NBSIR 77-1291

Report of the Workshop on Cryptography in Support of Computer Security

Held at the National Bureau of Standards
September 21-22, 1976

Dennis Branstad
Jason Gait
Stuart Katzke

Systems and Software Division
Institute for Computer Sciences and Technology
National Bureau of Standards
Washington, D. C. 20234

September 1977

U.S. DEPARTMENT OF COMMERCE

NATIONAL BUREAU OF STANDARDS

NBSIR 77-1291

REPORT OF THE WORKSHOP ON CRYPTOGRAPHY IN SUPPORT OF COMPUTER SECURITY

Held at the National Bureau of Standards
September 21-22, 1976

Dennis Branstad
Jason Gait
Stuart Katzke

Systems and Software Division
Institute for Computer Sciences and Technology
National Bureau of Standards
Washington, D. C. 20234

September 1977

U.S. DEPARTMENT OF COMMERCE, Juanita M. Kreps, *Secretary*

Dr. Sidney Harman, *Under Secretary*

Jordan J. Baruch, *Assistant Secretary for Science and Technology*

NATIONAL BUREAU OF STANDARDS, Ernest Ambler, *Acting Director*

LIST OF FIGURES

Page

Report of the Workshop on Cryptography in Support of Computer Security

Held at the National Bureau of Standards
September 21-22, 1976

Dennis Branstad
Jason Gait
Stuart Katzke

This publication reports on the Workshop on Cryptography in Support of Computer Security held at the National Bureau of Standards on September 21-22, 1976. The workshop was organized to obtain expert opinions on the mathematical and statistical characteristics of the proposed Data Encryption Standard (DES) as it relates to computer security. This report summarizes formal presentations that were made, outlines major issues that were raised, quotes statements that were made for the record and answers several of the major questions that were asked.

Key words: Cryptanalysis ; cryptography; encryption; key management; known plaintext attack; security; work factor.

1. EXECUTIVE SUMMARY

1.1 Organization

1. The workshop was divided into three time periods: introduction, parallel working sessions, and summary.

2. A total of 42 people attended from the Federal Government, industry and universities.

3. The workshop chairman was Professor Julian Bigelow, the Mathematics group leader was Dr. Howard Campaigne and the Applications group leader was Dr. Joseph Eachus.

1.2 Introductory Session

1. The purposes of the introductory session were to introduce the objectives of the workshop, i.e., to analyze the mathematical and statistical characteristics of the proposed Data Encryption Standard (DES); to provide a forum for identifying potential weaknesses of the DES; and to develop procedures for generating and distributing keys.

2. Individual participants presented a description of the DES,the results of a previous NBS sponsored workshop on technology affecting the DES, and preliminary analysis of the DES.

3. Professor Martin Hellman, of Stanford University, presented a prepared statement.

4. Mr. John Scantlin, of the Lexar Corp., submitted for distribution a written paper which analyzed the DES.

1.3 Mathematics Working Group

1. The mathematics working group discussed potential weaknesses of the DES, such as the limitations in key length, the non-random structure of the S-boxes, and possible vulnerabilities to less than exhaustion atacks.

2. Some participants felt that the 56-bit key was too short against high- technology, high cost attack. One assertion was made that the algorithm could be sucessfully attacked for a cost of $20 million. It was pointed out that the first workshop on technology included estimates that the actual cost of building a key-extraction machine would be at least $72 million, the completion date would be 1990, the exhaustion time would be approximately 20 hours, and the probability of success would be low. One participant stated that his personal estimate of the cost (actual cost of production to a manufacturer) to build such a machine would be on the order of $200 million, could not be delivered until at least 1981, would produce 1 key per day, would have a low probability of success and that such a machine would never

be built. Claims were made that the cost would decrease by an order of magnitude every five years. The general response was that in spite of this the key was satisfactory for all security requirements of economic data (money transfers, proprietary data) and that using the algorithm serially (cascading two chips) satisfied all security requirements for data protected by the proposed DES.

3. There was a concern that S-boxes were non-random and the designer stated this to be true. When reasons for the choice of non-random S-boxes were requested, the designer stated:

a. Non-random entries were necessary to provide security.

b. The design criteria, independently derived, coincided with some that were classified and the designers agreed not to make them public.

c. Of the possible good S-boxes, these were chosen to minimize combinatorial logic.

d. The draft DES, published by NBS, was exactly as designed and submitted.

4. The acceptability of having a standard based on classified criteria was questioned. Instances were given of some standards based on such criteria (DOD, AEC). The consensus of group was that the DES was completely and uniquely specified for implementation.

5. A question was raised regarding the acceptability of having a standard based on criteria potentially favorable to one manufacturer. The designer stated that the minimization criteria are obvious to any logic designer choosing to implement S-boxes in boolean logic.

6. The following characteristic of the algorithm was demonstrated: $E(k, p) = c$ and $E(-k, -p) = -c$; i. e., enciphering plaintext with a key produces ciphertext and enciphering the complement of the plaintext with the complement of the key produces the complement of the ciphertext. It was asserted that this characteristic would reduce the work factor of "breaking the algorithm" by 50%. It was pointed out that not only must matched ciphertext for known plaintext be obtained but also matched ciphertext for the complement of the known plaintext. Further, although the number of keys that must be tested with the DES algorithm is reduced by a factor of two, each resultant ciphertext must be compared with both the ciphertext corresponding to the given plaintext and the complement of the ciphertext corresponding

to the complemented plaintext. Thus the net savings will be less than 50%.

7. A participant stated that the initial permutation and its inverse added no security to the algorithm. The designer stated that every logic element and wire contributed to the security of the algorithm.

8. Questions were raised concerning the amount of testing of the algorithm that had been done. The designer stated that 17 man-years of effort had been expended in analysis, gave references to five consultants who aided in analysis, and said that no short cuts in cryptanalysis had been found.

9. The discussants attempted to identify less than exhaustion attacks on the algorithm without success.

10. The representative of the Commission on Electronic Fund Transfer stated that as a result of his attending the two workshops, he planned to recommend the use of the proposed standard in electronic funds transfer applications.

1.4 Applications Working Group

1. The emphasis was on key generation and distribution. The consensus was that potential security problems would be the loss or misuse of keys rather than analysis of the algorithm.

2. Keys should be distributed independently of the communication system they are protecting.

3. NBS should publish guidelines for key distribution and usage at a detail useful to the user but not so detailed that potential penetrators could "track" key utilization.

4. Complex keys, consisting of subelements from independent sources, should be considered for use in cryptographic systems.

1.5 Summary Session

1. On key length, it was concluded that a 48 bit key is too short for most applications. A 56 bit key is adequate at present for business applications; a longer key would provide more security.

2. The benefits, costs and threats of encryption should be defined.

3. An analysis and statement of strength of the DES should be made. If an analysis would result in deriving 8-10 bits of key, it should be considered significant if derived mathematically or statistically. The range of the number of bits considered significant by individual participants was 3-20 bits. The 8-10 bit range represents the consensus. A reduction of 1-2 bits was not considered significant.

4. Attack on the economic system of the U. S. by foreign subversive elements should be considered in utilizing all security measures, including encryption.

5. Work should continue on developing a replacement encryption standard for either simpler software implementation or improved security against projected future threats.

6. Some participants felt that since the design principles of the S-boxes were independently discovered, they should be publishable even though they are considered classified.

7. Assertions were made that S-boxes should contain the exclusive-or combination of S-boxes chosen by NBS, the designer of the algorithm and IEEE.

8. It was agreed that the S-box entries were not selected at random but were chosen according to some unspecified criteria. Most of the participants accepted the designers explanation that this was done to strengthen rather than weaken the algorithm.

9. The consensus was that the DES should be adopted as a standard at this time but that work should continue in demonstrating or disproving the strength of DES. No suggestions of who should do the work or how it should be funded were made.

10. NBS agreed to prepare responses to questions raised during the workshop (see attachment 8.4).

2. OVERVIEW

The workshop began with a number of introductory

comments and brief presentations. Professor Julian Bigelow, Institute for Advanced Studies at Princeton, welcomed the participants to the workshop and outlined the workshop objectives. Dr. Ruth Davis, Director of the Institute for Computer Sciences and Technology, gave an overview of the development process of the proposed Data Encryption Standard (DES). Technical presentations by ICST members and other workshop participants provided descriptions of the DES and how it may be used in computer systems.

The objective of the mathematics working group was to identify and analyze potential weaknesses of the DES algorithm. The prime arguments centered around the length of the key and the structure of the substitution boxes (S boxes). The first argument reiterated the concern that a 56-bit key length was inadequate to prevent a key exhaustion attack against the algorithm for the next 10-20 years. While the results of the Workshop on Estimation of Significant Advances in Computer Technology, devoted to this issue, showed that the cost and feasibility of using today's technology, or that expected in the next 10-15 years, did not support the foundation of this concern, the issue was discussed at length. The second argument concerned the apparent structure in the eight S-boxes of the algorithm and the reason for this structure.

These arguments were not completely resolved. It was felt that the proposed DES was adequate in its simplest form for normal business applications and could be used in series (cascaded) to provide a higher level of security whenever the application or technology warranted it. It was felt that if a mathematical attack on the algorithm existed which provided a method for deriving a number of bits (8-10 were felt significant), it could be used in conjunction with an exhaustion attack to reduce the security of the algorithm. However, no such attack was formulated and no such method is known to exist. A demonstration of a characteristic of the algorithm which complements (in a mathematical sense) the output if all the inputs are complemented was given. This could be used to reduce the security of the algorithm to an effective 55-bit key if a penetrator is allowed to choose the plaintext and has knowledge of the resulting ciphertext.

It was determined that the S-boxes indeed had structure. They had been selected by the designer of the algorithm from all possible 4x16 matrices, the rows of which are permutations of the integers 0 to 15. The cryptographic characteristics selected by the designer happened to coincide with some that were considered classified and the designer agreed not to publicly describe them. A question on the propriety of a standard based on a classified design was raised. It was agreed that the algorithm itself was

completely described and could be implemented and used but that independent verification of the security of the algorithm would be easier if the design criteria were published. One participant had analyzed the structure of the S-boxes and concluded that the structure did not provide any cryptographic weakness that he could identify but might be similar to the structure that might hide a trap- door. The designer stated that no trap-door had been designed into the algorithm, no accidental one was discovered after 17 man years of analysis and none was felt to exist.

The objectives of the applications working group were concerned with investigating methods of generating and distributing encryption keys, protecting them, and utilizing the DES in various applications. It was felt that the keys must not only be protected against unauthorized use but also must be protected against destruction and unavailability for authorized use. Keys must be distributed, at least in part, outside the system that they are protecting. The consensus was that the potential security problems with the DES would be loss or misuse of keys rather than analysis of the algorithm or exhaustive techniques of deriving a key. It was suggested that complex keys (consisting of subelements distributed through independent channels and combined only during usage) should be considered for use in cryptographic systems.

3. INTRODUCTORY SESSION, SEPTEMBER 21

For convenience and clearness of describing the events at the workshop, the write up is divided into separate sections for each of the two days. Each section is further divided into a description of the formal presentations followed by the resulting discussions.

3.1 Summaries of Presentations, September 21

The workshop session was opened by the chairman, Professor Julian Bigelow, of the Institute for Advanced Studies at Princeton, New Jersey. Professor Bigelow's introductory remarks dealt with the overall purpose of the workshop, set it in the context of the introduction and adoption of a Data Encryption Standard and set forward the overall format for the various sessions of the workshop.

BIGELOW: The purpose of this workshop is to explore the general area of encryption technology as it relates to the data encryption standard that has been proposed by the National Bureau of Standards. For our purposes we will not be concerned with the specific hardware aspects of the problem, i. e., the details of the introduction of cryptographic equipment into computer systems, existing or future, but with the effectiveness of the encryption algorithm in the proposed data encryption standard, i. e., the question of whether the proposed standard has any logical "gaps, " or weaknesses that are concealed from the cursory view of the cryptanalytically unsophisticated.

