THE FEDERAL DATA ENCRYPTION STANDARD IN THE 1980'S

Harrison R. Burris
NOETECHNIC INDUSTRIES INC.
P.O. BOX 277
REDONDO BEACH, CA
90277

ABSTRACT

The development of the federal data encryption standard is traced from the requirements leading to inception of the project through the publication of federal and commercial (ANSI) standards. The algorithm is briefly reviewed and strengths and weaknesses are discussed. Current applications are described and some potential developments are presented.

INTRODUCTION

The first federal data encryption standard (DES) went into affect with the approval of FIPS No. 46 in January 1977. Since that time both Government and Commercial standards groups have published standards for the use of the DES but the number of applications have been extremely few. This paper presents an overview of the present DES status and attempts to assess the immediate future. The discussion covers the following topics: Government and Civilian needs for DES, Development history, DES algorithm, Typical applications, Strengths and weaknesses and Assessment of the future.

GOVERNMENT AND CIVILIAN NEEDS

In the early 1970's several forces were at work creating a need for a non-Department of Defense controlled encryption algorithm. Congress and federal agencies were concerned about both data privacy and data security in the newly emerging Federal computer data network and civilian manufacturers of systems related to banking and other vulnerable enterprises wanted to secure their data communications services. Use of a DOD controlled encryption algorithm entailed meeting electromechanical, personnel and administrative requirements beyond the funding capabilities of many agencies. The commerically available devices were mostly produced by foreign vendors and were also considered of

questionable cryptographic strength. Civilian manufacturers wanted a device blessed by the Government (nobody wants to be sued for delivering a weak algorithm).

DEVELOPMENT HISTORY

Rising interest in the privacy of information in computers and communications (e.g. , 1,2) and an upsurge in proposed and approved federal privacy legislation (e.g., 3,4) resulted in the 1972 tasking of the National Bureau of Standards to develop an algorithm suitable for non-Department of Defense applications. In May 1973, NBS advertised in the Federal Register (39FR12763) for sources of a data encryption algorithm suitable for non DOD use. IBM responded and a variant of the IBM LUCIFIER system was selected by NBS. The algorithm was published in the Federal Register in March 1975 (40FRI2067) for public comment. After a public forum was held the algorithm was adopted as Federal Information Processing Standard No. 46, in January 1977.

As approval of the DES became nearly certain two other standards groups began efforts on the next steps in the story. The Data Encryption Subcommittee (SC3) of the Federal Telecommunication Standards Committee (FTSC) began development of standards for the employment of DES within federal telecommunications systems, and an Ad Hoc Encryption Study Group of the American National Standards Institute (ANSI) Computers and Information Processing Subcommittee (X3) began work leading to ANSI network encryption standards for commercial applications. The standards thus far resulting from these activities are: FED-STD 1026, Telecommunications: Compatibility Requirements for use with the Data Encryption Standard; FED-STD 1027 Telecommunications: Security Requirements for use with the Data Encryption Standard; and the ANSI Standard X3.92, Data Encryption Algorithm (DEA), the commercial standard for the DES algorithm. Link encryption standards are being developed by the ANSI X3S38 subcommittee and encryption standards for other levels of network protocols are being developed by the X3/T1 subcommittee.

DATA ENCRYPTION STANDARD ALGORITHM

DES Algorithm Flow

The Data Encryption Standard algorithm is classified as a block product cipher system. Block because it transforms more than one character at a time. Product (7) because it is composed of a series of transpositions, substitutions and additive encodings combined by a sequence of feedback cycles. The flow of the algorithm is illustrated in Figure 1.

