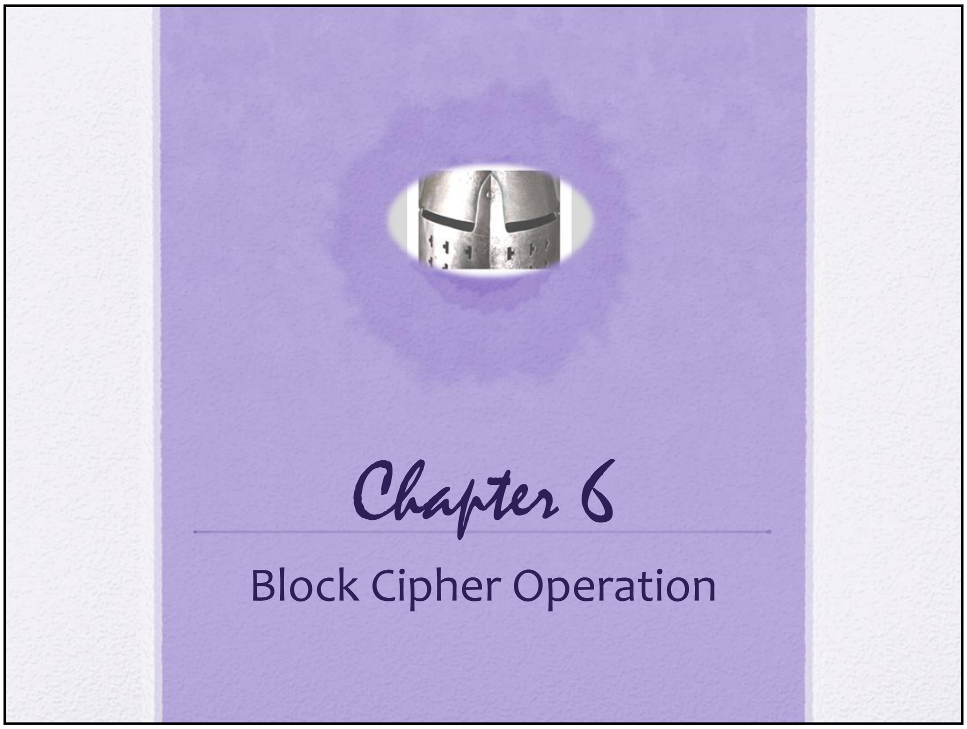
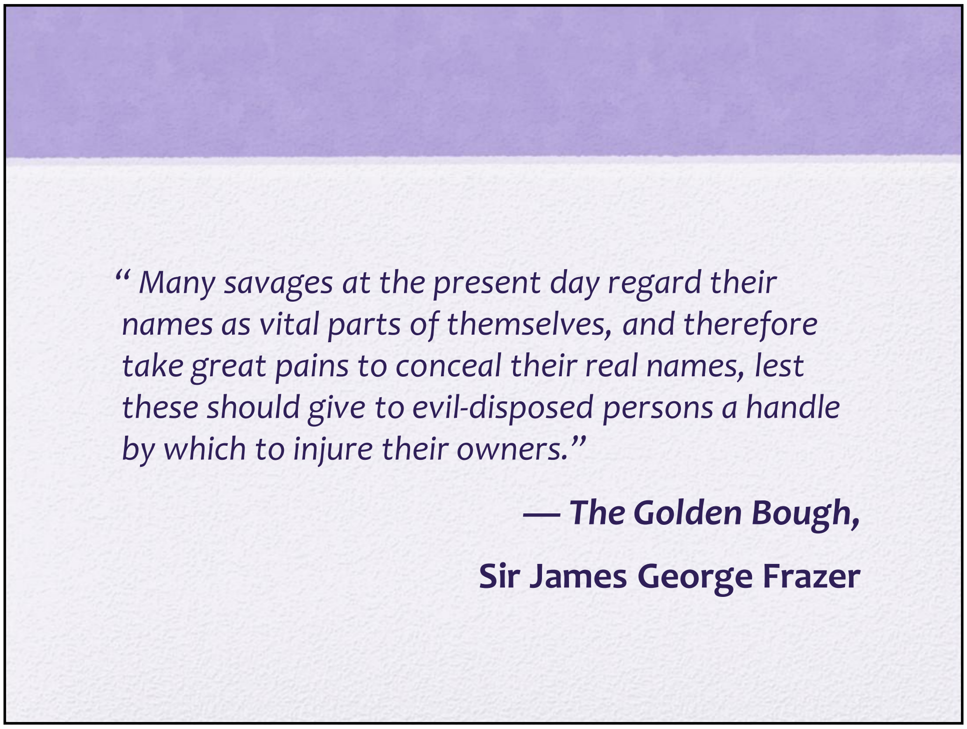