We should consider in detail two pertinent issues in this area: the first of these is whether there exists an inversion technique, of a purely mathematical nature, that would permit the recovery of the key purely from a knowledge of the form of the algorithm, the possession of some quantity of ciphertext and perhaps the possession of matched plaintext as well; next, we need to explore the use of known tools and techniques, such as statistical analysis, which might have the potential of providing concrete information about the relationship between ciphertext and key, or between matched plaintext-ciphertext and key. We need to realize, taking a realistic and practical view, the very real difficulties we face in attempting to prove things about encryption algorithms...the significant aspects of the problem are mathematically non-linear and all such problems are very difficult. Finally, we are not here to deal with the specific threat of brute force methods of breaking encryption algorithms...this aspect has been adequately and competently dealt with in a previous workshop which investigated the practical aspects of constructing a hardware device which would rapidly perform the necessary computations required in this attack. We shall hear a report of the findings of this workshop.

We will proceed during the course of the afternoon with a number of presentations whose purpose is to familiarize us with the details of how the DES algorithm works and perhaps some aspects of analytical approaches to gaining information about its underlying structure. Tomorrow, we will break up into two working groups in order to explore in some detail two important areas of interest. The mathematics working group, headed by Dr. Howard Campaigne, will deal with the strictly mathematical aspects of the algorithm, especially from a cryptanalytic point of view. The applications working group, headed by Dr. Joseph Eachus, will deal with the very practical areas of key generation, usage, and distribution that are so important in the day-to-day use of an encryption scheme.

Following Professor Bigelow's introduction, Dr. Ruth Davis, Director of the Institute for Computer Sciences and Technology, welcomed the participants, thanked them for their participation and outlined briefly the history of the NBS involvement with the Data Encryption Standard, the purpose of the standard and the anticipated contribution of the workshop.

DAVIS: It has long been recognized that a publicly available encryption technique was needed to protect data as it is stored in a computer or transmitted from one computer to another. To this end NBS has been working on a data encryption standard since 1972. The purpose of the standard is to provide a uniform technique for all Federal agencies to use. It is not intended to be universally applied wherever data is stored or transmitted within the United States. In selecting a candidate for a standard, NBS twice solicited in the Federal Register and selected the algorithm that best satisfied the requirements of a standard from among those submitted. In establishing a standard, the encryption algorithm is not left in vacuo. It will be embedded in a framework of guidelines that recommend procedures and environments in which the algorithm is used as only one part of an overall security system. We are now working on developing such guidelines. We feel that the vulnerability of computer systems to risk has been, and will be more so in the future, substantively reduced by our efforts in this area.

A good deal of our work towards developing a standard was in conjunction with other Federal agencies who will be the actual users of the standards and guidelines that we produce. This work has been difficult and tedious, but necessary and rewarding because it keeps us in close contact with those who have the deepest, most abiding interest in the standard, and in using the standard in an efficient and cost effective way. Once a standard is established, we continually monitor its use by maintaining contact with the agencies. There is, as well, an automatic review proceedure at five year intervals which provides for the evaluation of the continued effectiveness and efficiency of a standard.

Dr. Dennis Branstad, of the Institute for Computer Sciences and Technology, described the proposed data encryption standard to the group.

BRANSTAD: (An overview of the cryptographic algorithm specified in the proposed Data Encryption Standard was made. Figures 1-3 were used to describe the iterative process of the DES algorithm and the structure of the substitution boxes in the enciphering function).

Figure 1 is a flow diagram of the sixteen iterations, or "rounds", of the algorithm. Sixty four bits of input are enciphered under control of the sixty four bit key (56 bits are actively used in the algorithm and 8 are used for error detection in the entered key) and a sixty four bit cipher is produced. The structure of the algorithm is such that half of the input is used to generate a pseudo-random 32-bit binary number which is exclusive-ored (XORed) with the other half. The halves are then switched and the operation repeated sixteen times. The input is preprocessed with an initial fixed permutation and the result is postprocessed with the inverse of the initial permutation before output. Use of the algorithm results in a 64-bit output in which every bit of the output depends on every bit of the input and every bit of the 56-bit active key.

Figure 2 shows the mathematical combining function F which uses the 32-bit right half of the input and a 48-bit subset of the 56-bit active key to produce a pseudo-random 32-bit binary number. The algorithm is structured so that neither the key nor the input are derivable from the output after the sixteen rounds are completed. The function E expands the 32-bit number to a 48-bit number by copying specified bits twice. The operation KS is a key selection of 48 bits from the active 56 bits. The bits are selected so that each of the 56 active bits are used between 12 and 15 times during the 16 rounds. The two 48-bit numbers are XORed together and the result enters the 8 substitution boxes (S boxes). The first 6 bits enter S1, the second 6 bits enter S2, etc. Each S box contains 64 entries of 4 bits each. The 6-bit entry is used as an index into the S box tables and the 4-bit quantity is substitued as output of the S box operation. The contents of each S box are different. Several different methods may be used in implementing the S boxes but they are described as tables having 4 rows and 16 columns. The eight 4-bit results are then permuted according to a fixed permutation P and the resulting 32-bit number is the pseudo-random number described in Figure 1.

Figure 3 shows a sample selection function (S box) and how the 6-bit input is used. The outer 2 bits are used as a row index and the inner 4 bits are used as a column index. The entries are shown as decimal numbers in the range 0-15 in each row.

Mr. Thomas Pyke, Chief of the Computer Systems Engineering Division in the Institute for Computer Sciences and Technology, detailed the events of a preceding workshop that dealt with hardware aspects of 'brute force' attacks on the DES algorithm. The results of this workshop, have been

published in the "Report of the 1976 Workshop on Estimation of Significant Advances in Computer Technology. " The details of Mr. Pyke's presentation are therefore omitted from this report. Following his presentation Mr. Pyke responded to several questions.

PYKE: Participation in the previous workshop was very broad-based, involving component, mainframe, and semiconductor manufacturers as well as individuals from academic environments and independent peripheral manufacturers. They represented a good cross-section of expertise. Trade organizations and professional societies were asked to participate by submitting nominations for participation. This was how the list of participants was developed.

Further discussion relating to Mr. Pyke's presentation is detailed in following sections.

Dr. Jason Gait, Institute for Computer Sciences and Technology, presented an introductory analysis of the structure of the algorithm.

GAIT: The DES algorithm is essentially a series-parallel connection of S-box operations. To analyze this structure, consider first an individual S-box. Each of the eight independent S-boxes is a 4x16 matrix, each row of which is a permutation of the integers 0-15. Before entry to any one S-box, six bits of data and six bits of key are XORed to produce a six bit result. Two bits of the result are used as a row index while the other four bits are used as a column index in the matrix. The corresponding S-box entry is the substitution "ciphertext. " An S-box transformation is not an invertible mapping (six bits map to four). It is also notable that brute force key searching requires the testing of several corresponding plaintext -ciphertext pairs. On the average 2.5 pairs must be tested to be certain that the 6-bit key is correct; the maximum number required is eight.

In the DES the S-boxes are used in parallel (Figure 4). Forty eight bits of plain and forty eight bits of key are XOR'd and the six bit segments are used to determine an independent S-box entry. The resulting 32 bits is the substitution "cipher. " Note again that the parallel connection is not invertible. The average number of plaintext-ciphertext pairs that must be tested per 48-bit key increases to four.

A single 'round' of the algorithm is based on this parallel connection (Figure 5). A round is set up to process 64-bit plaintext blocks and produce 64-bit ciphertext blocks. The difference between this and the parallel connection of S-boxes is mainly a question of data flow. The round is invertible. The average number of plaintext-ciphertext pairs that must be tested is still four.

A configuration of 16 rounds in series is the "guts" of the algorithm; the only significant difference is in the key schedule (Figure 6). This analysis model is based on a 768 bit key, each 48 bit segment is used as a key for one of the 16 rounds. This series configuration is invertible. The average number of corresponding plaintext-ciphertext pairs required to recover a key is still four.

One round of the DES as well as the complete sixteen rounds of the algorithm can be tested as pseudo-random number generators. A computation of the power spectrum of the results produces better than average randomness properties (Figure 7). The results of analyzing the output of the sixteen rounds show that it is a very good random number generator for many applications.

In the DES algorithm the beginning and ending permutations are now included with the previous configuration. The effect of the key schedule is that the 16 previous independent operations are no longer independent of one another. The number of plaintext-ciphertext pairs that must be tested to recover a key uniquely is unknown, but may well be larger than one. The statistical properties of the output in the complete algorithm, considered as a pseudorandom number generator, are substantially improved over the properties exhibited by the output of the sixteen independent-operation model.

Dr. Howard Campaigne briefly introduced the topic for the mathematics working group to meet the following day.

CAMPAIGNE: Our meeting tomorrow in the mathematics working group will have the purpose of trying to determine the strengths and weaknesses of the DES and to look at statistical and other methods of breaking the algorithm.

Mr. Stephen Kent, of the Massachusetts Institute of Technology, presented a variety of methods of using the DES in practical applications, the factors that would determine such use, and the advantages that accrue.

KENT: There are two basic methods of using the DES, each having certain advantages and disadvantages. The first is block mode, or "electronic code book" mode. In this mode 64 bits of data are encrypted at a time and each such 64-bit block is encrypted independent of any other block. The second method is cipher feedback mode in which normally a character at a time is encrypted by using the last 64 bits of cipher that were generated as input to the DES and using a number of the output bits to XOR with the character to produce the cipher. This cipher is used as input for the next encryption operation. Cipher feedback is most useful for character oriented communications or for the encryption of serial data for storage. Cipher feedback cannot be used to encrypt storage files that are to be randomly accessed. It cannot be used for encryption across packets in packet switching networks since decryption is serial dependent and packets often arrive out of order. Block mode is faster than cipher feedback, but cipher feedback is self synchronizing and provides message integrity.

Dr. Joseph Eachus described the areas of interest for the applications workshop that he would be heading the next day.

EACHUS: We will need to discuss keying control and distribution. We must assume that an adversary possesses all the characteristics that we do not want him to have, i. e., he is unscrupulous, resourceful, knowledgeable and shrewd. We must always keep in mind that the best means for an adversary to get the best return on his investment is not by using esoteric techniques of analysis to obtain encrypted information, but by using bribery and theft to obtain the required information. We must stress the profound importance of changing the key in any practical working encryption system.

Mr. Herbert Bright of Complan, Inc. presented his ideas on the implementation of the Data Encryption Standard and its usage.

BRIGHT: As we view it, the main problems are access control and audit trail generation. The major difficulty is that existing encryption systems are protected by what must charitably be regarded as trivial algorithms, or by no encryption at all. The obvious solution is to introduce protection by a strong encryption algorithm. But even at that, a strong algorithm isn't enough...the system itself must resist penetration. File protection requires that the key,

plaintext, and programs must be protected. The canonical threats are spoofing, misrouting, playback, interference, and cryptanalysis. We use a package of techniques including encryption methods, secret control algorithms, and priviliged mode.

3.2 Discussion

There was considerable give and take discussion during and following some of the presentations. To preserve the integrity of the presentations, this discussion is grouped together in this section. Following Mr. Pyke's presentation on the preceeding workshop concerning a hardware device to do 'brute force' key searching, the discussion was particularly wide ranging.

HELLMAN(Stanford University): Why was the IBM group that has done a good deal of analysis on the algorithm not consulted. It seems that their estimates of time frame, rate of key generation, and cost for building a key searching machine are significantly less than those that were evolved during the first workshop.

KONHEIM(IBM): IBM did estimate those costs, but we neglected to include the cost of development.