An input string of 64 bits is first passed through an initial permutation (transposition T1). The transposed string is then separated into two 32 bit strings (L = bits 1 to 31 and R =

bits 32 to 64). The portion of the DES called the inner algorithm, because it is cycled sixteen times for every input block processed, is now entered. String R is passed to a temporary store L' and then R is expanded by a substitution function, E, into a 48 bit string. The 64 bit key string (call it the current key) is processed by one of a series of substitutions to produce a 48 bit key (call it the operating key). The operating key is then exclusive ORed with the 48 bit expanded R string. The 48 bit string resulting from this operation is then reduced to 32 bits by a series of substitution functions (S1 to S8) each of which reduces 6 adjacent bits into 4 bits. The 32 bit string produced by these substitutions is then transposed (T2) and the resulting string is exclusive ORed with the 32 bit string L. The resulting string R' becomes R and L' replaces L, and another cycle of the inner algorithm beginning with the transfer of R to L' is repeated using the next selection of operating key. When sixteen cycles of the inner algorithm have been completed, the 64 bit string formed by the concatenation of the last L' and R' strings into string R'L' is given a final permutation (transposition TI). The permuted 64 bit string is the output of the algorithm.

All steps in the algorithm are identical for encryption and decryption except for the order in which operational keys are selected from the current key. The series of 16 key selection patterns used for encryption is reversed when a block is being deciphered.

Modes of Operation

Two modes of operation for the data encryption standard are described in the draft guideline (5), these are called Electronic Code Book (ECB) and Cipher Feedback (CFB).

Electronic Code Book

In this mode of operation, the sender and receiver process an indefinite length string of data blocks using a single fixed value for the current key. A block of input data is processed by the encrypt sequence of operational keys at the sending device and is then recovered at the receiving device by processing the input with the decrypt sequence of operational keys. Since the current key setting is not affected by the number of data blocks exchanged all data blocks may be encrypted and decrypted in any order until the current key is changed. Figure 2.

Cipher Feedback

In the Cipher Feedback mode, both the sending and receiving nodes, cycle the operational keys in the same encryption (or decryption) sequence to combine a 64 bit cipher feedback string (input) and a current key into a "cipher string". This cipher string is then XORed with the data to be transmitted (of 1 to 64 bits in length) to produce the encrypted output.

When the encrypted output is XORed with the same “cipher string” at the receiving node, the plain text is recovered. This mode permits data of less than 64 bits to be transmitted (e.g., a byte-oriented terminal interface). Once a current key is set, initialization for the CFB mode requires that a sufficient string (64 bits) be sent to the receiver to synchronize it. The XORed string becomes the cipher feedback string input to the encrypted algorithm when the next cipher string is generated. See Figure 3.

The continuing work of the FTSC and ANSI standards groups has resulted in definition of two additional modes of operation.

Cipher Block Chaining

The primary functional difference between the CFB and CBC modes is that in CBC mode the modulo-2 addition (XOR) of text with cycle string occures before the DES operation, and in the CBC mode the XOR occures after the DES operation. See Figure 4.

Output Block Feedback

In the output block feedback mode, both the sending and receiving nodes, cycle the operational keys in the same encryption sequence. On this mode the 64 bit output of the DES is fedback as the input for the next cycle and this same output is used as a cipher string (key stream). At the sending node plaintext data is combined with the cipher string by the XOR operation. This encrypted data is again XORed with the cipher string at the receiving node in order to receive the plaintext. See Figure 5.

Certification for Federal Use

Federal agencies and departments using the DES must employ hardware implementations of the algorithm that have been validated by NBS as conforming to the standard (software implementations are not acceptable for Government applications and there is no need to validate hardware devices being used in non-government applications). DES device manufacturers may submit their product for NBS validation according to the procedures outlined in NBS Specification Publication 500-20. NBS will issue a validation certificate to the manufacturer upon successful completion of the tests. DES device makers such as Collins Radio (Rockwell International), IBM, Intel and Motorola have had devices validated while others such as American Microsystems, Inc. have taken the position that validation is the device users responsibility. Manufacturers following the AMI philosophy would be somewhat less vunerable to litigation should the DES algorithm or the validation procedures ever prove faulty.

