NIST-7/72

U.S. DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

FIPS PUBLICATION CHANGE NOTICE

CHANGE NUMBER: 2

DATE OF CHANGE: 1996 May 31

FIPS PUBLICATION NUMBER: 81

PUBLICATION TITLE

FIPS PUB 81, DES Modes of Operation.

THIS OFFICE HAS A RECORD OF YOUR INTEREST IN RECEIVING CHANGES TO THE ABOVE FIPS PUBLICATION. THE CHANGE(S) INDICATED BELOW HAVE BEEN PROVIDED BY THE MAINTENANCE AGENCY FOR THIS PUBLICATION AND WILL BE INCLUDED IN THE NEXT PUBLISHED REVISION TO THIS FIPS PUBLICATION. QUESTIONS OR REQUESTS FOR ADDITIONAL INFORMATION SHOULD BE ADDRESSED TO THE MAINTENANCE AGENCY:

Department of Commerce
National Institute of Standards and Technology
Computer Systems Laboratory
Gaithersburg, MD 20899

CHANGE ITEM(S)

This change notice provides editorial changes, updated references to documents and organizations, a correction to Figure 3, and additional guidance to agencies regarding the 64-bit Output Feedback Mode to FIPS 81, DES Modes of Operation. These changes are considered to be included whenever reference is made to the publication.

This change notice should be filed with FIPS 81.

Attachment
4 pages

Copies of FIPS are available from:

National Technical Information Service (NTIS)
ATTN: Sales Office, Sills Building
5285 Port Royal Road
Springfield, VA 22161
Phone - (703) 487-4650
Office Hours - 7:45am to 5pm

ELECTRONIC FORM

U.S. Department of Commerce
National Institute of Standards and Technology

FIPS Publication Change Notice

FIPS PUB 81, *DES Modes of Operation*
Change No.: 2
Date of Change: 1996 May 31

Change Items:

This change notice provides editorial changes, updated references to documents and organizations, a correction to Figure 3, and additional guidance to agencies regarding the 64-bit Output Feedback Mode to FIPS 81, *DES Modes of Operation*. These changes are considered to be included whenever reference is made to the publication.

This change notice should be filed with FIPS 81.

Attachment
4 pages

Change No. 2 to FIPS PUB 81
Date of Change - 1996 May 31

1. There is a correction to Figure 3 on Page 9, which diagrams the flow for k-bit CFB mode. In the decryption state, it is the k bits of cipher text which should be fed back into the rightmost k bits of the input block; a line segment should extend from the cipher text box to the line that points to the input block. The leftmost k bits of the output block should only be fed into the exclusive-OR function with the k bits of cipher text. These bits from the output block should not be fed back into the input block. The corrected diagram for Figure 3 is shown here:

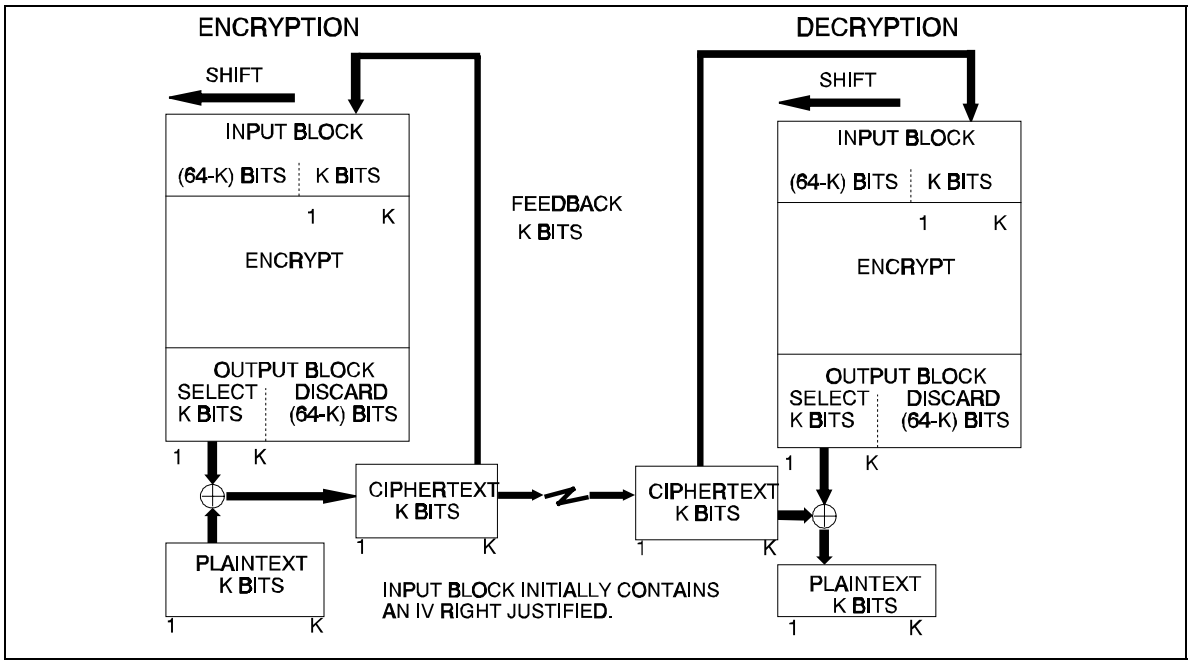

Figure 3: ***k-bit Cipher Feedback (CFB) Mode***

2. After the publication of FIPS 81, it was discovered that when less than 64 bits of feedback are used in the OFB mode (paragraph 5, p. 8), there is a risk of generating short cycles. That is, when the same key is used, and multiple encryptions or decryptions have occurred, then the resulting output block may be equal to an input block from a previous iteration. If that occurs, then further encryption or decryption using the same key will result in a repetition of previously generated output and input blocks. This increases the risk of a cryptanalyst recovering the original plain text. Because of this short cycle property, NIST does not support the use of the OFB mode for any amount of feedback less than 64 bits. Note that this short cycle property is not a problem with the DES algorithm, and would occur using any block cipher in a similar manner.

   Tables E1 and E2 in Appendix E are accurate examples for using the OFB mode with 1- and 8-bits of feedback. However, only 64-bits of feedback should be used, as stated above. Table E3 should be added, which gives an example for using 64-bits of feedback:

Table E3

An Example of the 64-bit Output Feedback Mode

The 64-bit OFB mode in the encrypt state has been selected.

Cryptographic Key = 0123456789abcdef

Initialization Vector = 1234567890abcdef

The plain text is the ASCII code for:
"We the people of the United States, in order to "

These seven-bit characters are written in hexadecimal notation (0, b7, b6,. . ., b1). The ⊕ represents bit-by-bit, modulo 2 addition. Note that all 64 bits of the DES output block are exclusive-ORed with the 64 bits of plain text.

TIME	DES INPUT BLOCK	DES OUTPUT BLOCK	⊕	P	=	C
1	1234567890abcdef	bd661569ae874e25	⊕	5765207468652070	=	ea03351dc6e26e55
2	ea03351dc6e26e55	f75b04e2a914a8b9	⊕	656f706c65206f66	=	9234748ecc34c7df
3	9234748ecc34c7df	d459dee65c9c67aa	⊕	2074686520556e69	=	f42db6837cc909c3
4	f42db6837cc909c3	dc1d0251dd29af70	⊕	7465642053746174	=	a87866718e5dce04
5	a87866718e5dce04	7890b81ad467a062	⊕	65732c20696e206f	=	1de3943abd09800d
6	1de3943abd09800d	baa00ff9674763ba	⊕	7264657220746f20	=	c8c46a8b47330c9a

Change No. 2 to FIPS PUB 81
Date of Change - 1996 May 31

In addition, the following editorial changes and updates are made to the Announcement Section of FIPS 81, DES Modes of Operation.

The introductory paragraph is updated as follows:

Federal Information Processing Standards (FIPS PUBS) are issued by the National Institute of Standards and Technology (NIST) after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Management Reform Act of 1996 and the Computer Security Act of 1987, Public Law 104-106.