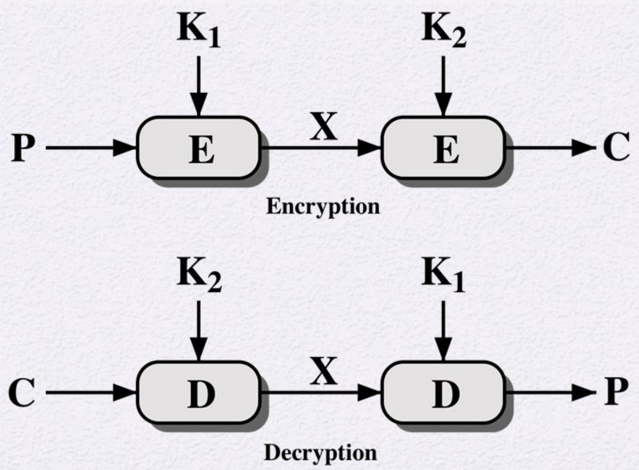
Chapter 6

Block Cipher Operation



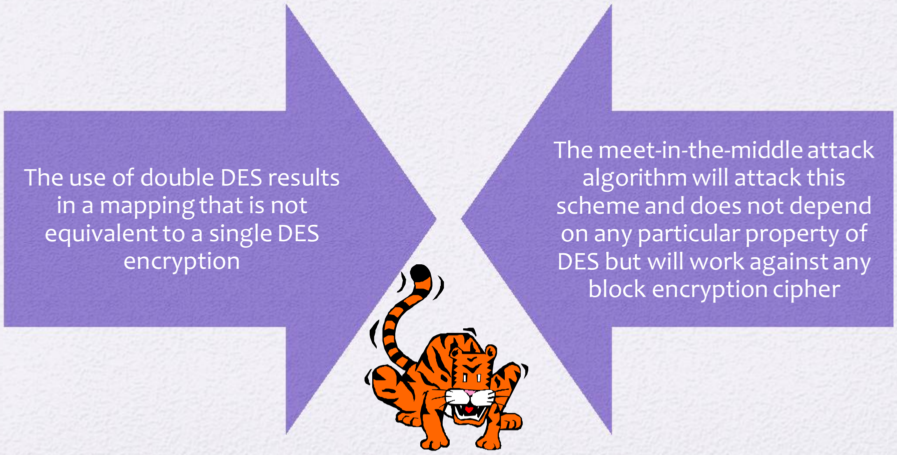
> *" Many savages at the present day regard their names as vital parts of themselves, and therefore take great pains to conceal their real names, lest these should give to evil-disposed persons a handle by which to injure their owners."*
>
> ***— The Golden Bough,***
>
> **Sir James George Frazer**