TYPICAL DES APPLICATIONS

The Federal Reserve Banking Network (FED-WIRE) is using the CFB mode with 8-bit characters in a link encryption system. IBM, Motorola and Rockwell-Collins developed the DES products used for FED-WIRE. The Government has let some competitive contracts for development of high speed (eg T1 channel or D3 channel bank) encryption/ decryption units. Commercially the DES is finding use in applications such as TRW's Secure Access Control Systems (SACS) where they provide link security between a central control station and badge readers in physically secured buildings.

STRENGTHS AND WEAKNESSES

The DES algorithm uses feedback to spread combinations of information bits over the physical bits, the result being that any single bit change in the cipher text will result in several bits being changed in the plaintext when it is received. This is a very good indication of attempted tampering. When the DES is operated in the ECB mode this benefit is fully available, however when the DES uses the XOR combining function only some of the protection is available (the XOR operation does not support error extension).

The key size of the DES has been categorized as vulnerable to exhaustive enumeration - all keys are vulnerable to this, given enough time; and the time required to defeat a DES can be quite long enough for commercial applications (6,7)

ASSESSMENT OF THE FUTURE

Neither the Government or commercial markets have met the expectations of the chip manufacturers. In the case of the missing Government market the most likely cause is the nature of the privacy laws and standards themselves. FIPS 46 defines the encryption algorithm that must be used by nonDOD federal agencies when they require encryption security. It remains for other laws and standards to identify which agencies require encryption security; and these laws have not been forthcoming. Without a requirement Government Project Managers can not justify the funds to install DES on their systems. Also FIPS 46 does not standardize enough of the encryption/decryption protocol, the chip requires too much interfacing hardware/software to be cost effective. As a result, while some trunk encryption applications are progressing the hundreds of thousands of encrypted Government data terminals once expected, have not yet materialized. In the case of the commercial market the precieved benefits do not yet exceed the costs except for a very few applications. This is partly due to the high cost of interfacing the devices mentioned above, but also results from the scare stories circulated by the advocates of the public key systems.

When will the Government market open up? When a Senator decides pushing Government security and privacy is a role to keep him in office or when a newspaper gets a security story that embarrasses the Government into passing laws. The commercial market will open up when the public begins to regard computer/network crimes as typical rather than as unusual or isolated instances or when the costs of using DES drop to the point of being a worthwhile investment as insurance against computer crime and the liability arising from a successful crime.

REFERENCES

1. Westin, Alan F.; Lufkin, Daniel; and Martin, David B. H., The Impact of Computer-Based Information Systems on Citizen Liberties in the Advanced Industrial Nations. A report for the German Marshall Fund of the U.S., Washington, D.C., 1973.

2. Turn, R., "Privacy and Security in Personal Information Databank Systems," RAND Corporation Document R-1044-NSF, March 1974.

3. U.S. Senate Commitee on Government Operations, Report No. 93-1183, "Protecting Individual Privacy in Federal Gathering, Use and Disclosure of Information."

4. Privacy Action of 1974, Public Law 93-579, 93rd Congress, December 31, 1974.

5. Branstad, D. K., Draft Guidelines for Implementing and Using the NBS Data Encryption Standard, National Bureau of Standards, November 10, 1975.

6. Burris, H. R., "Micro-Computer Implemented NBM Encryption Algorithm," Proc. Microcomputer '77, IEEE, April 1977, pp. 75-80.

7. Burris, H. R., "A Security Analysis of the Federal Data Encryption Standard" Proc. Eleventh Annual Asilomar Conference on Circuits, Systems, and Computers, IEEE, November 1977, pp. 481-486.