TUCHMAN(IBM): My personal opinion is that if IBM were to build such a key searching machine consisting of a million special purpose chips, the development and production costs alone would result in a cost to the manufacturer an order of magnitude larger than the 20 million dollar figure that was estimated by Martin Hellman. The resulting machine would produce one key a day but would not be delivered before 1981 and the probability of success would be very low. IBM has no intention of building such a machine and I do not believe anyone would attempt to build such a machine.

DAVIS: It should be noted that the hardware workshop results were based on scenarios that were judged to be most favorable for the penetrator, i. e., minimize cost and time simultaneously.

HELLMAN: Regarding the brute force method and neglecting I/O considerations, the computer time required to perform calculations has been decreasing by a factor of ten every five years. It doesn't seem that technological factors of this kind were reflected in the first workshop.

BIGELOW: They were.

SEDELOW(NSF): May we have some clarification on the export control and licensing problem as it relates to the DES.

DAVIS: Export control and licensing were not explicitly specified in the requirements for a DES.

BRIGHT: We should keep in mind that the figures determined in the first workshop were based on the worst possible case of assuming the key remains constant for a long period of time. If the user has the ability to alter the key, then these figures do not accurately reflect the magnitude of the brute force method. The costs must include obtaining matched plain and cipher every time the key is changed.

HELLMAN: Assuming that it takes 12 hours to find one key by exhaustive search, even if the key were changed every hour, it would be possible to recover one key during the first hour on the average every 12 days.

KAHN(New York University): Is it permitted to export the DES?

DAVIS: That question is handled through the State Department and the Munitions Control Board.

A particularly important issue was raised during Dr. Gait's presentation, to which much subsequent attention was devoted.

SLOAN(Bell Labs): It looks like the S-boxes are constructed rather than randomly generated.

BIGELOW: There is nothing unique about the particular S-boxes used in the algorithm, there are many other possible choices.

TUCHMAN: The S-boxes are certainly not randomly generated, but were deliberately selected according to criteria that strengthen cryptographic effectiveness. From a large set of such cryptographically effective S-boxes, IBM selected the ones which had the smallest minimal combinatorial circuit realization of those tested so they could be efficiently implemented on a chip.

SLOAN: Why are the permutations not random.

GAIT: It appears that the initial and final permutations were selected to facilitate byte-wise manipulation of data on the chip; in particular, IO takes place efficiently eight bits at a time.

SCANTLIN(Lexar, Inc.): Is it possible that the group be informed of how the S-boxes were chosen.

TUCHMAN: When we attempted to get the algorithm approved for export, we discovered that we had inadvertently utilized classified design principles. IBM has been requested by the National Security Agency not to divulge these principles.

HELLMAN: The important N. Y.-Washington link will not be using the DES for protection, but will use a special NSA supplied algorithm. This seems to indicate that the DES is unsatisfactory.

DAVIS: The DES will be used to protect areas where previously there had been no protection at all.

DEAVOURS: Does NBS plan to adopt a standard whose design principles are kept secret?

BIGELOW: It doesn't seem that the design principles are relevant, since the algorithm itself is fully specified.

TUCHMAN: IBM has spent 17 man years of effort in analyzing the DES and has employed a number of outside consultants. These efforts failed to find any cryptanalytic shortcuts.

KAHN: Why not pick the S-boxes out of a hat?

TUCHMAN: The method used produces a stronger algorithm.

SCANTLIN: Our company is a potential user of the algorithm for transactions involving the transfer of large sums of money. We feel we have an interest in the strength of the algorithm. While it is true that the algorithm is completely specified, we feel it would be prudent to evaluate the algorithm objectively in order to get an idea of its strength. We feel we know how the algorithm works, but not why it works. Our own work on the algorithm shows that we can reduce the exhaustive search time by a factor of two and we feel that this indicates potential for future reduction as well. We are disturbed by the potential the S-boxes possess for concealing a trap door and the more we carry forward our own analysis, the more uneasy we become.

4. CONTINUATION OF INTRODUCTORY SESSION, SEPTEMBER 22

On the morning of September 22, the introductory session continued with a formal presentation by Dr. Hellman of Stanford University and additional discussion before breaking up into working groups.

4.1 Summary of Formal Presentation

HELLMAN: We seem to have agreed that a 64-bit key is better than a 56-bit key, but this still is not enough. I have attempted to communicate my concern in this area to NBS for some time, but they have paid no attention. The design structure of the DES should have no secret aspects. All these principles must be known so the level of security offered can be objectively assessed. We must have a public disclosure of the other algorithms that were submitted. If this is to be a public algorithm, we must have an objective statement of its strength or lack of strength. It is clear that NSA has a vested interest in imposing a weak algorithm. I cannot but disagree profoundly with the conclusions of the previous workshop. I think brute force key extraction is practical now. If an analytical attack reduces the key by as few as 5-10 bits, extraction of key by exhaustion is then trivial. It is questionable whether NSA would use such a short key and it is known that NSA systematically blocks the use of algorithms using longer keys. We feel there is no technical difficulty in increasing the key length substantially. We cannot accept the necessity for the initial and final permutations in the algorithm and in the key schedule since they slow down software implementations. I have information that, while IBM designed the algorithm, the key size was set by NSA. The problem of public disclosure is a political one. NBS should have stated that the key size could not be justified technically. It is absolutely imperative that the underlying design principles be published.

4.2 Discussion

The discussion following the Hellman presentation was prolonged and wide ranging.

BLANC(NBS): There doesn't appear to be a scientific basis for the attacks on the algorithm. Hellman is concerned with political issues.

JEFFERY(NBS): The concerns that have been expressed are certainly interesting. Hellman is scared to death of NSA influence. But it is improper to assume impropriety where there is no evidence. If there is something wrong with the S-boxes, please tell us so. That's why we're here.

BIGELOW: We need to objectively evaluate the risk factors involved. As I see it, there are three: the risk that the key can be extracted by brute force, the risk that the algorithm can be broken analytically, and the risk that the algorithm has been designed with a trap door. All objective evidence indicates that it is at present impractical to extract keys by force. There is no way we can prove that the algorithm cannot be broken analytically. Entertaining the idea of a trap door seems to me foolish.

BRIGHT: A standard is not immutable and can always be changed later.

SLOAN: The design of the S-boxes is not acceptable. They should be randomly generated.

MORRIS(Bell Labs): I take sharp issue with my colleague, Mr. Sloan. I feel that well designed S-boxes must be significantly better than randomly generated ones. It appears that we know of no feasible attack on the algorithm. Under the circumstances, the algorithm is probably the best that can be devised. But in case someone shoots it down, we should be working on a better one. I am shocked by the reluctance to talk about the design of the S-boxes. I feel that this information should be released. I feel that irrelevant parts of the algorithm should be removed in future designs. I would like to suggest that the present algorithm can be used in much more secure ways, for instance cascading, which doubles the effective key.

TUCHMAN: The algorithm as published is precisely what IBM submitted. The responsibility for the algorithm rests solely with IBM, not with NSA, and certainly not with NBS. We analyzed the algorithm extensively, and found no short cuts at all. The purpose of the structure in the S-boxes is to make a stronger algorithm. It is only an accident that NSA has an interest in keeping the design principles secret. There is no collusion.

DIFFIE(Stanford University): How can we have a FIPS standard based on classified design principles?

HELLMAN: We have brought up many questions. When will they be addressed? I am prepared to agree that the DES is probably the best standard that could be promulgated at the present time. But I feel it necessary that the classified material involved be declassified.

SCANTLIN: I would like to review with you the work that we have done privately on the algorithm. It is clear that the S-boxes are critical to the strength of the algorithm. There are many choices of S-boxes that would certainly result in a weak algorithm and it is by no means clear that the present choice is not weak. The strong potential of a trap door puts us in the place of an antagonist. Since important information was withheld, we tried to evaluate the strength of the algorithm. The results were not reassuring. The NBS position is that the algorithm resists all attacks except brute force, but we are able to reduce the work by a factor of two using analytical methods and we see much potential for further reduction. We are concerned about possible trap doors and about the short key. We feel that a standard must be completely visible. We also feel that IBM is placed at an advantage in producing the chip because it is keeping the design secret. We do not think this is proper for a standard.

BIGELOW: You seem to be operating under the hypothesis of intentional fraud. This is hardly possible. All parts of the algorithm have been made completely public and all have an equal chance at analysis. Each manufacturer can design the chip as he sees fit. There is no advantage to IBM. Your report does not direct itself to any significant attack on the algorithm, but merely shows that simple minded things don't work. The DES is not intended to offer perfect security. A larger and more complex DES could include trap doors.

HELLMAN: IBM should publish the attacks they made on the DES and the results they obtained.

BRIGHT: We would have avoided a lot of trouble if the S-boxes had been randomly generated, but short random sequences have trap doors of their own. We need public disclosure of the design principles. The DES would be useful now and is in the public interest. It is inadvisable to delay public availability. The present DES can be used intelligently to enhance security. Meanwhile work can proceed to develop a stronger standard.

SLOAN: I would like to record my suspicions about the regularity in the structure. This is not an acceptable design. I recommend that the S-boxes be randomly generated.

BRIGHT: Random S-boxes don't necessarily make a better algorithm.

MORRIS: I feel that the deterministic design of the S-boxes is fine. I don't feel that the key size is as bad as it sounds. Cascading two chips is very secure. But I am disturbed by the secret design in the S-boxes and I feel this secrecy gives IBM a manufacturing advantage.

5. REPORT ON THE MATHEMATICS WORKING GROUP

The objectives of the mathematics working group, chaired by Dr. Campaigne, were to provide definitions of important terms, to provide a forum for the analysis of the DES from the point of view of mathematical attacks, and to evaluate the relative resistence to cryptanalytic attack of various ways of using the DES.

KONHEIM: I wonder if anyone actually has a concrete idea of how to attack the algorithm. Assume that you are provided with virtually unlimited plaintext and corresponding ciphertext. Can you devise a way of recovering the key? Can you invent a viable method of attack against the algorithm?

TUCHMAN: These ideas have been around for years, the algorithm has been around for years. As far as I know nobody has ever got anywhere with the problem.

SNOW(Mitre Corporation): I would like to propose a method that might get us somewhere. The idea is based on the fact that it is surely easier to break into an eight round DES than it is to break the full sixteen rounds. What I suggest is simultaneously working forward and backward, meeting at the half-way point. One assumes a value for the key and compares the two resulting ciphertexts. The assumption is that if the assumed key is 'close' to the true key, then the two ciphertexts will also be 'close'. It isn't clear to me how to formalize this. It just seems to me that after only eight rounds the confusion effect hasn't had time to really take effect yet.

HELLMAN: I would call this a 'key clustering' attack. I don't see how it buys you more than one bit.

TUCHMAN: We tried something very much like it and it doesn't work. In fact we tried a lot of things for a long time, until we were collectively frustrated. I wish you all would work on this problem until you shared our frustration. Get all this out of your system.

HELLMAN: Even if the attack worked, it would be very easy to defend against. It's only necessary to double the number of rounds in order to give the confusion effect time to work. I would like to know why IBM hasn't published its attacks? Are all IBM's attacks classified?

TUCHMAN: Yes, they are. NSA has asked us not to release the details of any attack that we tried.

SCANTLIN: Once this algorithm actually becomes a standard, the economic value of breaking it will be very much higher than it is now. I don't see how it can stand up for long when there are millions of dollars at stake. There will be real economic advantage to breaking it.

HELLMAN: It's particularly disturbing to me when some individual at NBS or IBM does a piece of research on the algorithm only to have NSA come along and not allow it to be published.

SCANTLIN: When my customers use encryption, they use a particular key for as long as a month. Furthermore, it's effectively a much shorter key than 56 bits because the average user will just enter printable characters as a key, which is equivalent to only 48 bits of key. This is a human nature problem and the average user is just not sophisticated enough to do it differently.

KONHEIM: We make sure that our customers understand the rationale of key selection and we make sure they know how to enter a proper key. We educate them. When we get through with them, if they're still dumb enough to use their wives' names for a key, it's their fault.