Double DES



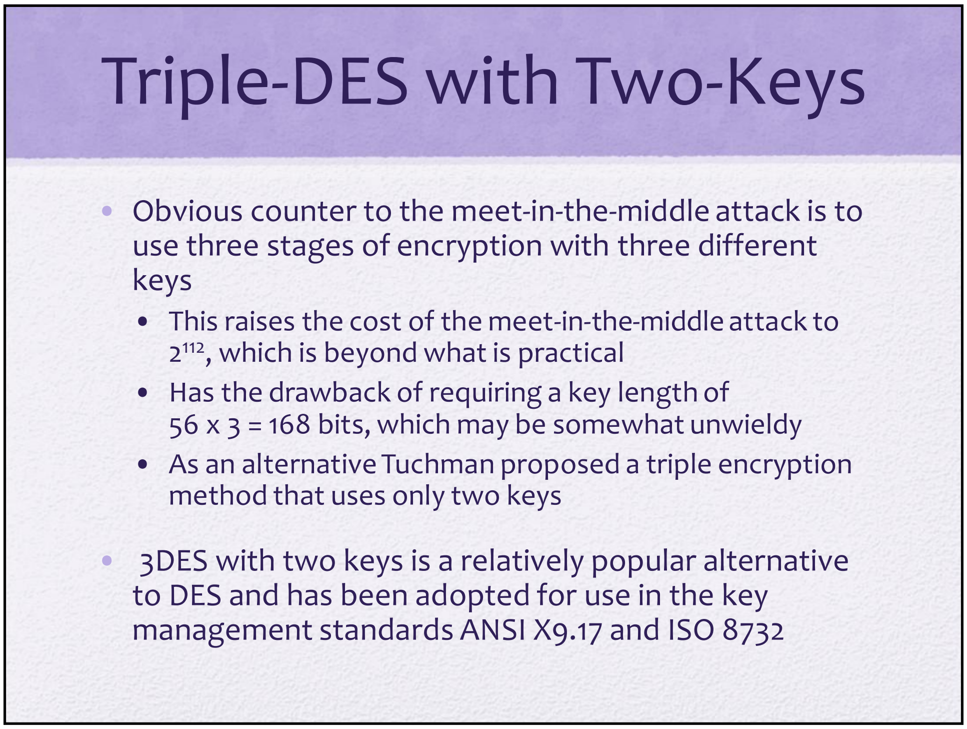
(a) Double Encryption

Meet-in-the-Middle Attack



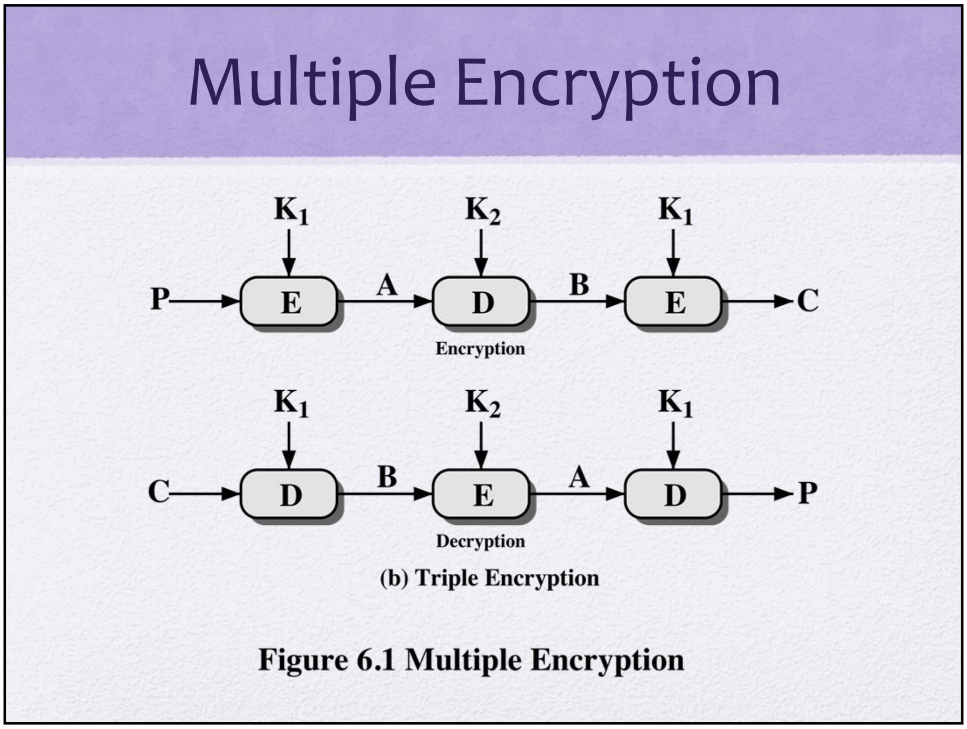
The use of double DES results in a mapping that is not equivalent to a single DES encryption

The meet-in-the-middle attack algorithm will attack this scheme and does not depend on any particular property of DES but will work against any block encryption cipher



Triple-DES with Two-Keys

- Obvious counter to the meet-in-the-middle attack is to use three stages of encryption with three different keys
  - This raises the cost of the meet-in-the-middle attack to 2^{112}, which is beyond what is practical
  - Has the drawback of requiring a key length of 56 x 3 = 168 bits, which may be somewhat unwieldy
  - As an alternative Tuchman proposed a triple encryption method that uses only two keys
- 3DES with two keys is a relatively popular alternative to DES and has been adopted for use in the key management standards ANSI X9.17 and ISO 8732



