Federal Standard 1026 has been redesignated as Federal Information Processing Standards Publication (FIPS PUB) 139. Issued by the National Institute of Standards and Technology pursuant to Section 111(d) of the Federal Property and Administrative Services Act of 1949 as amended by the Computer Security Act of 1987, Public Law 100-235.

FEDERAL STANDARD 1026

GENERAL SERVICES ADMINISTRATION

INTEROPERABILITY AND SECURITY REQUIREMENTS FOR USE OF THE DATA ENCRYPTION STANDARD IN THE PHYSICAL LAYER OF DATA COMMUNICATIONS

Prepared By:
National Communications System
Office Of Technology & Standards

Published By:
General Services Administration
Office Of Information Resources Management

August 3, 1983

FEDERAL STANDARD

TELECOMMUNICATIONS: INTEROPERABILITY AND SECURITY REQUIREMENTS FOR USE OF THE DATA ENCRYPTION STANDARD IN THE PHYSICAL LAYER OF DATA COMMUNICATIONS

This standard is issued by the General Services Administration pursuant to the Federal Property and Administrative Services Act of 1949, as amended.

1. Scope

1.1 Description. This standard specifies interoperability and security related requirements for using encryption at the Physical Layer of the ISO Open Systems Interconnection (OSI) Reference Model in telecommunication systems conveying Automatic Data Processing (ADP) and/or narrative text information. The algorithm used for encryption is the Data Encryption Standard (DES), described in Federal Information Processing Standards Publication 46. Requirements contained in this standard relate to the interoperation of Physical Layer Data Encryption Equipment, or their interoperation with associated Data Terminal Equipment or Data Circuit-terminating Equipment. Additional security requirements, not directly relating to interoperability, are contained in Federal Standard 1027.

1.2 Objectives

1.2.1 Interoperability. To facilitate the interoperation of Government data communication facilities and systems that require cryptographic protection using the Data Encryption Standard (DES) algorithm

1.2.2 Security. To prevent the disclosure of plaintext

1.3 Application. This standard applies to all DES cryptographic components, equipment, systems, and services procured or leased by Federal departments and agencies for encryption of ADP and/or narrative text information in the Physical Layer of data communications using the Data Encryption Standard (DES) algorithm. Encryption of video signals and facsimile documents is not within the scope of this standard. Guidance to facilitate the application of this standard, with respect to degradation of security by improper implementation or use, will be provided for in a revision to Federal Property Management Regulation 41 Code of Federal Regulations 101-35.3.

1.4 Definitions. The following definitions, conventions, and terminology apply in this standard. Further definitions are contained in Federal Standard 1037.

a. Ciphertext: Encrypted data.

b. Data Encryption Equipment (DEE): DES Cryptographic Equipment used in data communications. This equipment may be integrated into Data Terminal Equipment, Data Circuit-terminating Equipment, or be stand-alone.

c. DES: The Data Encryption Standard algorithm specified in Federal Information Processing Standards Publication 46.

d. DES Cryptographic Equipment: Equipment embodying one or more DES devices and associated controls, interfaces, power supplies, alarms and the related hardware, software, and firmware used to encrypt, decrypt, authenticate, and perform similar operations on information.

e. DES Device: The electronic hardware part or subassembly which implements just the DES algorithm specified in Federal Information Processing Standards Publication 46, and which is validated by the National Bureau of Standards.

f. DES Key Variable: The 64 bits used to key DES Data Encryption Equipment. Eight bits are used for parity checking and 56 bits are used by DES devices for encryption and decryption.

g. Initializing Vector (IV): A vector used in defining the starting point of an encryption process within a DES device.

h. Narrative Text: Text for which the semantic content is not changed by Automatic Data Processing (ADP) equipment (e.g., record or narrative traffic).

i. Plaintext: Unencrypted data.

j. Service Data Unit: The unit of data provided as input to a given layer of the ISO Open Systems Interconnection Reference Model from the next higher layer.