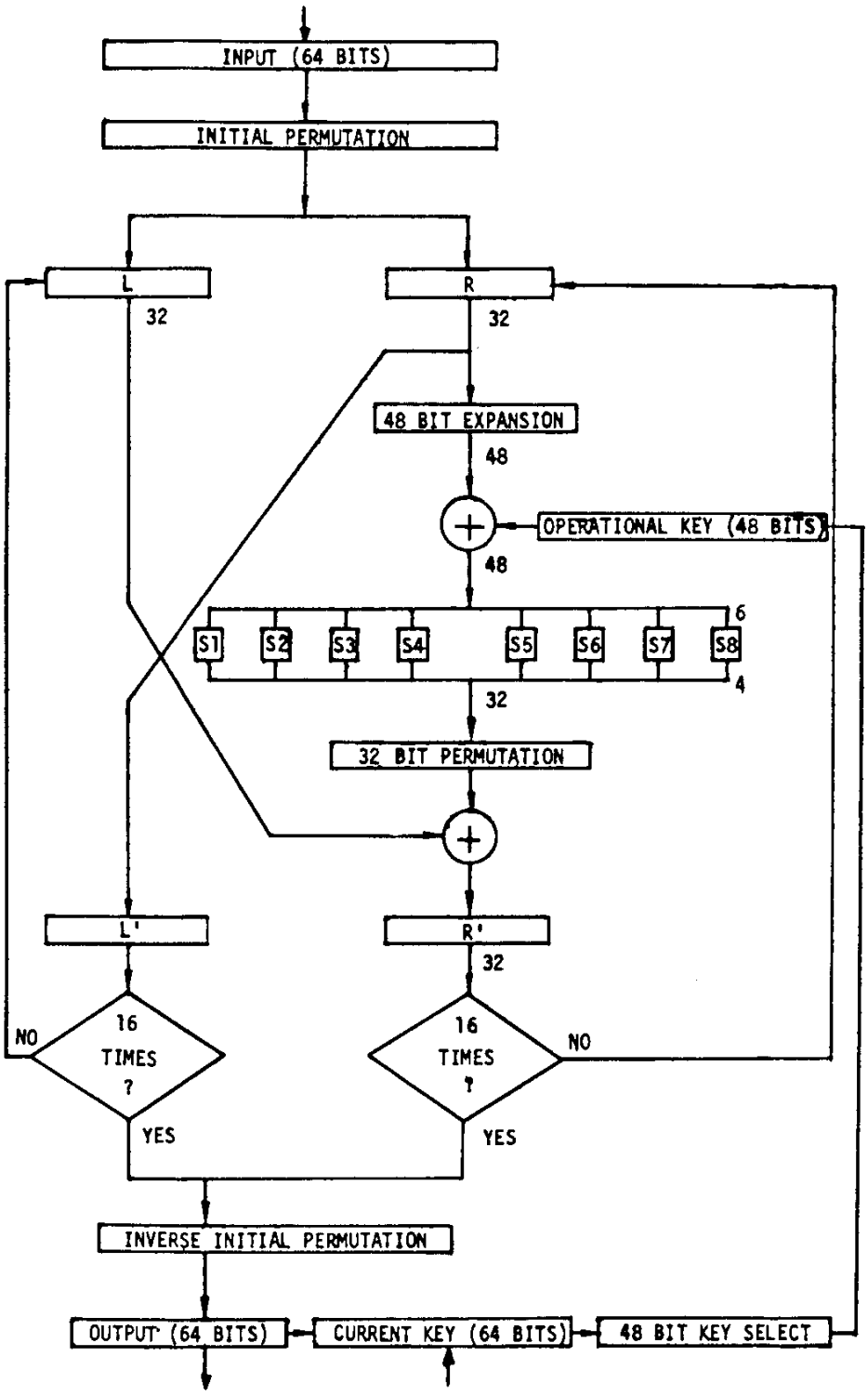

Figure 1. DES Algorithm

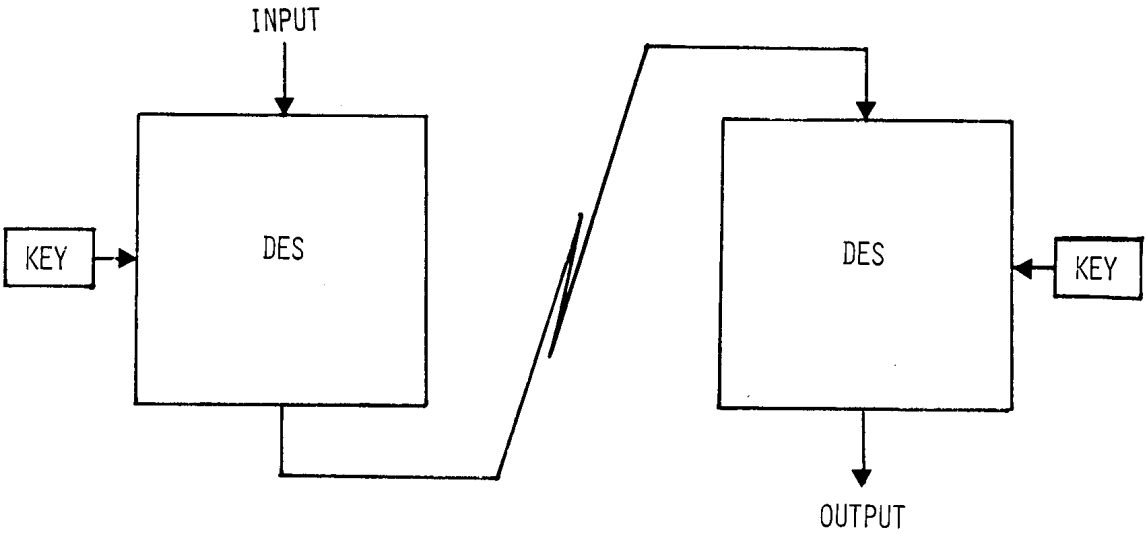