Multiple Encryption

(b) Triple Encryption

Figure 6.1 Multiple Encryption

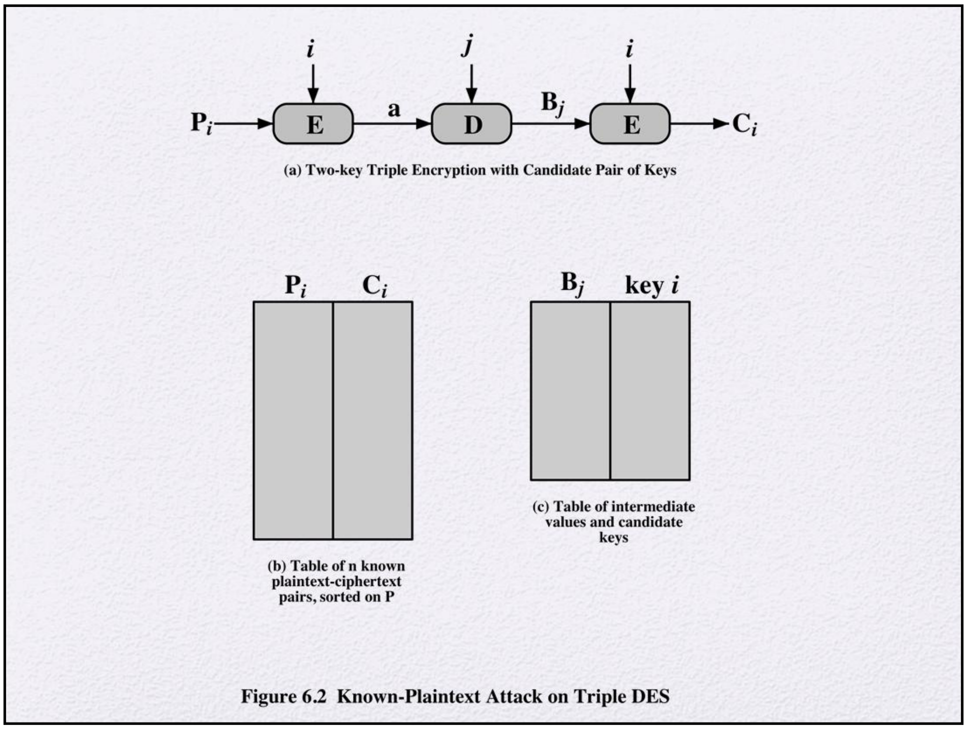
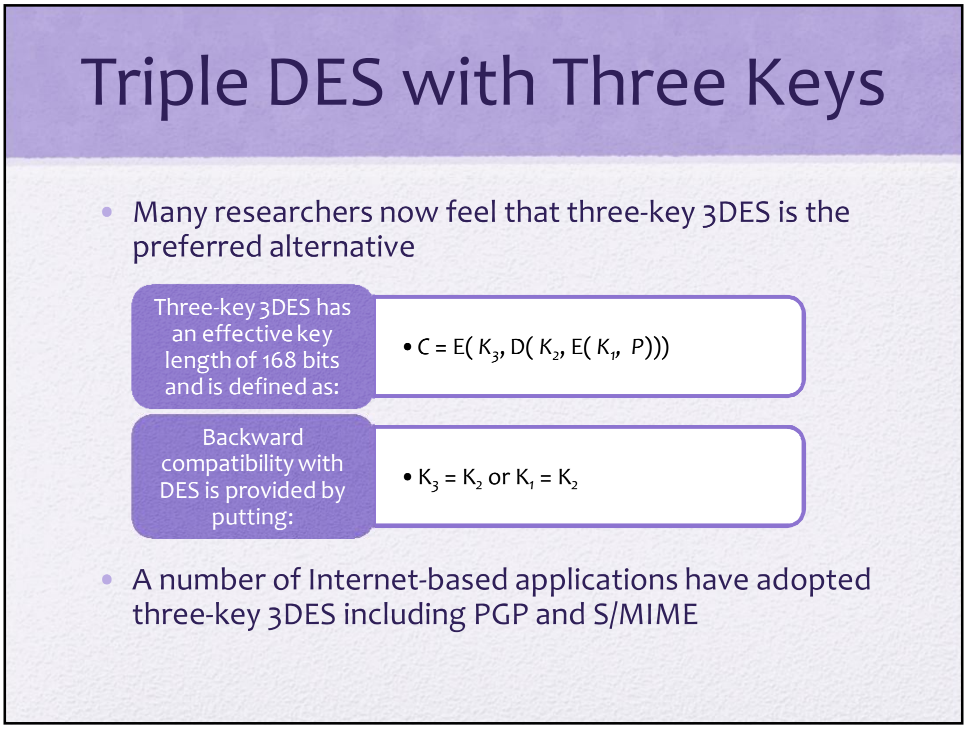

i
j
i
P_i
E
a
D
B_j
E
C_i
(a) Two-key Triple Encryption with Candidate Pair of Keys
P_i
C_i
B_j
key i
(b) Table of n known plaintext-ciphertext pairs, sorted on P
(c) Table of intermediate values and candidate keys

Figure 6.2 Known-Plaintext Attack on Triple DES



Triple DES with Three Keys

- Many researchers now feel that three-key 3DES is the preferred alternative

Three-key 3DES has an effective key length of 168 bits and is defined as:

- $C = E(K_3, D(K_2, E(K_1, P)))$

Backward compatibility with DES is provided by putting:

- $K_3 = K_2$ or $K_1 = K_2$

- A number of Internet-based applications have adopted three-key 3DES including PGP and S/MIME

Modes of Operation

- A technique for enhancing the effect of a cryptographic algorithm or adapting the algorithm for an application
- To apply a block cipher in a variety of applications, five *modes of operation* have been defined by NIST
  - The five modes are intended to cover a wide variety of applications of encryption for which a block cipher could be used
  - These modes are intended for use with any symmetric block cipher, including triple DES and AES

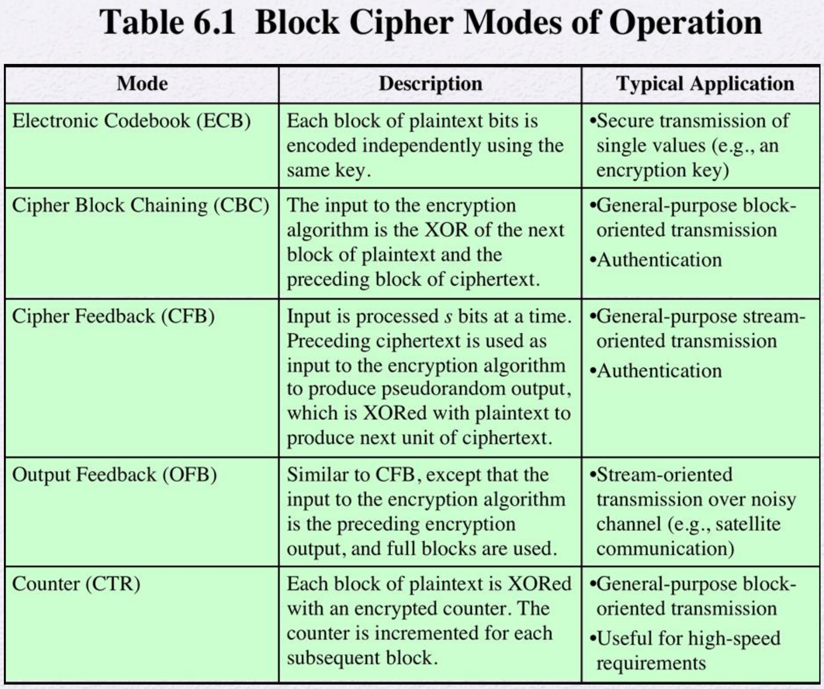
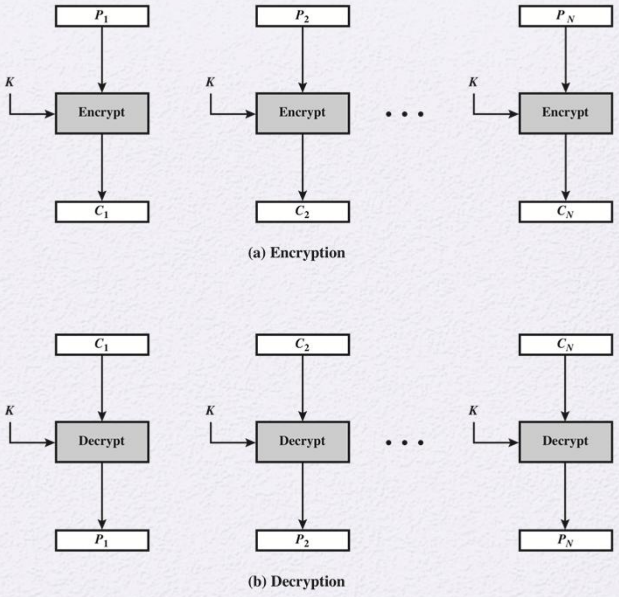


Table 6.1 Block Cipher Modes of Operation

Mode	Description	Typical Application
Electronic Codebook (ECB)	Each block of plaintext bits is encoded independently using the same key.	•Secure transmission of single values (e.g., an encryption key)
Cipher Block Chaining (CBC)	The input to the encryption algorithm is the XOR of the next block of plaintext and the preceding block of ciphertext.	•General-purpose block-oriented transmission •Authentication
Cipher Feedback (CFB)	Input is processed *s* bits at a time. Preceding ciphertext is used as input to the encryption algorithm to produce pseudorandom output, which is XORed with plaintext to produce next unit of ciphertext.	•General-purpose stream-oriented transmission •Authentication
Output Feedback (OFB)	Similar to CFB, except that the input to the encryption algorithm is the preceding encryption output, and full blocks are used.	•Stream-oriented transmission over noisy channel (e.g., satellite communication)
Counter (CTR)	Each block of plaintext is XORed with an encrypted counter. The counter is incremented for each subsequent block.	•General-purpose block-oriented transmission •Useful for high-speed requirements

