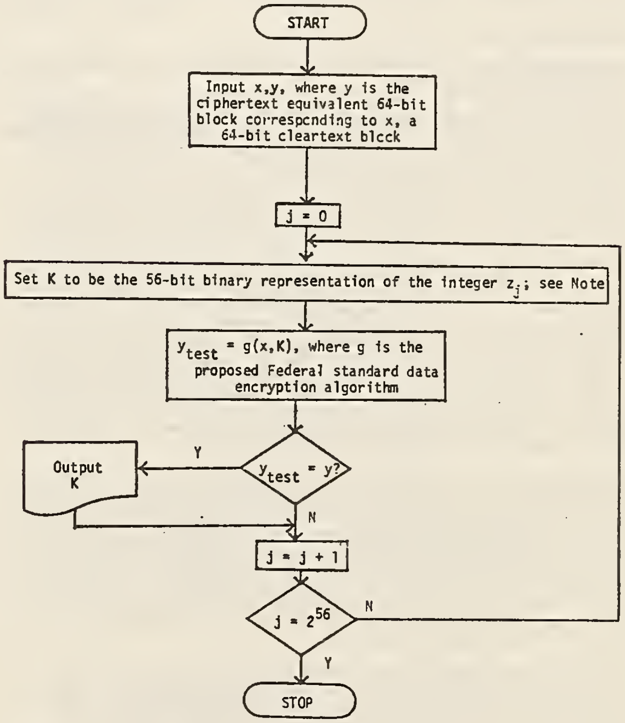
VI. WORKSHOP PROOUCT

The product of the Workshop will be a technical report on the topics treated, to be produced by NBS (ICST) according to a format to be determined by the Workshop participants. This report will serve as a significant element in NBS' recommendations to the Executive Branch, to Congress, and to public groups for needed actions pertaining to the subject areas of the Workshop.

VII. WORKSHOP ARRANGEMENTS

The Workshop will be held at NBS, Gaithersburg, Maryland on August 30 - 31, 1976 in Dining Room C, Administration Building.

ATTACHMENT A: EXHAUSTIVE EXTRACTION ALGORITHM


START
Input x,y, where y is the ciphertext equivalent 64-bit block corresponding to x, a 64-bit cleartext block
j = 0
Set K to be the 56-bit binary representation of the integer z_j; see Note
$y_{test} = g(x,K)$, where g is the proposed Federal standard data encryption algorithm
$y_{test} = y$?
Y
Output K
N
j = j + 1
$j = 2^{56}$
N
Y
STOP

Note:

z_j may be defined as follows:

let $z_0 = 0$

$z_{j+1} = z_j + 1$

Any other technique which will systematically generate all keys K_j may in the interval $(0, 2^{56} - 1)$ may be substituted for the above.

Federal Information
Processing Standards Publication

Date ________

ANNOUNCING THE

DATA ENCRYPTION STANDARD

Federal Information Processing Standards Publications are issued by the National Bureau of Standards pursuant to the Federal Property and Administrative Services Act of 1949 as amended, Public Law 89-306 (79 Stat 1127) as implemented by Executive Order 11717 (38 FR 12315, dated May 11, 1973), and Part 6 of Title 15 CFR (Code of Federal Regulations).

Name of Standard. Data Encryption Standard (DES)

Category of Standard. ADP Operations, Computer Security.

Explanation: This Data Encryption Standard specifies an algorithm for the cryptographic protection of computer data. This publication provides a complete description of a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information. Encrypting converts data to an unintelligible form called cipher. Decrypting converts the cipher back to the original data. Both of these mathematical transformations are based on a single binary variable called the key.

Data may be protected against unauthorized disclosure by generating a random key and issuing it to the authorized users of the data. The cipher that has been produced by performing the steps of the encryption algorithm on data using a particular key can only be returned to the original data by use of the decryption algorithm using the identical key. Unauthorized recipients of the cipher who may have the algorithm but do not have this key cannot derive the original data. A standard algorithm based on a user-generated key thus provides a basis for compatible cryptographic protection of computer data while preventing unauthorized use of the data in cipher form.