Paragraph 3, Explanation; Paragraph 6, Related Documents; and Paragraph 9, Qualifications; are updated as follows:

All references to FIPS 46 are changed to FIPS 46-2, Data Encryption Standard, December 30, 1993.

Paragraph 5. Maintenance Agency. is updated as follows:

U.S. Department of Commerce, National Institute of Standards and Technology (NIST), Computer Systems Laboratory.

Paragraph 6, Related Documents, is updated as follows:

Delete references to Proposed Federal Standards 1026 and 1027. Add reference to FIPS 140-1, Security Requirements for Cryptographic Modules, January 11, 1994.

Paragraph 9, Qualifications, is updated as follows:

The DES modes of operation described in this standard are based upon information provided by many sources within the Federal Government and private industry. These modes are presently being implemented in cryptographic equipment containing DES devices. However, a standard of this nature must, of necessity, remain flexible enough to adapt to advancements and innovations in science and technology. As such, this standard should not be construed as being either exhaustive or static. It will be reviewed every five years in order to incorporate new implementations whose technical or economic merit justify the issuance of a revised standard. FIPS 46-2 requires implementation of the DES algorithm when agencies determine that cryptographic protection is required for unclassified information. FIPS 46-2 and this standard may be implemented in hardware, software, or firmware, or any combination thereof. Cryptographic modules which implement this standard shall conform to the requirements of FIPS 140-1.

Paragraph 10, Export Control, is updated as follows:

Cryptographic devices and technical data regarding them are subject to Federal Government export controls as specified in Title 22, Code of Federal Regulations, Parts 120

through 131 (International Traffic of Arms Regulations -- ITAR). Some exports of cryptographic modules implementing this standard and technical data regarding them must comply with these Federal regulations and be licensed by the U.S. Department of State. Other exports of cryptographic modules implementing this standard and technical data regarding them fall under the licensing authority of the Bureau of Export Administration of the U.S. Department of Commerce. The Department of Commerce is responsible for licensing cryptographic devices used for authentication, access control, proprietary software, automatic teller machines (ATMs), and certain devices used in other equipment and software. For advice concerning which agency has licensing authority for a particular cryptographic device, please contact the respective agencies.

Paragraph 12, Implementation Schedule, is updated as follows:

This standard became effective on June 2, 1981.

Paragraph 13, Waivers, is updated as follows:

Under certain exceptional circumstances, the heads of Federal departments and agencies may approve waivers to Federal Information Processing Standards (FIPS). The head of such agency may re-delegate such authority only to a senior official designated pursuant to section 3506(a) of Title 44, U.S. Code. Waivers shall be granted only when:

a. Compliance with a standard would adversely affect the accomplishment of the mission of an operator of a Federal computer system, or

b. Cause a major adverse financial impact on the operator which is not offset by Government-wide savings.

Agency heads may act upon a written waiver request containing the information detailed above. Agency heads may also act without a written waiver request when they determine that conditions for meeting the standard cannot be met. Agency heads may approve waivers only by a written decision which explains the basis on which the agency head made the required finding(s). A copy of each such decision, with procurement sensitive or classified portions clearly identified, shall be sent to: National Institute of Standards and Technology; ATTN: FIPS Waiver Decisions, Building 820, Room 509; Gaithersburg, MD 20899.

In addition, notice of each waiver granted and each delegation of authority to approve waivers shall be sent promptly to the Committee on Government Reform and Oversight of the House of Representatives and the Committee on Governmental Affairs of the Senate and shall be published promptly in the Federal Register.

When the determination on a waiver applies to the procurement of equipment and/or services, a notice of the waiver determination must be published in the Commerce Business Daily as a part of the notice of solicitation for offers of an acquisition or, if the waiver determination is made after that notice is published, by amendment to such notice.

Change No. 2 to FIPS PUB 81
Date of Change - 1996 May 31

A copy of the waiver, any supporting documents, the document approving the waiver and any supporting and accompanying documents, with such deletions as the agency is authorized and decides to make under 5 U.S.C. Section 552(b), shall be part of the procurement documentation and retained by the agency.