HELLMAN: MULTICS has a particularly sensible key generating scheme that obviates some of these problems. They generate keys with the same digraph frequencies as English so the keys are easy to remember but not easy to guess. What I still want to know is this: what are the actual costs of going to a larger key?

CAMPAIGNE: There is no real limitation on the size of the key. The fact that the key comes in 64 bit blocks is essentially irrelevant.

JEFFERY: During the last workshop we got some information on this. In particular, Motorola indicated that a 10 percent increase in the complexity of the chip would probably delay their production of the chip by about two years. They felt strongly that it would be impractical for them to use a larger key. Moreover, Collins Radio has said that if the key size is increased, then they will be unable to produce their high-speed chip at all.

SCANTLIN: That Collins chip is too big. Nobody makes 300 mil chips anymore. The real question is what percentage of the chip is required for the key registers.

JEFFERY: We need a definition of what an adequate defense against a threat means. To any threat less than 50 million dollars, the 56 bit key seems to be adequate. For a threat larger than 50 million dollars, the 56 bit key is perhaps not adequate. It depends on the threat.

MORRIS: Can we not say now that the DES algorithm will adequately protect any realistic business or private information for some reasonable number of years? Can we not further say that we do not know of any reasonable attacks on the algorithm at the present time or of any attacks that will be reasonable for the near future?

BIGELOW: We need to remember too that an encryption device is itself just one part of a larger system, and that security depends on the entire system.

JEFFERY: The standard specifically outlines the kind of risk analysis that is necessary to evaluate the effectiveness of encryption in the entire security system.

SEDELOW: Another factor is that traditional mercenary motives may not be the only motives that would lead one to break the cipher.

SNOW: Getting back to the main problem, if we cascade two or more chips in series, won't that eliminate the difficulty with the 56 bit key? This effectively doubles the key size.

MORRIS: I think that is the answer we have been getting at all along.

HELLMAN: There is still the problem of not having a satisfactory answer for the S-boxes. I don't see how this information about the S-boxes can remain secret and still have a standard. I think that NSA and IBM should publish the secret information about the S-boxes and also publish the attacks they tried that didn't work. I also feel strongly that the permutations should be dropped from the standard...I gather the chip won't have to be redesigned and it makes a software implementation practical. Removing the permutations does not hurt the strength of the algorithm.

6. REPORT ON THE APPLICATIONS WORKING GROUP

Dr. Eachus suggested that the following five objectives be considered during the applications working session:

1. Evaluate alternative key distribution schemes, both for communications and for data storage.

2. Evaluate the cost effectiveness of various modes of using the DES.

3. Identify the practical aspects of using an encryption algorithm, e. g., how often is it practical to change the key.

4. Identify and evaluate guidelines for the practical use of cryptography in the general security context.

5. Evaluate the practicality of various alternative modes of using the DES.

BARNES(Burroughs): I would like to raise the following questions about using the cipher feedback mode:

1. What are the implications of the data containing long sequences of all zeroes? In that case you are providing an interceptor both ciphertext and the corresponding plaintext.

2. It is going to be hard to avoid cases of double (super) encryption and , if it happens, will it cause any problems?

BRANSTAD: The first question is equivalent to asking the security of the DES against the known plain text attack and we have stated that only testing of all possible keys will guarantee obtaining the key in this case. In the

second case, double encryption is possible with this algorithm as the decryption process is different from the encryption process. For algorithms not having this characteristic, encrypting twice results in plaintext and not encrypted ciphertext.

EACHUS: Due to our limited time, I suggest that we limit our discussion to the use of the DES in communications. The topic of key generation and distribution needs to be discussed for this application.

KENT: The key should be suitably recorded on some storage medium such as a magnetic striped card and the user must present the card as well as some identifying personal characteristic in order to gain computer access.

EACHUS: A practical means of entering a key at a terminal is needed.

DeLUCAS: We may have 100-200 people using each communication line and we have to know how to handle the key or keys in this situtation.

KENT: A multiplexed device can be used if the line has cipher produced with multiple keys. One device will suffice if the data is multiplexed before it is enciphered.

BRIGHT: It is important to protect the key in the system at the highest level of protection available.

DeLUCAS: How do you get new keys to 500 terminals?

KENT: A multiple level key distribution system is best. A new key is either built from several independent keys or distributed under the protection of a key distributed outside the communication system that is being protected.

CHRISTENSEN (Honeywell): You can use a security officer's key to encrypt or decrypt the user's key.

KENT: Whit Diffie has published a paper on a public key distribution system.

BRANSTAD: A public key distribution system would reduce the cost of key distribution. His scheme, however, requires an encryption algorithm with very special properties. Diffie suggested an algorithm similar to the square function having an inverse square-root function. One is easy to compute and the other is relatively difficult. He hasn't developed a usable function yet. The DES algorithm does not satisfy the needed criteria.

EACHUS: Can the U. S. Mail be used to distribute keys?

KENT: The Mail can be used to carry SECRET documents and should be able to be used for keys.

DeLUCAS: A book of keys should be generated and distributed for use.

BRIGHT: The book had better be protected.

KENT: People should not have to remember their keys. A simpler system is needed.

GLUCK (Burroughs): Multi-level keys or complex keys must be the answer.

EACHUS: Two physical methods of distribution should be used, e. g., courier and the mail service.

DeLUCAS: Government users need more information on the application and use of the algorithm.

CHRISTENSEN: Follow on standards are needed for communications based on the DES.

EACHUS: NBS should publish guidelines for computer systems security and use of the DES, including the necessary protocols and key management.

BRANSTAD: We are doing that. However, we do not know at what level of detail these guidelines should describe key generation and distribution. If they are too specific, potential penetrators can track your methods, especially once one key is compromised, lost or stolen. In addition, the frequency of change depends on many parameters which are peculiar to individual systems. There are no simple rules to follow.

EACHUS: Two part keys would add to the protection.

DeLUCAS: It appears that keys should be cycled over a period of time. Each line should have a separate key. However, this may cause a lot of problems at regional data processing centers where all the keys must be handled and protected.

BRANSTAD: How do you give practical guidelines that are universally applicable?

KENT: Probably by giving rules for computing frequency of change based on cost and time.

BRANSTAD: Thats the approach we are using. We are attempting to analyze these factors as well as risks to provide such guidance.

BRIGHT: One probably needs some real-time computational capability at the terminal to assist in key computation.

CHRISTENSEN: Examples of key distribution systems are needed based on these parameters as well as the size of the system or network. Large systems are quite different than small systems.

GLUCK: People must always realize that you must have a secure key in order to distribute other keys.

BRIGHT: Encryption applications for protecting stored data will require different ways of supplying keys. In addition, if a key is lost that is protecting stored data, the data is also effectively lost. If the key is destroyed during communication, it is immediately obvious.

EACHUS: It is obvious that key distribution and protection must be given great consideration before designing a cryptographic system. It is also obvious that protection of the key against pragmatic threats is of utmost concern and must be given highest priority. I also feel that guidance that is too specific can be used incorrectly by the unwary and unknowing user. Thank you for your contributions at this working session.

7. THE SUMMARY SESSION

On the afternoon of September 22, the working groups completed their discussions and the entire group met for a summary and evaluation of what had occurred, including further discussion.

Dr. Eachus summarized the consensus of the applications working group as follows:

*Highest priority must be given to protecting the keys within a system, both to deny unauthorized access to the

keys and to assure authorized access to keys used for long term retention of encrypted data.

* It is essential that some element of the key be distributed to remote locations by a process which is outside the system that is being cryptographically protected.

* More than one level of key management is acceptable and in some cases, necessary. The multi-level key management system may take the form of super encipherment (i. e., encrypting more than once) or of a complex generation (i. e., separate components of the actual key are combined only when the actual key is needed at the place the key is needed).

* It is not advisable that NBS publish guidelines which specifically describe key generation and use.

* It is not advisable that a single key be used for all stations in a multi-station cryptographic system.

* It is important that key distribution methods be considered before installing crytographic devices.

* Communication encipherment and file encipherment will require different key management. It is desirable that keys used for communications be destroyed when the communications they are protecting terminate. Files may have a long term use or a multi-use lifetime in which the key must be accessible throughout.

* The physical means of inserting a key into a DES device is of high importance. It can have a profound effect on the process of generating and distributing the keys. The experiences of credit card companies should be utilized when considering generation and distribution systems.

* Costs of generating and distributing keys should be estimated before a cryptographic system is designed or procured.

* Key distribution systems will depend on the size, complexity and topology of the crytographic system. Problems in large systems will differ from those in small systems.

Dr. Campaigne summarized the consensus of the mathematics working group as follows:

* The key and the protection of the key is the most important security consideration when using the DES algorithm.

* The 56-bit key is acceptable but a 64-bit key would have been better. A 48-bit key would have been unacceptable as

the basis of a standard encryption algorithm.

* The cost of expanding the algorithm to a 64-bit key is too high for most applications, is not necessary at this time, and delaying the standard for this reason is not warranted. The algorithm may be used two or three times if security warrants it for special applications.

* NBS should publish key usage guidelines, including using the key twice in sequential encryptions (or three or more times).

* The scenario of brute force key extraction should be publicly described and anticipated return-on-investment should be computed by users.

* Analysis of the DES algorithm should continue.

* One analysis scheme suggested was to partially encipher the plaintext and partially decipher the ciphertext and correlate the intermediate results.

* Use of more than one key sequentially with the algorithm wouldn't weaken the process.

* Independent evaluations of the algorithm are needed.

*No one could show lack of security provided by the algorithm.

* The algorithm was acceptable for business applications and non-military government applications.

Following these summaries of the working groups, the following discussion ensued:

SEDELOW: The record should show that although the consensus of the mathematics working group was that a 56-bit key was adequate, there were members who vigorously opposed the 56-bit key as being inadequate.

SPIRA: Most of those not satisfied with 56 bits would have been satisfied with 64 bits.

BIGELOW: The consensus was that the maximum amount of information should be made available on the kinds of tests which failed to break the DES. A list of such tests would increase the confidence in the DES. This list should include a description of the tests, the level of effort expended and why they failed.

HELLMAN: The group discussed whether or not a FIPS standard should contain undisclosed information.

BLANC: The group could find no properties of the S boxes that compromised security nor were there any presentations of properties that could be added to the S boxes to increase their security.

MORRIS: The context of adequacy is very important...the algorithm may be adequate for business applications but perhaps not adequate for military or political applications.

BIGELOW: The DES is recommended for non-military applications of economic or social importance which do not represent a national threat.

HELLMAN: Another important factor is the potential delay of the standard if any alternative would result in a very long delay in its promulgation. It should be stated for the record that there was a serious discussion on key length.

DAVIS: This kind of precision in risk analysis for security is unprecedented. NBS has been involved in developing guidelines for risk assessment for some time and has been unable to specify such precision in related security matters. NBS will attempt to include such considerations in the guidelines that will accompany the publication of the DES.

HELLMAN: Work should be proceeding at the present time toward developing a subsequent encryption standard even if the present standard is adopted.

SEDELOW: The international economic warfare scenario should not be overlooked in any analysis involving the recommended use of the DES.

BIGELOW: This scenario is very difficult to quantify now or in the future since economic warfare presents such a large and varied threat. In any case, cryptography should not be the only method of protection in this scenario. Such an issue should be directed to the national security community for analysis and recommendations.

DeLUCAS: Does NBS intend to have another workshop before the standard is adopted which is directed towards Government agencies who are planning to use the DES?