Approving Authority. Secretary of Commerce.

Maintenance Agency. Institute for Computer Sciences and Technology, National Bureau of Standards.

Applicability. The Data Encryption Standard will be used by Federal agencies for protecting unclassified computer data when the responsible authority for the data or the computer systems of that agency has stipulated that cryptographic protection is required. Data that is considered sensitive by the responsible authority or data which has a high value or represents a high value should be cryptographically protected if it is vulnerable to unauthorized disclosure or undetected modification during transmission or in dormant storage. During transmission data may be encrypted at a terminal and the resulting cipher transmitted. Data may also be encrypted before it is written as cipher onto a storage device (magnetic tape, removable disk pack, etc.) which may be removed and read by unauthorized personnel. However, cipher must be decrypted before it can be processed. Data stored in cipher form can only be read if the key used to encrypt it is stored until the data is to be read and used. This standard is not applicable for the cryptographic protection of computer data that is classified according to the National Security Act of 1947 or the Atomic Energy Act of 1954, as amended. Provisions of these Acts and their implementing regulations specify the means for protecting classified data.

Implementation. This standard becomes effective six months from the date of its publication following approval by the Secretary of Commerce. As new ADP systems and networks are developed and current systems are improved, Federal agencies, based upon their specific data protection requirements, should develop and implement regulations for the use of this standard. These regulations should specify when and where data encryption should be used and include administrative procedures for using it in a computer system or network. Instructions for procuring data processing equipment utilizing the DES will be provided by the General Services Administration.

The algorithm specified in this Data Encryption Standard is to be implemented in special purpose hardware when used by Federal agencies. An electronic device which performs the mathematical steps of the algorithm may comprise one or more Large Scale Integration (LSI) "chips" in a single electronic package. An alternate implementation may consist of many Medium Scale Integration (MSI) electronic packages. Developing technologies may allow the effective and efficient performance of the algorithm in other electronic devices (e.g., micro-computers with Read Only Memories) which are dedicated to performing the operations of the algorithm. Only hardware implementations of the algorithm which can be tested and certified as being accurate will be considered as complying with the standard. Such devices must also conform to the export controls of Title 22, Code of Federal Regulations, Parts 121 through 128. These regulations specify that cryptographic devices or cryptographic information are controlled if intended for export.

Cryptographic devices implementing this standard may be covered by U. S. and foreign patents held by the International Business Machines Corporation, which has agreed to grant nonexclusive, royalty-free licenses under the patents to make, use and sell apparatus which complies with the standard. The terms, conditions and scope of the licenses are set out in a notice published in the May 13, 1975 issue of the Official Gazette of the United States Patent and Trademark Office (934 O. G. 452).

Specifications. Federal Information Processing Standard (FIPS) Data Encryption Standard (affixed).

Cross Index:

a. FIPS PUB 31, "Guidelines to ADP Physical Security and Risk Management"

b. FIPS PUB 41, "Computer Security Guidelines for Implementing the Privacy Act of 1974"

Qualifications. This Data Encryption Standard specifies an algorithm which may be utilized in many applications and environments. A device which performs the algorithm may be used as a fundamental building block in applications areas where cryptographic protection is needed. Implementation of a cryptographic system comprising many cryptographic devices located in computer terminals, computer "front end" communications processors and computer storage device data channels is a complex task. Guidelines for implementing and using data encryption devices will be provided by NBS. A series of technical notes describing alternative ways of using data encryption devices will be produced. For example, the algorithm may be used both directly as an encryptor of blocks of data and indirectly as a binary stream generator which may be combined with the data to produce the cipher. The cipher produced with the latter technique has the same high degree of cryptographic protection as the cipher produced if the data were entered directly into the data encryption device. In either case, the cryptographic device must be properly interfaced to the other system components in the application area. When properly implemented and used, Government agencies may rely on the DES to provide a high level of cryptographic protection to valuable and sensitive information. NBS, supported by the technical assistance of appropriate Government agencies, has determined that the algorithm in this Data Encryption Standard can provide this level of protection beyond the normal life cycle of its associated ADP equipment.