Figure 2. ECB Mode

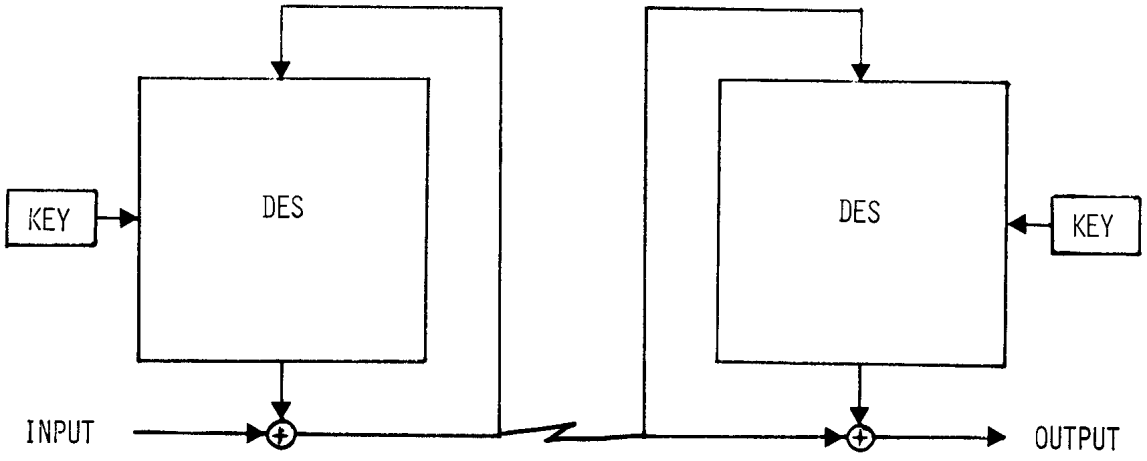

Figure 3. CFB Mode