DAVIS: The DES has already been formally coordinated within the Federal Government according to the Federal standards making process. In addition, NBS is conducting many workshops such as this because of the wide spread interest in the DES, because of the lack of general familiarity with cryptography, and because of some special aspects of mathematics and technology relating to the proposed standard. NBS does not intend to repeat the process which should already have informed Government agencies of the proposed standard. However we are now working with individual agencies and will continue to work with and assist them with their implementations. This is part of the responsibility of NBS under the Brooks Act and is not part of the standards making process. In addition, NBS will continue its efforts in making technical information and guidance available to Federal agencies, both through formal guidelines on implementing and using the DES and through Government-wide conferences and workshops on computer security and the DES.

BRIGHT: It is very surprising and disappointing that some general mathematical principles that were independently discovered cannot be published.

SCANTLIN: Will this information ever be made available to the public.

DAVIS: Some of the suggestions that have been made and questions asked can not be responded to or answered by NBS. Some are outside the scope or knowledge of NBS. However, for those that are technically or managerally within the responsibility of NBS, we will provide public responses. Those outside our purview, we will forward to the agencies involved.

HELLMAN: It is disturbing that IBM will not provide reasons for doing things in a certain way, e. g., why LSI implementation, why minimize the logic functions implementing the S boxes, why the initial permutation and its inverse. This lack of information places them in a competitive advantage and a full disclosure of the design and implementation principles should be required.

MORRIS: The suggested conclusions made during the morning session should be placed in the record. The points that surfaced during the working session make one more comfortable regarding the DES. There are ways of using the DES that can make it secure enough for any conceivable business transaction. NBS should publish guidelines for key entry

and key generation. Care should be taken to prevent people who use the standard from using it in such a way that the security of the algorithm is reduced, i. e., an effective key length of 42 or 48 bits. Use of the algorithm without cascading (i. e., multiple use of the DES) provides adequate security for business purposes against compromise by people and organizations with purely economic motives. However, it is not secure against those with political or military aims.

The alternatives that NBS might consider for support statements may be outlined:

* NBS and its advisors know of no attack against the DES.

* NBS and its advisors know of no attack against the DES other than trying all possible keys.

* NBS and its advisors believe there is no feasible attack against the DES.

* NBS and its advisors feel that this code was the best devised within existing constraints and that these are reasonable.

DIFFIE: It is a serious question whether a FIPS should be adopted that was based on non-disclosed information.

BRIGHT: In view of the extensive public exposure and examination that the DES had received as compared to other FIPS, the group is engaging in overkill with regard to their concerns.

HELLMAN: Overkill in this standard will make it clear to the people who come up with the next standard that more attention should be devoted to standards. Next time around, NBS should not only go to NSA for advice but to others as well.

BIGELOW: NBS solicited publicly for algorithms and related information over a year and a half period. The selected algorithm was published twice for public comment as well as for formal Federal comment.

This discussion concluded the formal content of the workshop. Dr. Davis closed proceedings by expressing her thanks to the participants for their cooperation.

8. APPENDICES

8.1 Workshop Syllabus

I. BACKGROUND

DATA ENCRYPTION

The Institute for Computer Sciences and Technology (ICST) of the National Bureau of Standards has recommended data encryption as the preferred method for providing protection against unauthorized access to data in transit within computer networks or in selected instances when data is resident within computer system data banks. The ICST has recommended a data encryption standard (commonly known as DES) as a satisfactory, uniform, cost-effective way to achieve the needed ADP data protection by Federal agencies outside the National Security Community.

The basis for the data encryption standard is a data encryption algorithm. The requirements NBS levied for acceptable encryption algorithms included the following:

- *They must be completely specified and unambiguous.*
- *They must provide a known level of protection, normally expressed in length of time or number of operations required to recover the key in terms of the perceived threat.*
- *They must have methods of protection based only on the secrecy of the key and not on the secrecy of the algorithm.*
- *They must not be discriminatory against any user or supplier.*

SCIENTIFIC EXPERTISE IN CRYPTOGRAPHY

There is little specialized expertise in cryptography in the academic or industrial communities. Within the government, the expertise is almost totally resident within the National Security Agency (NSA). NBS (ICST) recognized in 1971 both the emergent need for data security and the lack of scientific resources in the academia and industry available for its development of encryption procedures.

NBS embarked on two courses simultaneously; namely, 1) to utilize the most highly competent existing scientific and technical resources available, and 2) to promote as rapidly as possible a receptive environment for developing cryptographic technology appropriate for the public sector. Two solicitations for a data encryption algorithm were made in 1973 and 1974. Recognizing that NSA is the national communications security authority, we accordingly asked for and received assistance from NSA in evaluating these algorithms. Only one was assessed as acceptable for protection of privileged government information. This algorithm then formed the basis for the proposed Data Encryption Standard which was published for comment in 1975 prior to its being officially submitted for adoption as a Federal standard. The standard has not yet been officially submitted.

THE ACADEMIC AND INDUSTRIAL COMMUNITIES

Scientific knowledge and skills in cryptography which can provide the foundation for data encryption capabilities is limited. The best information available shows fewer than 50 cryptographic researchers outside NSA--about 35 are in universities; the remainder in industrial laboratories. NBS believes it is cognizant of these researchers and their relevant scientific activities.

The establishment of professional societies is a traditional and accurate indicator of the existence of a growing and potentially viable profession or scientific discipline. There are no such societies in the field of cryptography--or in the closely-related disciplines. The American Cryptogram Association, although active and well-accepted by its members would probably not be called a professional society. Therefore, NBS had no professional society to call upon in its technical development leading up to a data encryption standard.

In an informal search for colleges or universities with courses in cryptology, some four or five were identified. An exact identification of academic interest was difficult since some institutions gave relevant courses only intermittently. Courses given were solid but elementary: institutions giving such courses included Eastern Tennessee State University, Albion University, University of Arizona and the University of Georgia.

As one might expect from these findings, only elementary textbooks exist, no centers of excellence exist and no scientific breakthroughs or major achievements were found in this informal search for scientific and technical competence.

THE AVAILABILITY OF CRYPTOGRAPHIC TECHNOLOGIES

The technologies associated with cryptography can be loosely but usefully separated into four major clusters, namely:

- *Mathematical and statistical aspects,*
- *Engineering aspects of designing and constructing encryption/decryption devices and their host systems and networks,*
- *Associated protection measures integral to the employment of data encryption, and*
- *The technical and administrative management technologies leading to optimal use of data encryption procedures; key management; administrative security procedures; and monitoring, evaluating and auditing encryption performance.*

NBS has attempted to provide to the public domain, without affecting National Security, government expertise and guidance in the proper application of cryptography as an aid in the protection of information, the maintenance of privacy and the prevention of computer abuse.

NBS recognized in 1971 that the lack of any market for data encryption (outside the National Security Community) would severely constrain industrial motivation to develop additional expertise. Similarly, we knew that the long history of disinterest, the lack of formal academic structure and the almost non-existent supply of teachers would severely dampen academic motivation.

Indeed, the development of technology has been slow. The major constructive changes to data are exemplified by:

- *The development of product lines of encryption devices incorporating the proposed NBS data encryption standard by a number of commercial vendors,*

- *The increasing number of scientific and technical papers on the several technologies associated with cryptography which are being presented at professional meetings,*

- *The development by the Federal Reserve Board of a specification for a cryptographic device using DES to secure the data links of the Federal Reserve Communications System, and*

- *The dynamic and responsible efforts by associations and organizations such as the American Banking Association, and the National Retail Merchants Association to implement the proposed NBS data encryption standard and to accelerate the development of the needed cryptographic technologies within their own constituencies.*

II. RATIONALE FOR THIS WORKSHOP

In order to take advantage of expertise in academia and industry, NBS is sponsoring two workshops in the summer/autumn of 1976.

The first is concerned with the engineering aspects of encryption and is entitled:

> *"The 1976 Workshop on Estimation of Significant Advances in Computer Technology"*

The second workshop is the one to which this paper is addressed, namely:

- *"The NBS Workshop on Cryptography in Support of Computer Security"*

III. SPECIFIC WORKSHOP OBJECTIVES

Specific objectives of this Workshop within its general setting of the mathematical and statistical aspects of cryptography include:

A. Considerations of questions directly related to the analysis of the proposed NBS Data Encryption Standard, such as:

1. Factors in determining the "strength" of an encryption algorithm.

2. Possible "less than exhaustion" attacks on the DES encryption algorithm.

3. Formal proofs of the strength or security of the DES encryption algorithm.

4. Applicability of the method of exhaustion for keying variable recovery.

B. Consideration of questions about the effectiveness of DES in providing security protection, such as:

1. Effectiveness of electronic codebook mode.

2. Effectiveness of cipher feedback mode.

C. Consideration of questions related to keying variable control and distribution, such as:

1. Electronic keying variable distribution.

2. Error detection provided for in keying variable.

3. Generation of keying variables.

D. Consideration of the feasibility of producing cryptographic guidelines to aid in the understanding and application of DES.

IV. WORKSHOP PRODUCT

The technical product of the Workshop will be a report on topics treated in the Workshop to be written in an agreed-upon format and distributed to all Workshop participants.

Dependent upon Workshop members' suggestions or constraints, the Workshop report will be produced by NBS (ICST) and made available to interested parties.

The Workshop proceedings will be used as a significant and recognized contribution to NBS' activities in providing data protection through encryption.

V. WORKSHOP ARRANGEMENTS

1. The Workshop will be held at NBS, Gaithersburg, Maryland, on September 21-22, 1976 in the 10th Floor Conference Room, Administration Building.

2. The Chairman will be Mr. Julian Bigelow, Institute for Advanced Studies, Princeton, New Jersey.

8.2 Workshop Agenda

AGENDA

Tuesday, September 21, 1976

1:15 p.m.	*Introduction*	*Mr. Julian Bigelow*
	Welcoming Remarks	*Dr. Ruth M. Davis*
	Description of Proposed Data Encryption Algorithm	*Dr. Dennis Branstad*
	Report of "Architecture Workshop"	*Mr. Thomas Pyke*
	Introductory analysis of proposed DES	*Dr. Jason Gait*
3:00 p.m.	*COFFEE*	
3:30 p.m.	*Introduction to Workshop Topics*	*Mr. Julian Bigelow*
	1. Analysis of proposed DES	*Dr. Howard Campaigne*
	2. Effectiveness of DES in different modes	*Mr. Steven Kent*
	3. Keying control and distribution	*Dr. Joseph Eachus*
	4. DES implementation and usage	*Mr. Herbert Bright*
4:45 p.m.	*Organization of working groups*	
5:00 p.m.	*End of first day*	

Wednesday, September 22, 1976

9:00 a.m.	*COFFEE*	
9:30 a.m.	*Meet in working groups*	
12:00 noon	*Lunch*	
1:00 p.m.	*Working Group Reports*	
2:30 p.m.	*Summary statements*	*Dr. Ruth M. Davis* *Mr. Julian Bigelow*

8.3 Workshop Participants

Mr. Julian Bigelow
Institute for Advanced Study
Princeton, New Jersey 08540

(609) 924-0945

Walter Carlson
NAS/NCR Evaluation Panel
Bldg. 029, 5600 Cattle Rd.
San Jose, California 95193

(408) 997-4081

JoAnn Christensen
Honeywell Information Systems
P. O. Box 6000
Phoenix, Arizona 85005

(602) 995-3432

Alan Konheim
IBM Research Center
P. O. Box 218
Yorktown Heights, New York 10598

(914) 945-1715

Walter Tuchman
IBM (Kingston Dev. Lab)
Neighborhood Rd., D69L
Kingston, New York 12498

(914) 383-3124

Herbert A. Robinson
Applied Math Division
National Bureau of Standards
U. S. Department of Commerce
Washington, D. C. 20234

(301) 921-2631

7. *Russell A. Kirsch*
Applied Math Division
National Bureau of Standards
U. S. Department of Commerce
Washington, D. C. 20234

(301) 921-2337

8. *Phil Spira*
Systems Control, Inc.
1801 Page Mill Road
Palo Alto, California 94304

(415) 494-1165

9. *Walter Sedelow*
National Science Foundation
1800 G Street, N. W.
Washington, D. C. 20550