Electronic Codebook Mode (ECB)



(a) Encryption

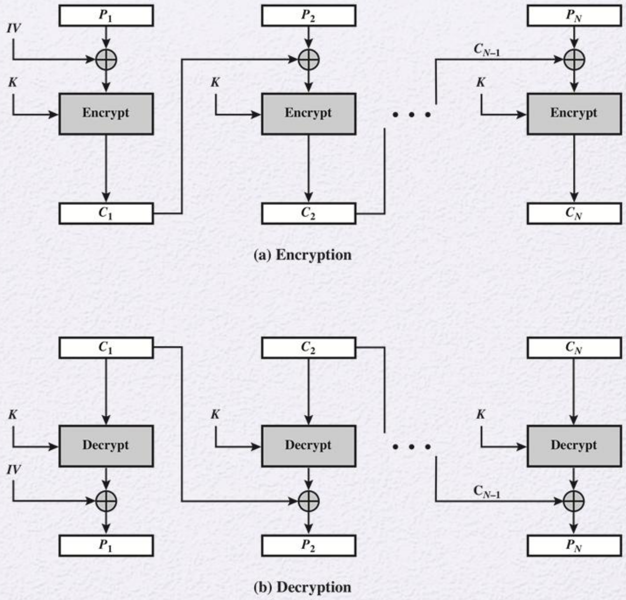
(b) Decryption

Figure 6.3 Electronic Codebook (ECB) Mode

Criteria and properties for evaluating and constructing block cipher modes of operation that are superior to ECB:

- Overhead
- Error recovery
- Error propagation
- Diffusion
- Security

Cipher Block Chaining (CBC)



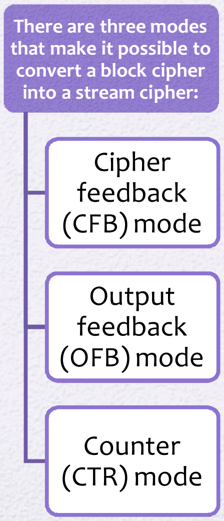
(a) Encryption

(b) Decryption

Figure 6.4 Cipher Block Chaining (CBC) Mode

Cipher Feedback Mode

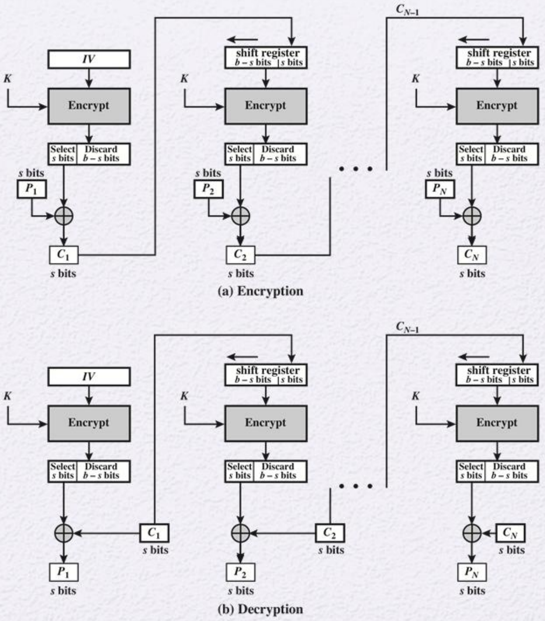
- For AES, DES, or any block cipher, encryption is performed on a block of *b* bits
  - In the case of DES *b* = 64
  - In the case of AES *b* = 128



There are three modes that make it possible to convert a block cipher into a stream cipher:

- Cipher feedback (CFB) mode
- Output feedback (OFB) mode
- Counter (CTR) mode

s-bit Cipher Feedback (CFB) Mode

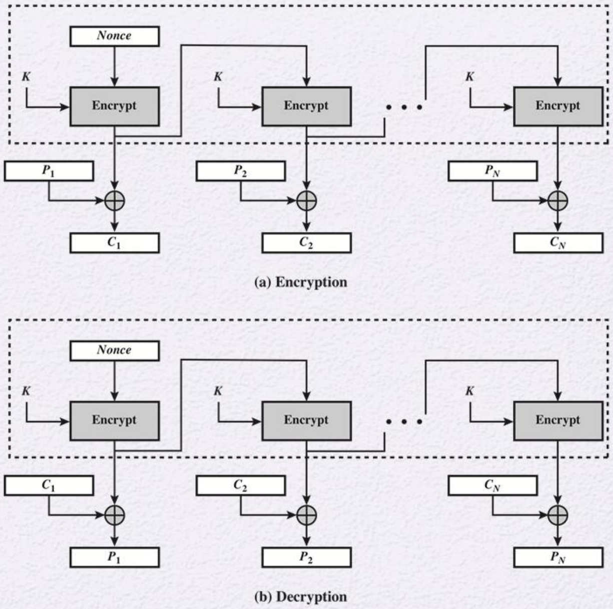


(a) Encryption

(b) Decryption

Figure 6.5 *s*-bit Cipher Feedback (CFB) Mode

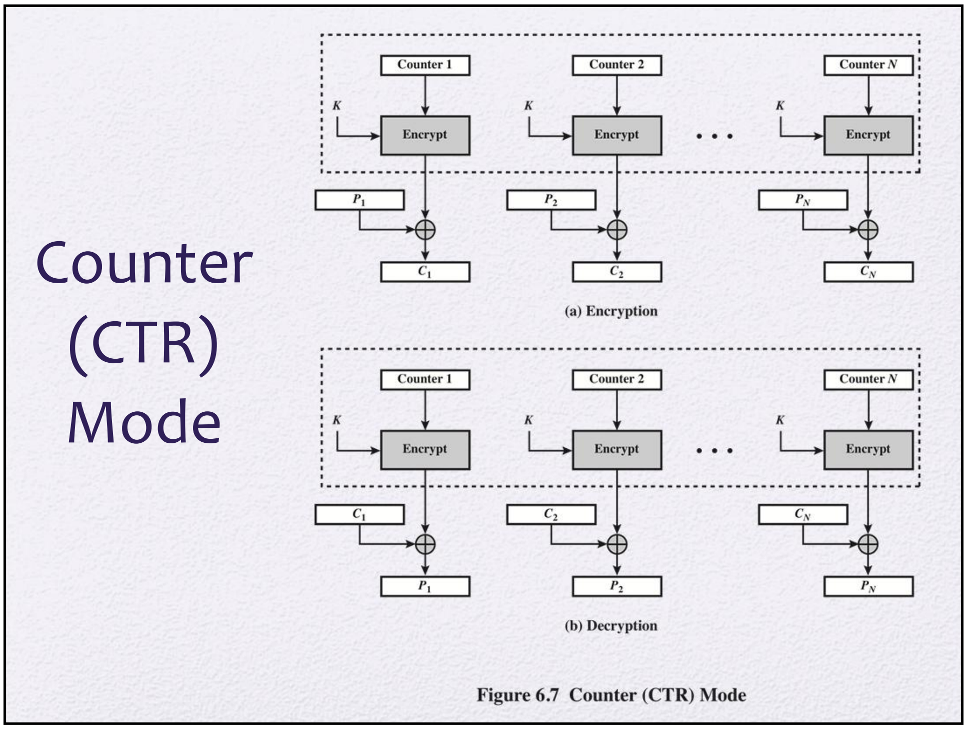
Output Feedback (OFB) Mode



(a) Encryption

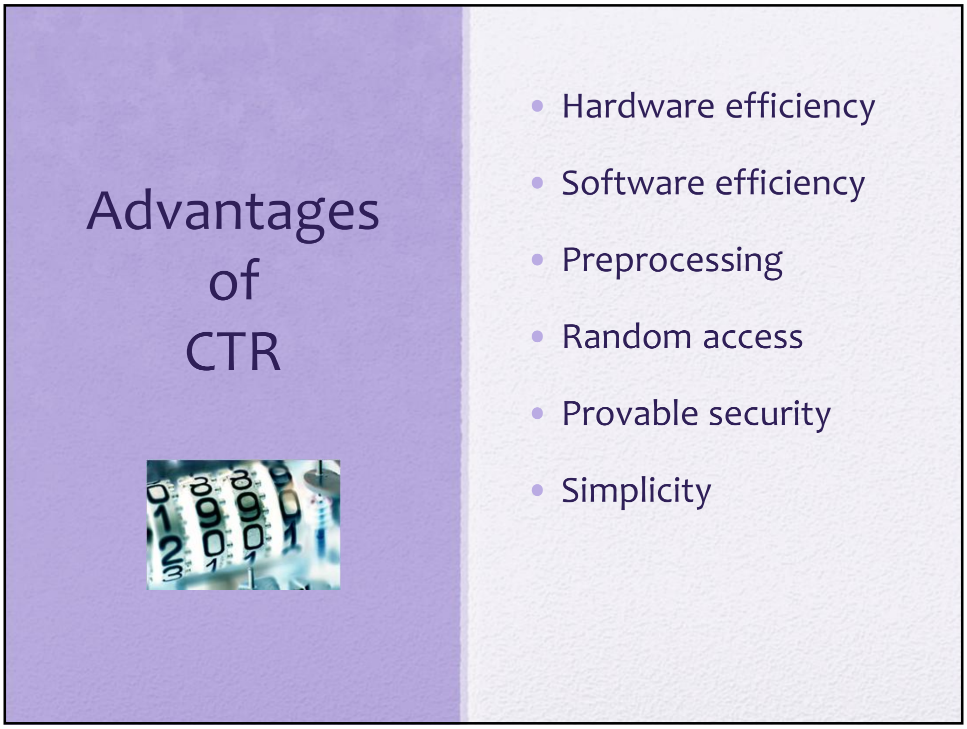
(b) Decryption

Figure 6.6 Output Feedback (OFB) Mode



Counter (CTR) Mode

Figure 6.7 Counter (CTR) Mode



Advantages of CTR

- Hardware efficiency
- Software efficiency
- Preprocessing
- Random access
- Provable security