Comments and suggestions regarding the use of this standard are welcomed and should be addressed to the Associate Director for ADP Standards, Institute for Computer Sciences and Technology, National Bureau of Standards, Washington, D. C. 20234.

Waiver Procedure. The head of a Federal agency may waive the provisions of this FIPS PUB upon proper justification and upon coordination with the National Bureau of Standards. A waiver is not necessary unless cryptographic protection is required for unclassified computer data and either a different encryption algorithm is to be used or a software implementation of this algorithm is needed. Letters describing the nature of, and reasons for, the waiver should be addressed to the Associate Director for ADP Standards, Institute for Computer Sciences and Technology, National Bureau of Standards, Washington, D. C. 20234.

Sixty days should be allowed for review and response by NBS. The waiver is not to be made until a reply from NBS is received; however, the final decision for granting the waiver is the responsibility of the agency head.

Where to Obtain Copies of the Standard.

a. Copies of this publication are for sale by the Superintendent of Documents, U. S. Government Printing Office, Washington, D. C. 20402 (___ per copy; SD Catalog Number C __________). There is a 25 percent discount on quantities of 100 or more. When ordering, specify document number, title, and SD Catalog Number. Payment may be made by check, money order, coupons, or deposit account.

b. Microfiche copies of this publication are available from the National Technical Information Service, U. S. Department of Commerce, Springfield, Virginia 22161. When ordering, refer to Report Number NBS-FIPS-PUB-____ and title. The cost is ____ per copy and payment may be made by check, money order, coupons or deposit account.

Federal Information
Processing Standards Publication

Date ________

SPECIFICATIONS FOR THE
DATA ENCRYPTION STANDARD

The Data Encryption Standard (DES) shall consist of the following Data Encryption Algorithm implemented in a special purpose electronic device. This device shall be designed in such a way that it may be embedded in a computer system or network and provide cryptographic protection to binary coded data. The method of implementation, the control of the cryptographic device and the interface of the device to its associated equipment will depend on the application and environment. The device shall be designed and implemented in such a way that it may be tested and validated as accurately performing the transformations specified in the following algorithm. Certification of compliance with this standard is the responsibility of the designer and manufacturer of the device.

DATA ENCRYPTION ALGORITHM

Introduction

The algorithm is designed to encipher and decipher blocks of data consisting of 64 bits under control of a 64 bit key. Deciphering must be accomplished by using the same key as for enciphering, but with the schedule of addressing the key bits altered so that the deciphering process is the reverse of the enciphering process. A block to be enciphered is subjected to an initial permutation IP, then to a complex key-dependent computation and finally to a permutation which is the inverse of the initial permutation IP^{-1}. The key-dependent computation can be simply defined in terms of a function f, called the cipher function, and a function KS, called the key schedule. A description of the computation is given first, along with details as to how the algorithm is used for encipherment. Next, the use of the algorithm for decipherment is described. Finally, a definition of the cipher function f is given in terms of primitive functions which are called the selection functions S_i and the permutation function P. S_i, P and KS of the algorithm are contained in the Appendix.

The following notation is convenient: Given two blocks L and R of bits, LR denotes the block consisting of the bits of L followed by the bits of R. Since concatenation is associative $B_1B_2...B_8$, for example, denotes the block consisting of the bits of B_1 followed by the bits of B_2... followed by the bits of B_8.

Enciphering

A sketch of the enciphering computation is given in Figure 1.

The 64 bits of the input block to be enciphered are first subjected to the following permutation, called the initial permutation IP:

IP

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

That is the permuted input has bit 58 of the input as its first bit, bit 50 as its second bit, and so on with bit 7 as its last bit. The permuted input block is then the input to a complex key-dependent computation described below. The output of that computation, called the preoutput, is then subjected to the following permutation which is the inverse of the initial permutation:

IP^{-1}

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

That is, the output of the algorithm has bit 40 of the preoutput block as its first bit, bit 8 as its second bit, and so on, until bit 25 of the preoutput block is the last bit of the output.