(202) 632-5743

10. *John R. Scantlin*
Lexar Corporation
11611 San Vicente Blvd.
Los Angeles, California 90049

(213) 826-6521

11. *Jason Gait*
Institute for Computer Sciences and Technology
National Bureau of Standards
U.S. Department of Commerce
Washington, D. C. 20234

(301) 921-3862

12. *Martin Hellman*
Stanford University
Durand 135
Stanford, California 94305

(415) 497-4002

13. Whit Diffie
Stanford University
Durand 137
Stanford, California 94705

(415) 497-4533

14. Bernard J. Pankowski
Computer Sciences Corp.
6565 Arlington Blvd.
Falls Church, Virginia 22046

(703) 533-8877

15. Stephen T. Kent
M.I.T. Lab for Computer Science
M.I.T. L.C.S.
545 Technology Square
Cambridge, Massachusette 02139

(617) 253-6037

16. David W. Snow
The Mitre Corp.
P.O. Box 208
Bedford, Massachusetts 01793

(617) 271-2061

17. David Kahn
Windsor Gate
Great Neck, New York 11020

(516) 487-7181

18. Frank Secretan
Collins
4311 Jamboree Road
Newport Beach, California 92663

(714) 833-4717

19. John C. DeLucas
Veterans Administration
810 Vermont Avenue, N. W.
Washington, D. C.
Mail Code 28A3

(202) 389-3891

20. Cipher Deavours
Kean College
41 Central Park West
New York City, New York 10023

(212) 595-8091

21. Aaron D. Wyner
Bell Telephone Laboratories
Murray Hill, New Jersey 07974

(201) 582-2916

22. R. Studley
House Information Systems
House Annex #2
Washington, D. C. 20515

(202) 225-0223

23. Robert Krell
Director's Office
National Bureau of Standards
A1011, Administration Bldg.
Washington, D. C. 20234

(301) 921-3136

24. Gerald B. Ahdunko
GSA/FPA
18th and F Sts., N.W.
Washington, D. C. 20405

(202) 737-5721

25. *Lillian S. Duffey*
GSA/FPA
18th and F Sts., N. W.
Washington, D. C. 20405

(202) 737-5721

26. *James Reeds*
University of California
at Berkley
The Chetwynd, Apt. 431
1030 Lancaster Avenue
Rosemont, Pennsylvania 19010

(215) 527-3309

27. *Herb Bright*
Computation Planning, Inc.
7840 Aberdeen Road
Bethesda, Maryland 20014

(301) 654-1800

28. *Joseph Harrison*
Institute for Computer
Sciences and Technology
National Bureau of Standards
B260, Technology Bldg.
Washington, D. C. 20234

(301) 921-3551

29. *Ford Rowan*
NBC-TV
4001 Nebraska Avenue, N. W.
Washington, D. C. 20016

(202) 686-4265

30. *Stuart Katzke*
Institute for Computer
Sciences and Technology
A265, Technology Bldg.
National Bureau of Standards
Washington, D. C. 20234

(301) 921-3485

31. *Robert P. Blanc*
Institute for Computer
Sciences and Technology
A200, Administration Bldg.
National Bureau of Standards
Washington, D. C. 20234

(301) 921-3768

32. *N. J. A. Sloane*
Bell Labs
Room 2C-363
Murray Hill, New Jersey 07974

(201) 582-2005

33. *George H. Barnes*
Burroughs Corp.
ADO
Box 517
Paoli, Pennsylvania 19301

(215) 648-7316

34. *Howard Campaigne*
Eastern New Mexico University
Portales, New Mexico 88130

(505) 562-3464

35. *Joseph J. Eachus*
Honeywell I. S.
85 Washington Avenue
Cambridge, Massachusetts 02140

(617) 354-3523

36. *Ruth M. Davis*
Director
Institute for Computer
Sciences and Technology
A200, Administration Bldg.
National Bureau of Standards
Washington, D. C. 20234

(301) 921-3151

37. *Dennis Branstad*
Institute for Computer Sciences and Technology
A265, Technology Bldg.
National Bureau of Standards
Washington, D. C. 20234

(301) 921-3861

38. *Jack McDonald*
NCEFT
1000 Connecticut Ave., N. W.
Washington, D. C. 20036

(202) 254-7400

39. *Robert Morris*
AT&T
1776 on the Green
Morristown, New Jersey 07960

(201) 540-6720

40. *S. Jeffery*
Institute for Computer Sciences & Technology
A-247, Technology Bldg.
National Bureau of Standards
Washington, D.C. 20234

(301) 921-3531

41. *Dana Grubb*
Institute for Computer Sciences & Technology
National Bureau of Standards
A-217, Technology Building
Washington, D.C. 20234

(301) 921-3427

42. *Tom Pyke*
Institute for Computer Sciences & Technology
National Bureau of Standards
A-229, Technology Bldg.
Washington, D.C. 20234

(301) 921-3436

8.4 Responses to Questions

The following questions reflect several primary issues that were raised during the workshop. The responses have been prepared either by the staff of NBS or by the agency or authority responsible for the area concerned.

1. Is it proper to have a standard based on classified design principles?

There is no precedent for the Federal Government to publish unclassified standards in the area of cryptography. DES is the first government cryptographic standard that has been published for use outside the classified community. Design criteria for cryptographic systems which are developed by the government or intended for use by the government are always classified. Even though the DES algorithm was designed by a private organization for use in unclassified, non-government applications, the design criteria which overlap with classified design criteria will not be published by the government and the designers of the DES algorithm have agreed not to publish them. Evaluation methods and criteria will be treated similarly.

The publication policy of unclassified standards in classified areas other than cryptography was not investigated. In general, design standards are not explicitly defined within the standard. On the other hand, performance standards do include a means of measuring compliance in the standard. The DES was developed as a design standard. A standard may be issued without specifying all the design criteria if it is useful, if competitors have an equal chance to utilize the standard and if it is explicit to the point that users and suppliers can adopt it.

2. What is the policy on export of the DES?

Export of equipment performing cryptographic functions is subject to Title 22, Code of Federal Regulations, Parts 121-128. The administration of this regulation is the responsibility of the Department of State, Office of Munitions Control. Inquiries concerning the export of devices implementing the DES and of technical data regarding them should be addressed to the Department of State, Office of Munitions Control, Room 800, State Annex #6, Washington, D. C. , 20520.

3. How were the S-boxes chosen?

The S-boxes in the DES were selected by the designer of the algorithm from among those that provided effective cryptographic capability and also exhibited some minimization properties in combinatorial circuit implementation.

4. What is a statement of strength for a good cryptographic algorithm?

A good cryptographic algorithm should be based on the following assumptions:

a. The algorithm is known by everyone, including adversaries.

b. An adversary knows substantial matched plain inputs and cipher outputs of the algorithm using a specific, but unknown, key.

A good cryptographic algorithm satisfies the following criteria:

a. There is no method of recoverying the key known that is easier than trying all the keys that are theoretically possible.

b. That the effort required to try all the theoretically possible keys is not economically feasible commensurate to the value of the data protected by the algorithm.

The algorithm specified in the DES exhibits the properties of a good cryptographic algorithm when used as specified.

5. Was any weakness of the DES algorithm identified during the workshop, or any information regarding the algorithm presented that had not been previously known?

No weakness of the algorithm was identified during the workshop. However, a characterisitc of the algorithm was demonstrated during the workshop that results in complementing the output if all the inputs are complemented. This was felt by some to be a weakness. It was felt that this characteristic could be used, under special circumstances, to get a "two-for-the-price-of-one" effect in a exhaustive search, cryptanalytic attack. All possible keys must be tested even under these special circumstances but two keys may be "tested" for each complete operation of the algorithm. Implementors of the algorithm pointed out that this could be used to test the DES devices during normal operation. The special circumstances require that not only plaintext and matching ciphertext must be obtained but also that the complement of the plaintext and its matching

ciphertext must be obtained. Each pair must be tested for each operation of the algorithm.

6. What are NSA's comments on the paper entitled "An Evaluation of The NBS Data Encryption Standard? "

A copy of this paper was forwarded to the National Security Agency for comment. NSA, acting in its capacity as the National COMSEC (Communication Security) authority prepared the following comments (received June 23, 1977).

8.4.1 NSA's Comments.

1. The evaluation of DES produced by the Lexar Corporation identified interesting structure in some of the S-boxes. We are not surprised by the existence of this structure (as was Lexar) and we are not concerned about it. We do not see any attack on DES based on these properties.

2. Some of the S-box structure found by Lexar is probably caused by the design criteria placed on the generation of the S-boxes. Some may be caused by chip layout constraints or by computer program anomalies. Several of the criteria were found by Lexar (one might expect such findings given the effort that seems to have been put into the analysis). The criteria found by Lexar will be identified in the detailed comments.

3. If plaintext P is enciphered with key K yielding ciphertext C, then the complement of P enciphered with the complement of K yields the complement of C. The report states that under these circumstances, one can reduce the cost of an exhaustive attack by a factor of two (50%). This property was considered in our evaluation and our continuing assessment is that it does not have a serious impact on the security of the DES.

4. The report stated that if the S-boxes were affine or almost affine, the DES would not be secure. We agree with the report results that these properties do not exist in the DES.

5. The report stated that the permutation PC-2 in the Key Schedule does not mix the contents of the C and D registers. Lexar views this "almost" problem as a potential way of reducing exhaustive key searching by a factor of 2. Although the choice of PC-2 may be aesthetically unpleasing to some, it does not lead to a security weakness. The PC-2 permutation was probably chosen based on chip layout constraints or engineering convenience.

Detailed Comments on "An Evaluation of DES"

PAGE	OBSERVATION	COMMENT
1,2	Fear that there exists a "trap door" in the algorithm. Key length of 56 bits is too small.	IBM designed the algorithm. NSA evaluated the algorithm at the request of NBS. Key length is adequate for the application.
3,4	Chosen plain text attack	Well-known cryptanalytic technique.
5,6	S(K,P) = -S(-K,-P)	No serious impact on the security of the algorithm.
	Could save another factor of 2 in cost if S-boxes had been carefully chosen.	S-boxes do not exhibit these adverse properties.
	If S-boxes linear, algorithm could be broken cheaply.	S-boxes do not exhibit this property.
	Curious S-box structure observed.	No security weakness has been discovered from this structure.

Detailed Comments on "An Evaluation of DES"

PAGE	OBSERVATION	COMMENT
	Diffie and Hellman put the cost of "special purpose" exhaustion at $20 million today, $200,000 in ten years.	Disputed by NBS Workshop I.
7	Details of attack based on S(K,P)=-S(-K,-P).	No serious impact on the security of the algorithm.
8,12	An "almost symmetry" caused by choice of PC2 which would have cut another factor of two off exhaustion.	"Poor" choice of PC2 could have been a problem if it were not for E and P. However, no security weakness has been discovered.
13	Looked for affine S-box. None were found.	S-box design criterion.
	S4(x)=S4(x+000001).	Could have been a problem except for P.
	Row 1 to row 2 permutation equals row 3 to row 4 permutation in S4.	Interesting structure but no security weakness has been discovered.

Detailed Comments on "An Evaluation of DES"

PAGE	OBSERVATION	COMMENT
14	PC2 should mix C and D registers	No security weakness found with current PC2.
15	If S-boxes were linear, algorithm could be broken cheaply.	S-boxes are not linear.
16	If S-boxes were affine, algorithm could be broken cheaply.	S-boxes are not affine.
	Discuss notion of "almost" affine S-box.	S-boxes are not "almost" affine.
17	Sums of output bits equaling sums of input bits would lead to an attack if E and P were judiciously chosen.	E and P chosen to eliminate this attack.
18	S-boxes chosen with certain structures in mind.	True.
	Randomly chosen S-boxes are as good as any.	S-boxes were randomly chosen, then tested to meet design criteria.