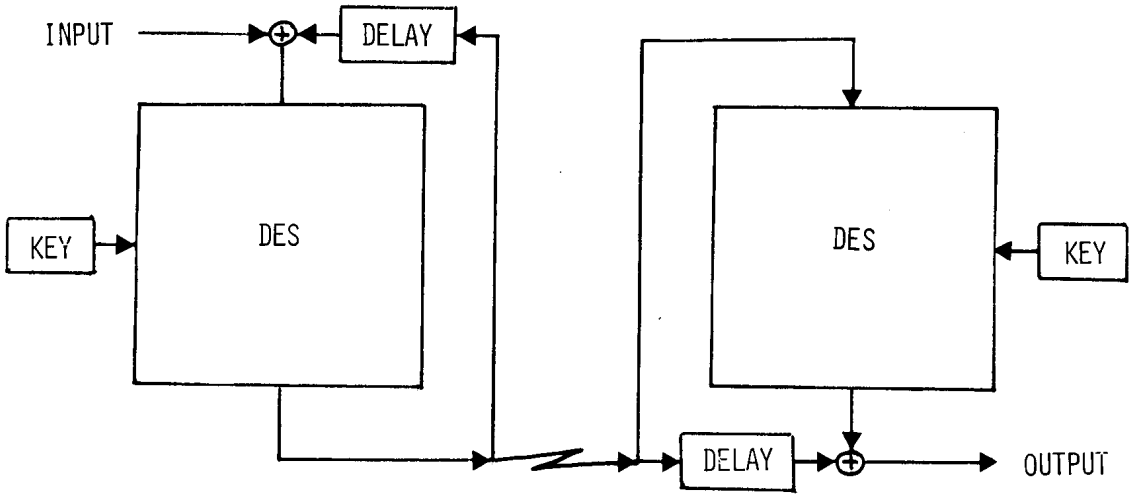

Figure 4. CBC Mode

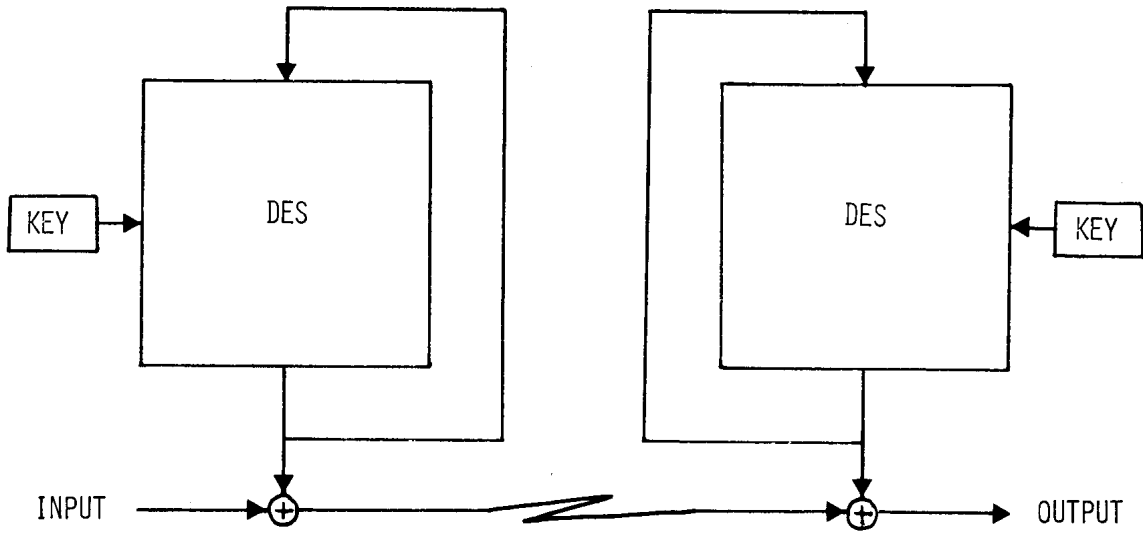

Figure 5. OBC Mode