The computation which uses the permuted input block as its input to produce the preoutput block consists, but for a final interchange of blocks, of 16 iterations of a calculation that is described below in terms of the cipher function f which operates on two blocks, one of 32 bits and one of 48 bits, and produces a block of 32 bits.

Let the 64 bits of the input block to an iteration consist of a 32 bit block L followed by a 32 bit block R. Using the notation defined in the introduction, the input block is then LR.

ENCIPHERING COMPUTATION

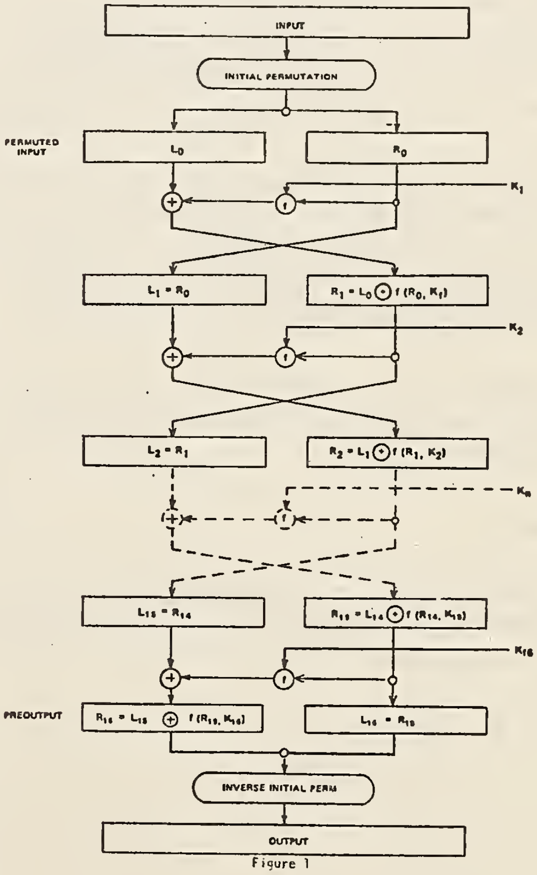


Figure 1

Let K be a block of 48 bits chosen from the 64 bit key. Then the output L'R' of an iteration with input LR is defined by:

$$(1) \quad L' = R$$
$$R' = L \oplus f(R,K)$$

where ⊕ denotes bit-by-bit addition modulo 2.

As remarked before, the input of the first iteration of the calculation is the permuted input block. If L'R' is the output of the 16th iteration then R'L' is the preoutput block. At each iteration a different block K of key bits is chosen from the 64 bit key designated by KEY.

With more notation we can describe the iterations of the computation in more detail. Let KS be a function which takes an integer n in the range from 1 to 16 and a 64 bit block KEY as input and yields as output a 48 bit block K_n which is a permuted selection of bits from KEY. That is

$$(2) \quad K_n = KS(n,KEY)$$

with K_n determined by the bits in 48 distinct bit positions of KEY. KS is called the key schedule because the block K used in the n'th iteration of (1) is the block K_n determined by (2). As before, let the permuted input block be LR. Finally, let L_o and R_o be respectively L and R and let L_n and R_n be respectively L' and R' of (1) when L and R are respectively L_{n-1} and R_{n-1} and K is K_n; that is, when n is in the range from 1 to 16,

$$(3) \quad L_n = R_{n-1}$$
$$R_n = L_{n-1} \oplus f(R_{n-1},K_n)$$

The preoutput block is then $R_{16}L_{16}$.

The key schedule KS of the algorithm is described in detail in the Appendix. The key schedule produces the 16 K_n which are required for the algorithm.

Deciphering

The permutation IP^{-1} applied to the preoutput block is the inverse of the initial permutation IP applied to the input. Further, from (1) it follows that:

$$(4) \quad R = L'$$
$$L = R' \oplus f(L',K)$$

Consequently, to decipher it is only necessary to apply the very same algorithm to an enciphered message block, taking care that at each iteration of the computation the same block of key bits K is used during decipherment as was used during the encipherment of the block. Using the notation of the previous section, this can be expressed by the equations:

$$(5) \quad R_{n-1} = L_n$$
$$L_{n-1} = R_n \oplus f(L_n,K_n)$$

where now $R_{16}L_{16}$ is the permuted input block for the deciphering calculation and L_0R_0 is the preoutput block. That is, for the decipherment calculation with $R_{16}L_{16}$ as the permuted input, K_{16} is used in the first iteration, K_{15} in the second, and so on, with K_1 used in the 16th iteration.