Detailed Comments on "An Evaluation of DES"

PAGE	OBSERVATION	COMMENT
19	Point out curious complementation structure in some of the S-boxes.	Interesting structure but no security weakness has been discovered.
20-22	Non-randomness of S-boxes identified due to the number of 25% and 50% XOR's observed as compared to random.	Interesting structure but no security weakness has been discovered.
23,24	S4 is 75% redundant. The mod 2 sum of the four output bits of S-box 4 is independent of x6.	Interesting structure but no security weakness has been discovered.
24,25	Each S-box chosen so that changing one bit changes at least two output bits.	S-box design criterion.
26,27	Table on page 27 exhibits pattern of four zeros when C2=1, C5=0.	Caused by S-box design criterion.
28	C=001100 is the only entry in table on page 27 with more than a single 1 which always causes at least two changes in the output.	S-box design criterion.

PAGE	OBSERVATION	COMMENT
26,29	Write S-box outputs as XOR sum of products and try to find polynomials which approximate the S-box output.	No security weakness has been discovered by this kind of analysis.
29	S1 has all permutations even; S2, S3 and S4 have all permutations odd; S5 shows OEEE permutations; S6 shows OEEO permutations; S7 and S8 shows OOOE permutations.	Interesting structure but no security weakness has been discovered.
30,31	Count matches between pairs of rows of S-boxes within and between S-boxes.	No security weakness has been discovered by this kind of analysis.
	There do not exist matches between rows 1-2, 1-3, 2-4, 3-4.	S-box design criterion.
31,32	Curious structure in S8.	Interesting structure but no security weakness has been discovered.

Detailed Comments on "An Evaluation of DES"

PAGE	OBSERVATION	COMMENT
32	No S-box is affine.	S-box design criterion.
32-40	Various S-box structures investigated but not found to exist in the present S-boxes.	No security weakness has been discovered by this kind of analysis.
40	S-boxes chosen to minimize the difference between the number of 1's and 0's in any S-box output when any single input bit is held constant.	Caused by S-box design criteria.
41-49	Statistical analysis on full 16 round algorithm and 2 round toy.	Statistical analysis is relevant.
	DES gets good grades on statistical regularity.	Agree.
	The 2 round toy exhibits poor statistics.	Exactly what one would expect.

PAGE	OBSERVATION	COMMENT
50	A two round toy can be easily broken.	Agree.

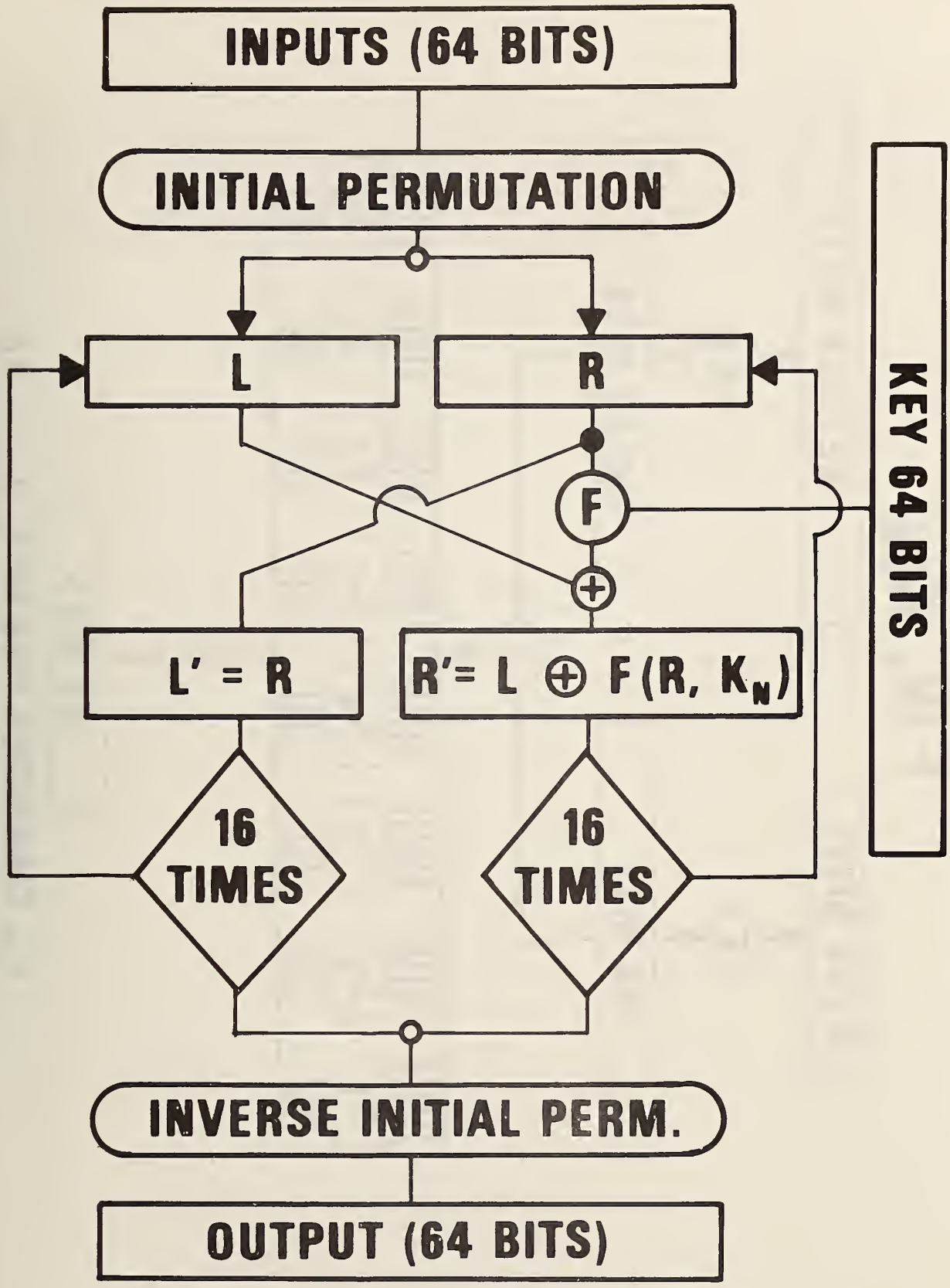

Figure 1. Flowchart of the DES algorithm

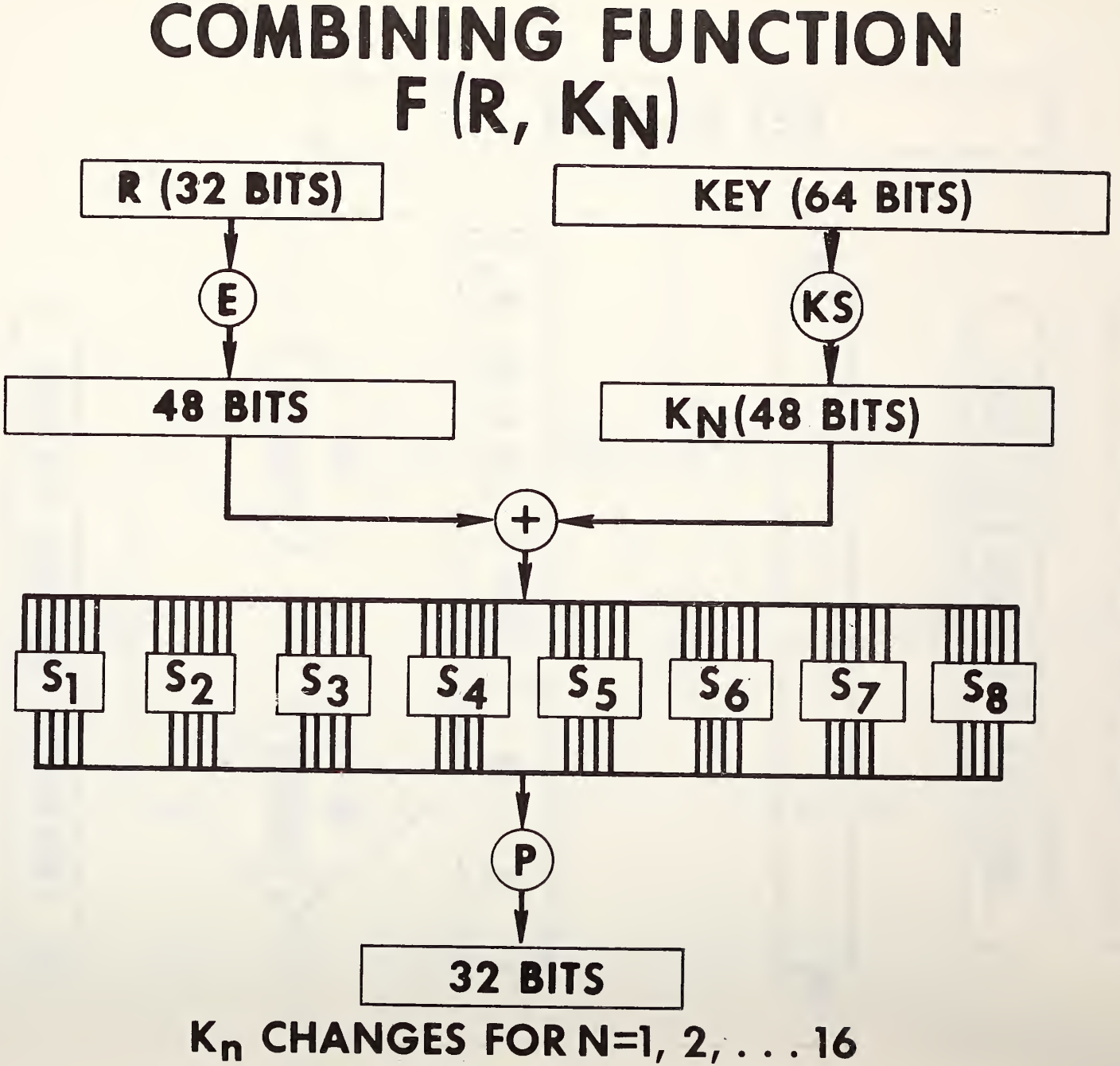

Figure 2. Details of the f-Function

Figure 3: One of the eight S-boxes in the DES. An S-box entry is determined by a six bit input, four of which determine a column and two determine a row. The output is the four bit S-box entry specified by the row and column. The eight S-boxes are connected in parallel, and are used in each of the sixteen rounds of the DES.

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

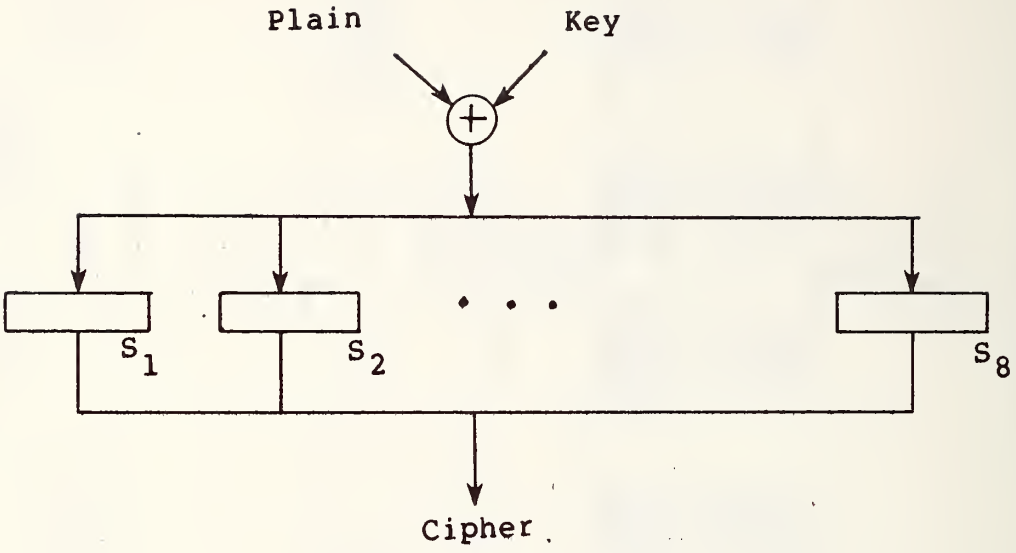

Figure 4 . The parallel connection of eight S-boxes.