2. Referenced Documents

a. Federal Information Processing Standards Publication 46: Data Encryption Standard. (Copies of this standard are available from the National Technical Information Service, U.S. Department of Commerce, 5285 Port Royal Road, Springfield, VA 22161).

b. Federal Information Processing Standards Publication 81: DES Modes of Operation. (Copies of this standard are available from the National Technical Information Service, U.S. Department of Commerce, 5285 Port Royal Road, Springfield, VA 22161).

d. Federal Standard 1011: Telecommunications: Character Structure and Character Parity Sense for Serial-By-Bit Data Communication in the American National Standard Code For Information Interchange. (Copies of this standard are available from the General Services Administration Specification Unit (WFSIS), Room 6039, 7th and D Streets S.W., Washington, D.C. 20407).

e. Federal Standard 1027: Telecommunications: General Security Requirements for Equipment Using the Data Encryption Standard. (Copies of this standard are available from the General Services Administration Specification Unit (WFSIS), Room 6039, 7th and D Streets S.W., Washington, D.C. 20407).

f. International Standard 7498: Open Systems Interconnection Reference Model. This document is available from the American National Standards Institute (ANSI), 1430 Broadway, New York, New York 10018.

3. Requirements

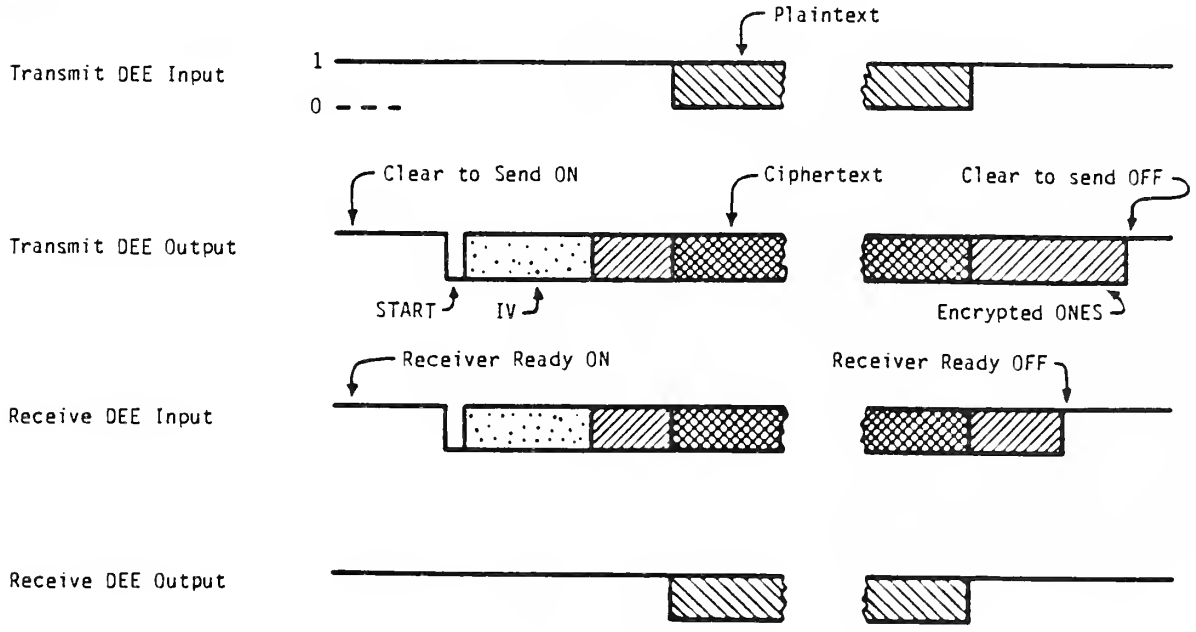
3.1 Overview. In Physical Layer encryption, all of the Physical Layer Service Data Unit is encrypted, except for START and STOP bits during asynchronous operation and parity bits when parity is being restored. An option is provided for restoring asynchronous character parity.

3.2 Mode of Operation. The capability shall exist to operate using the 1-bit Cipher Feedback mode of operation. (Ref. Federal Information Processing Standards Publication 81).

3.3 Synchronous Operation

3.3.1 Transmission. Upon the establishment of a physical connection between Data Encryption Equipment (corresponding to reception of initial Clear to Send indication), the Send Data interchange circuit is in a MARK (all ONEs) state. A 48-bit Initializing Vector (IV) is sent at this point in time, preceded by a single ZERO bit (SPACE) to delimit the IV. The first bit transferred of the 48-bit IV is placed in bit position 17 of the DES device input block (Ref. Federal Information Processing Standards Publication 81). (It may be desirable to delay Clear to Send indication to a transmitting unit of Data Terminal Equipment while the IV is sent). Immediately after transmission of the IV, all bits of the Physical Layer Service Data Unit (corresponding to all bits on the Send Data interchange circuit) are encrypted. This process continues indefinitely, until disestablishment of the physical connection (loss of Clear to Send indication).