The Cipher Function f

A sketch of the calculation of f(R,K) is given in Figure 2.

CALCULATION OF f(R,K)

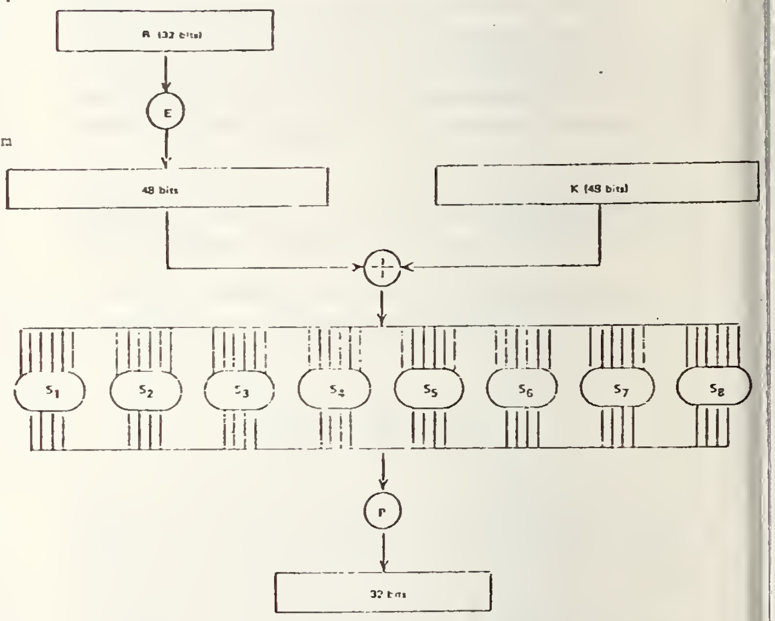


Figure 2

Let E denote a function which takes a block of 32 bits as input and yields a block of 48 bits as output. Let E be such that the 48 bits of its output, written as 8 blocks of 6 bits each, are obtained by selecting the bits in its inputs in order according to the following table:

E BIT-SELECTION TABLE

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Thus the first three bits of E(R) are the bits in positions 32, 1 and 2 of R while the last 2 bits of E(R) are the bits in positions 32 and 1.

Each of the unique selection functions S_1, S_2, ..., S_8, takes a 6 bit block as input and yields a 4 bit block as output and is illustrated by using a table containing the recommended S_1:

S_1

Column Number

Row No.	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

If S_1 is the function defined in this table and B is a block of 6 bits, then $S_1(B)$ is determined as follows: The first and last bits of B represent in base 2 a number in the range 0 to 3. Let that number be i. The middle 4 bits of B represent in base 2 a number in the range 0 to 15. Let that number be j. Look up in the table the number in the i'th row and j'th column. It is a number in the range 0 to 15 and is uniquely represented by a 4 bit block. That block is the output $S_1(B)$ of S_1 for the input B. For example, for input 011011 the row is 01, that is row 1, and the column is determined by 1101, that is column 13. In row 1 column 13 appears 5 so that the output is 0101. Selection functions S_1, S_2,...,S_8 of the algorithm appear in the Appendix.

The permutation function P yields a 32 bit output from a 32 bit input by permuting the bits of the input block. Such a function is defined by the following table:

P

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

The output P(L) for the function P defined by this table is obtained from the input L by taking the 16th bit of L as the first bit of P(L), the 7th bit as the second bit of P(L), and so on until the 25th bit of L is taken as the 32nd bit of P(L). The permutation function P of the algorithm is repeated in the Appendix.

Now let S_1,...,S_8 be eight distinct selection functions, let P be the permutation function and let E be the function defined above.