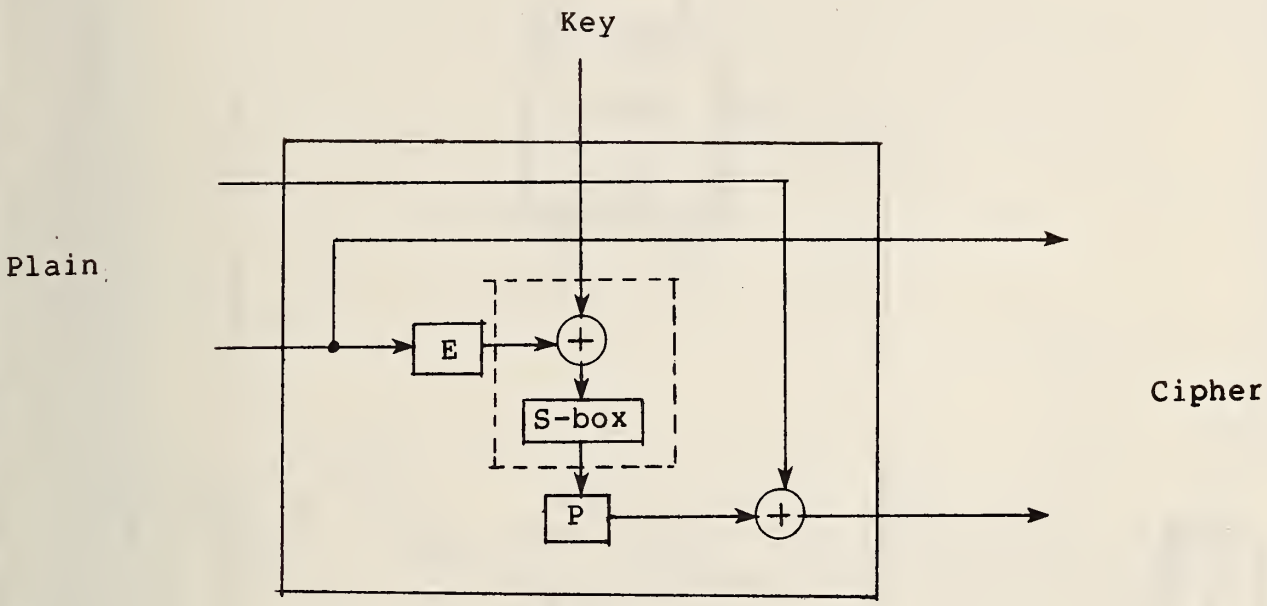

Figure 5 . Details for one round of the DES. The part outlined in dashed lines is a representation of Figure 4.

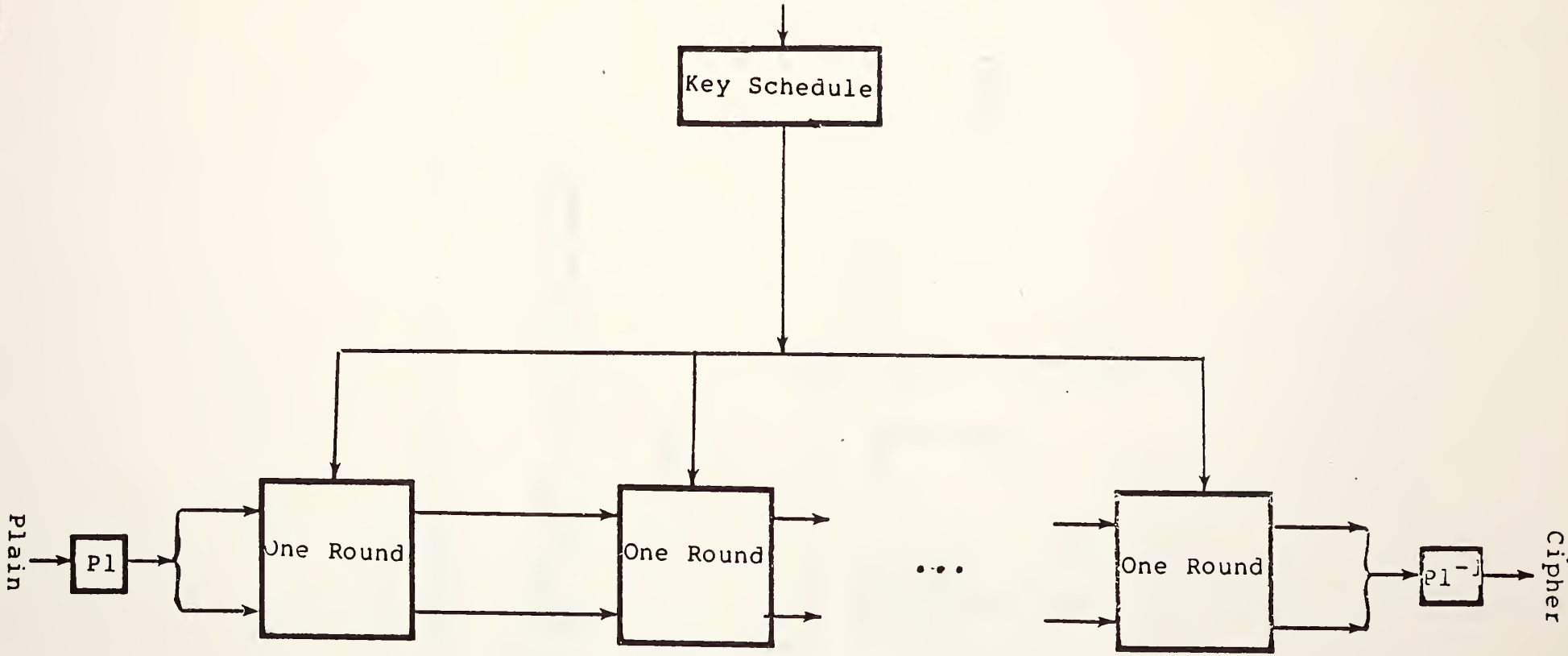

Figure 6 . Series connection of sixteen rounds.

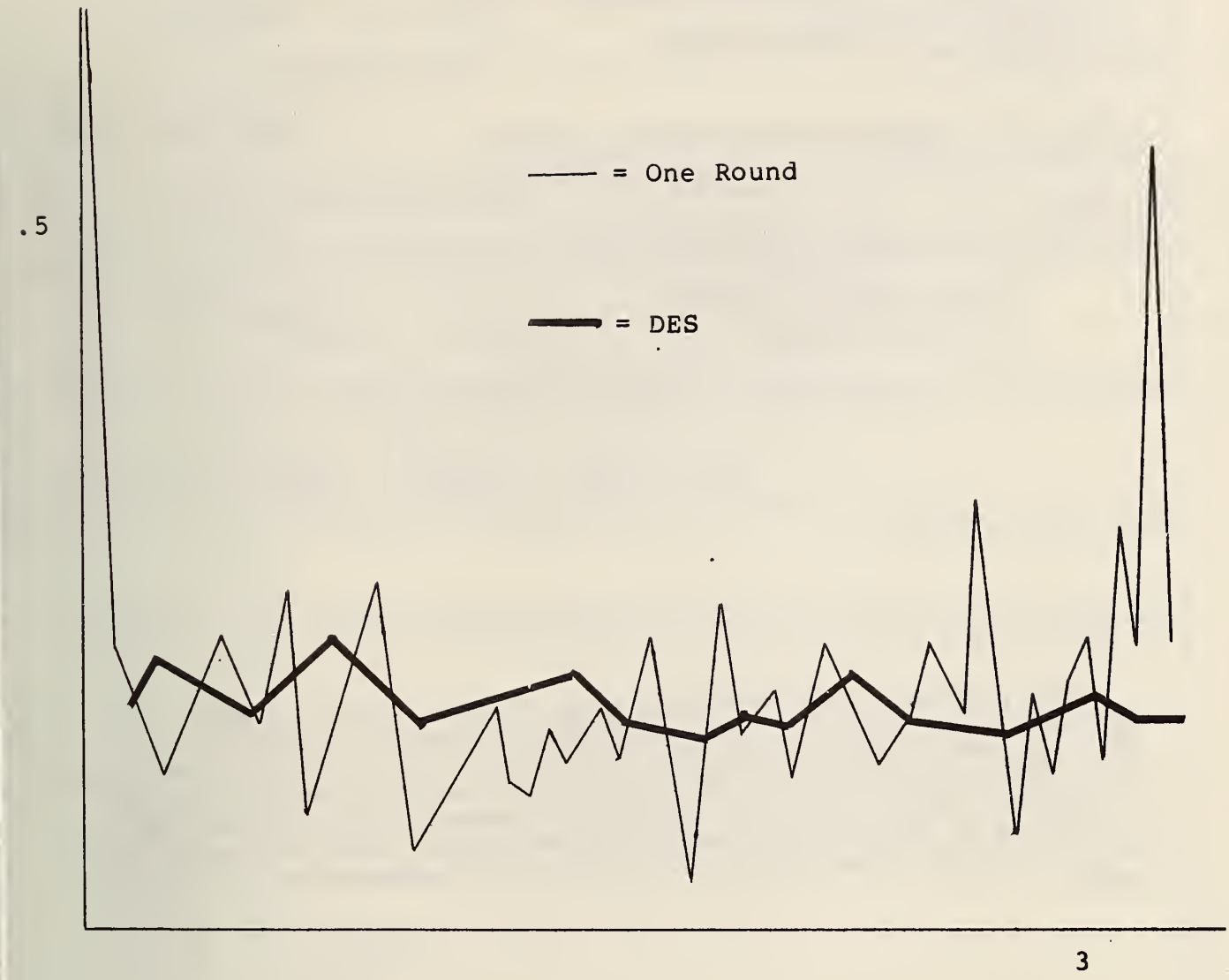

Figure 7 . Power spectrum for the output of one round of DES compared to spectrum for DES.

NBS-114A (REV. 7-73)

U.S. DEPT. OF COMM. BIBLIOGRAPHIC DATA SHEET	1. PUBLICATION OR REPORT NO. NBS IR-77-1291	2. Gov't Accession No.	3. Recipient's Accession No.

4. TITLE AND SUBTITLE

REPORT OF THE WORKSHOP ON CRYPTOGRAPHY IN SUPPORT OF COMPUTER SECURITY

5. Publication Date September 15, 1977

6. Performing Organization Code 640.01

7. AUTHOR(S) Branstad, Dennis; Gait, Jason; Katzke, Stuart.

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. 640.1112

11. Contract/Grant No.

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

13. Type of Report & Period Covered

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.)*

This publication reports on the Workshop on Cryptography in Support of Computer Security held at the National Bureau of Standards on September 21-22, 1976. The workshop was organized to obtain expert opinions on the mathematical and statistical characteristics of the proposed Data Encryption Standard (DES) as it relates to computer security. This report summarizes formal presentations that were made, outlines major issues that were raised, quotes statements that were made for the record and answers several of the major questions that were asked.

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)*

Cryptanalysis; cryptography; encryption; key management; known plaintext attack; security; work factor.

18. AVAILABILITY

- [X] 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
- [X] Order From National Technical Information Service (NTIS) Springfield, Virginia 22151

19. SECURITY CLASS (THIS REPORT)	21. NO. OF PAGES
UNCLASSIFIED	61
20. SECURITY CLASS (THIS PAGE)	**22. Price**
UNCLASSIFIED	$4.50

USCOMM-DC 29042-P74