3.3.2 Reception. Upon the establishment of a physical connection (corresponding to initial Receiver Ready indication), the Receive Data interchange circuit is in a MARK (all ONEs) state. The 48 bits received immediately following the first ZERO bit (SPACE) are considered to be the Initializing Vector. All following bits received are decrypted. This process continues indefinitely, until disestablishment of the physical connection (loss of Receiver Ready indication). An example of synchronous Physical Layer encryption, indicating some timing relationships, is shown in the following figure.



3.4 Asynchronous Operation

3.4.1 Normal Transmission

3.4.1.1 Overview. The encryption of asynchronous and synchronous Physical Layer data is closely related. The differences in encryption relate to use of START and STOP bits and accommodation of BREAK signals.

3.4.1.2 Initializing Vector. Upon the establishment of a physical connection (corresponding to initial Clear to Send indication), the Send Data interchange circuit is in a MARK (all ONEs) state. An Initializing Vector (IV) is sent at this point in time, subdivided into units the size of the characters about to be encrypted and transmitted. The IV length shall be the lowest integer multiple of the character size that is equal to or greater than 48 bits. The characters into which the IV is subdivided shall have appropriate START and STOP bits appended to them. In transmission of a 49-bit IV, for example, the first IV bit transferred is placed in bit position 16 of the DES device input block.

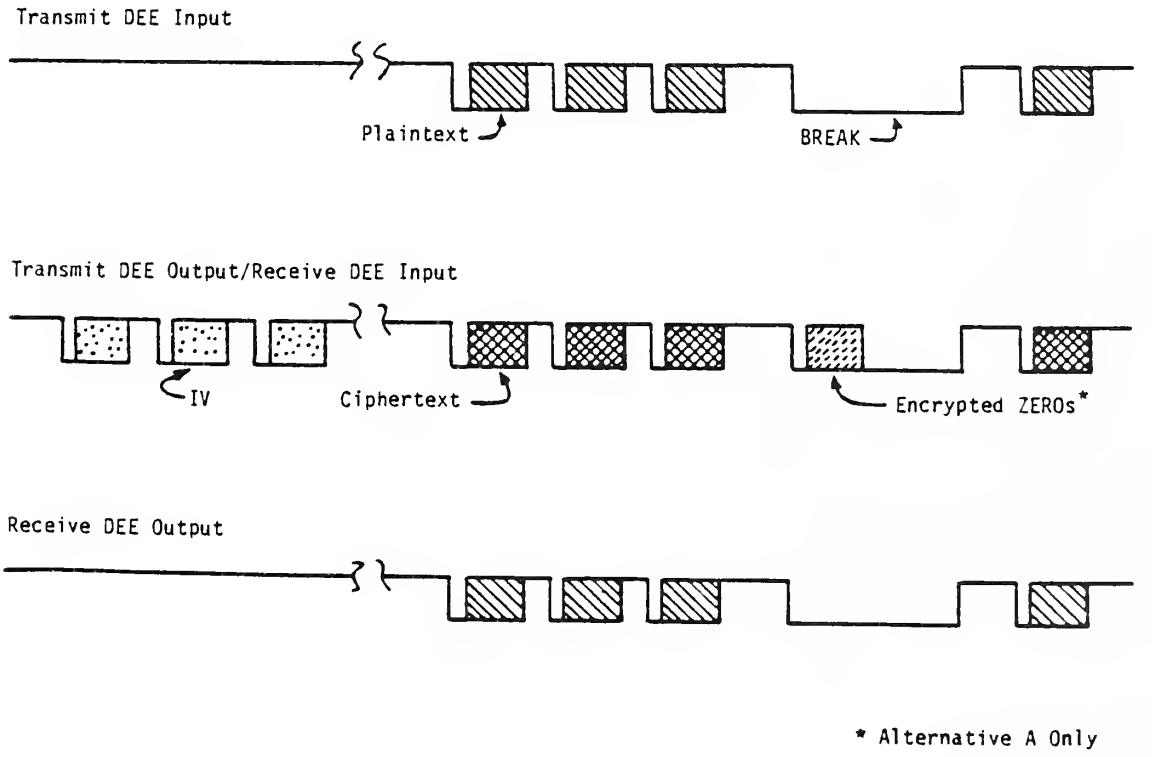
3.4.1.3 Starting Encryption. After transmission of the IV, characters of the Physical Layer Service Data Unit (corresponding to characters on the Send Data interchange circuit), framed within START and STOP bits, are encrypted. START and STOP bits are not encrypted. This process continues indefinitely, except for BREAK signals (described below), until disestablishment of the physical connection (loss of Clear to Send indication).