To define f(R,K) we first define B_1,...,B_8 to be blocks of 6 bits each for which

$$(6) \qquad B_1B_2\ldots B_8 = K \oplus E(R)$$

The block f(R,K) is then defined to be

$$(7) \qquad P(S_1(B_1)S_2(B_2)\ldots S_8(B_8))$$

Thus $K \oplus E(R)$ is first divided into the 8 blocks as indicated in (6). Then each B_i is taken as an input to S_i and the 8 blocks $S_1(B_1)$,$S_2(B_2)$,...,$S_8(B_8)$ of 4 bits each are consolidated into a single block of 32 bits which forms the input to P. The output (7) is then the output of the function f for the inputs R and K.

APPENDIX

PRIMITIVE FUNCTIONS FOR THE DATA ENCRYPTION ALGORITHM

The choice of the primitive functions KS, S_1, ..., S_8 and P is critical to the strength of an encipherment resulting from the algorithm. Specified below is the recommended set of functions, describing S_1, ..., S_8 and P in the same way they are described in the algorithm. For the interpretation of the tables describing these functions, see the discussion in the body of the algorithm.

The primitive functions $S_1, \ldots, S_8$, are:

S_1

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S_2

15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S_3

10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S_4

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

S_5

2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S_6

12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S_7

4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S_8

13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

The primitive function P is:

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

Recall that K_n, for $1 \le n \le 16$, is the block of 48 bits in (2) of the algorithm. Hence, to describe KS, it is sufficient to describe the calculation of K_n from KEY for n = 1, 2, ..., 16 That calculation is illustrated in Figure 3. To complete the definition of KS it is therefore sufficient to describe the two permuted choices, as well as the schedule of left shifts. One bit in each eight-bit byte of the KEY may be utilized for error detection in key generation, distribution and storage. Bits 8, 16, ..., 64 are for use in assuring that each byte is of odd parity.

KEY SCHEDULE CALCULATION

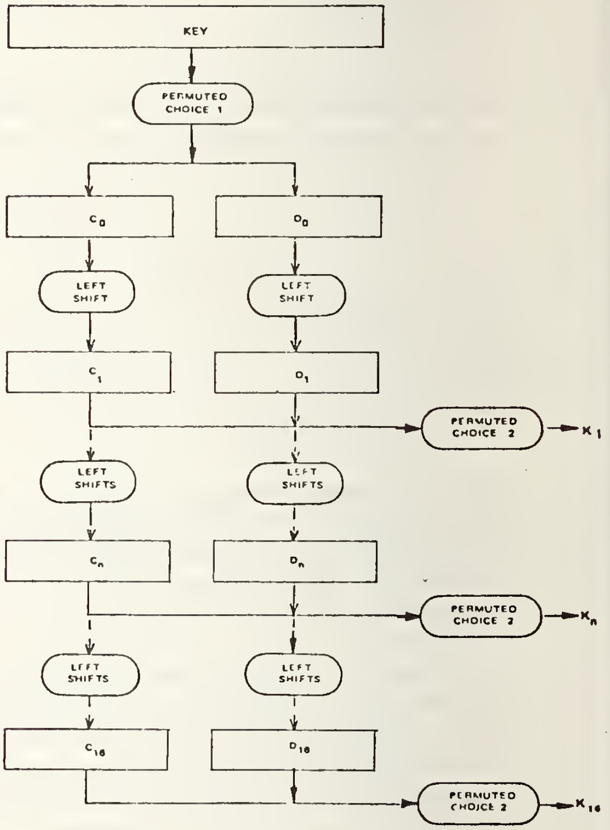


Figure 3

Permuted choice 1 is determined by the following table:

PC-1

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

The table has been divided into two parts, with the first part determining how the bits of C_o are chosen, and the second part determining how the bits of D_o are chosen. The bits of KEY are numbered 1 through 64. The bits of C_o are respectively bits 57, 49, 41, ..., 44 and 36 of KEY, with the bits of D_o being bits 63, 55, 47, ..., 12 and 4 of KEY.