3.4.1.4 BREAK Signal. BREAK signal is a SPACE (all ZEROs) condition existing for one character-time or longer. When such a condition occurs, it shall be treated in one of two ways.

3.4.1.4.1 Alternative A. The first ZERO bit of the BREAK signal is treated as a START bit. The next n ZERO bits are encrypted, where n is the normal character length. Subsequent ZERO bits are not encrypted. Encryption resumes after the next MARK to SPACE (ONE to ZERO) transition. This transition indicates the START bit of a new character.

3.4.1.4.2 Alternative B. Characters are delayed prior to encryption. A BREAK condition is a character-length or longer all ZEROs condition (including what would be the STOP bit interval). ZERO bits during the BREAK condition are transmitted unencrypted. Encryption continues on the next character that is framed with START and STOP bits.

3.4.2 Normal Reception. Upon establishment of a physical connection (corresponding to initial Receiver Ready indication), the Receive Data interchange circuit is in a MARK (all ONEs) state. Based upon character length, the first characters received, exclusive of START and STOP bits, are considered as the Initializing Vector (e.g., six 8-bit characters) All following characters, exclusive of START and STOP bits, are decrypted. This process continues indefinitely (except during BREAK signals), until disestablishment of the physical connection (loss of Receiver Ready indication). Decryption is suspended during BREAK signals. An example showing transmit Data Encryption Equipment input/output, for asynchronous Physical Layer encryption, is provided in the figure below.



* Alternative A Only

3.4.3 Operation With Parity Restored (Optional). As an additional capability, asynchronous Physical Layer Data Encryption Equipment may optionally be configured to restore parity on encrypted 7-bit-plus-parity (e.g. Federal Standard 1011) characters. To accomplish this, the first seven data bits of each character are encrypted as they would for the encryption of seven-bit characters. The 8th bit of each character is set as parity for the previous seven bits of ciphertext prior to transmission. At reception, within the unit of Data Encryption Equipment, the first seven bits of each character are decrypted and the 8th bit is set as parity for the previous seven bits of plaintext. Incorrect parity on ciphertext shall be translated into incorrect parity on plaintext. Since encryption is handled as it would be for 7-bit characters, the Initializing Vector shall consist of seven characters (49 bits of IV and 7 parity bits). When BREAK signals are used, alternative B (section 3.4.1.4.2) must be employed to preserve parity.

3.5 DES Key Variable Loading. The capability shall exist to operate (i.e. encrypt and decrypt data) with DES key variables loaded using one of the two methods described in Federal Standard 1027.

4. Changes. When a Government department or agency considers that this standard does not provide for its essential needs, a statement citing specific requirements shall be sent in duplicate to the General Services Administration (K), Washington, DC, 20405, in accordance with the provisions of the Federal Property Management Regulation 41 CFR 101-29.3. The General Services Administration will determine the appropriate action to be taken and will notify the agency.

PREPARING ACTIVITY:

National Communications System
Office of Technology and Standards
Washington, DC 20305

U.S. GOVERNMENT PRINTING OFFICE: 1984 - 421-595/3668

MILITARY INTERESTS:

Military Coordinating Activity
NSA — NS

Custodians
Army -- SC
Navy — EC
Air Force -- 02

Review Activities
Army -- AD, CR
Navy -- AS, OM
Air Force — 90
DCA -- DC
TRI-TAC -- TT
DLA -- DH

User Activities
Navy — SH, MC

This document is available from the General Services Administration (GSA), acting as agent for the Superintendent of Documents. A copy for bidding and contracting purposes is available from GSA Business Centers. Copies are for sale at the GSA Specification Unit (WFSIS), Room 6039, 7th and D Streets S.W., Washington, D.C. 20407; telephone (202) 472-2205. Please call in advance to arrange for pickup service.