With C_o and D_o defined, we now define how the blocks C_n and D_n are obtained from the blocks C_{n-1} and D_{n-1}, respectively, for n = 1, 2, ..., 16. That is accomplished by adhering to the following schedule of left shifts of the individual blocks:

Iteration Number	Number of Left Shifts
1	1
2	1
3	2
4	2
5	2
6	2
7	2
8	2
9	1
10	2
11	2
12	2
13	2
14	2
15	2
16	1

For example, C_3 and D_3 are obtained from C_2 and D_2, respectively, by two left shifts, and C_{16} and D_{16} are obtained from C_{15} and D_{15}, respectively, by one left shift. In all cases, by a single left shift is meant a rotation of the bits one place to the left, so that after one left shift the bits in the 28 positions are the bits that were previously in positions 2, 3, ..., 28, 1.

Permuted choice 2 is determined by the following table:

PC-2

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Therefore, the first bit of K_n is the 14th bit of C_nD_n, the second bit the 17th, and so on with the 47th bit the 29th, and the 48th bit the 32nd.

USCOMM-NBS-DC

NBS-114A (REV. 7-73)

U.S. DEPT. OF COMM. **BIBLIOGRAPHIC DATA SHEET**	1. PUBLICATION OR REPORT NO. NBSIR 76-1189	2. Gov't Accession No.	3. Recipient's Accession No.

4. TITLE AND SUBTITLE

Report of the 1976 Workshop on
Estimation of Significant Advances
in Computer Technology

5. Publication Date

December 1976

6. Performing Organization Code

7. AUTHOR(S) Paul Meissner

8. Performing Organ. Report No.

9. PERFORMING ORGANIZATION NAME AND ADDRESS

NATIONAL BUREAU OF STANDARDS
DEPARTMENT OF COMMERCE
WASHINGTON, D.C. 20234

10. Project/Task/Work Unit No.

6501115

11. Contract/Grant No.

12. Sponsoring Organization Name and Complete Address *(Street, City, State, ZIP)*

Same as item 9.

13. Type of Report & Period Covered

Final

14. Sponsoring Agency Code

15. SUPPLEMENTARY NOTES

16. ABSTRACT *(A 200-word or less factual summary of most significant information. If document includes a significant bibliography or literature survey, mention it here.)*

A workshop on the estimation of significant advances in computer technology was conducted by the Institute for Computer Sciences and Technology at the National Bureau of Standards on August 30-31, 1976. The workshop was attended by 20 representatives from industry, research organizations, universities and Government agencies. The workshop was held to obtain current scientific and technical information on advances in computer technology which could significantly impact the Federal Government's knowledge and use of computer technology developments in relation to computer security and export administration. Presentations were made on anticipated advances in computer architecture and semiconductor technology. It was indicated that the present trends in component density for LSI will continue to increase at the current rate for at least five years. The speed of logic circuitry has been increasing at a rate of about 1.5 megaHertz per year, and a speed of 30 megahertz is presently attainable. Speed-power ratios have been improving by a factor of 10 about every 4 years, and a similar improvement appears likely in the next 4 years. The current emphasis in development work is on achieving high density at low cost. In order to provide a vehicle around which to organize its discussions, the workshop considered the design of a hypothetical machine for extracting the key used for encrypting data under the proposed NBS Data Encryption Standard. Several designs were postulated and engineering estimates were developed for operating speed, size, development time, cost, and other factors.

17. KEY WORDS *(six to twelve entries; alphabetical order; capitalize only the first letter of the first key word unless a proper name; separated by semicolons)*

Computer architecture; computer security; computer technology; encryption; semiconductor technology; technology advances

18. AVAILABILITY ☒ Unlimited

□ For Official Distribution. Do Not Release to NTIS

□ Order From Sup. of Doc., U.S. Government Printing Office
Washington, D.C. 20402, SD Cat. No. C13

☒ Order From National Technical Information Service (NTIS)
Springfield, Virginia 22151

19. SECURITY CLASS (THIS REPORT) UNCLASSIFIED	21. NO. OF PAGES 33
20. SECURITY CLASS (THIS PAGE) UNCLASSIFIED	22. Price $4.00