- Simplicity

Feedback Characteristics of Modes of Operation

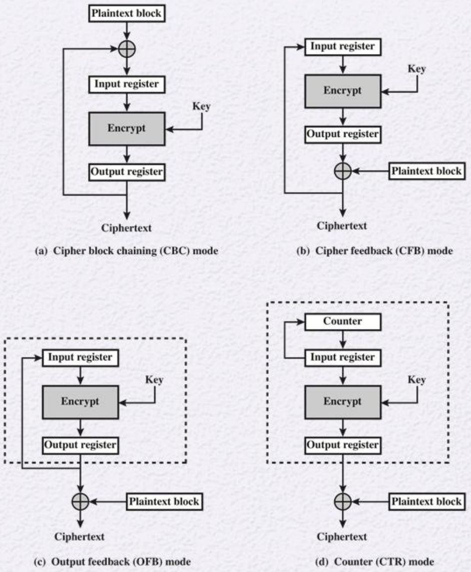
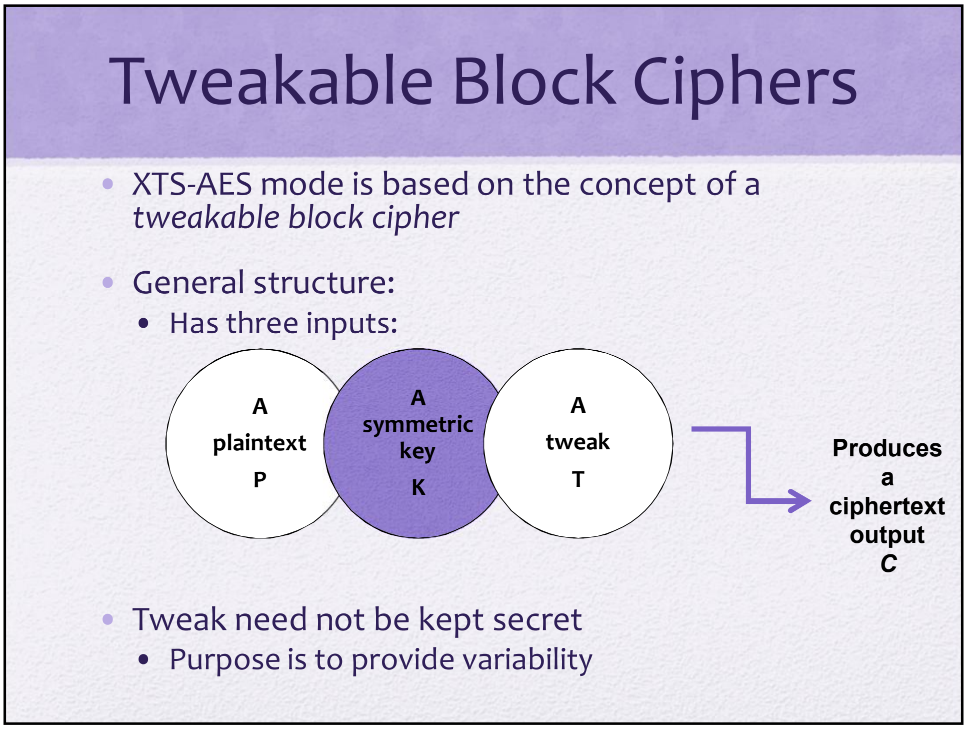


Figure 6.8 Feedback Characteristic of Modes of Operation

XTS-AES Mode for Block-Oriented Storage Devices

- Approved as an additional block cipher mode of operation by NIST in 2010
- Mode is also an IEEE Standard, IEEE Std 1619-2007
  - Standard describes a method of encryption for data stored in sector-based devices where the threat model includes possible access to stored data by the adversary
  - Has received widespread industry support

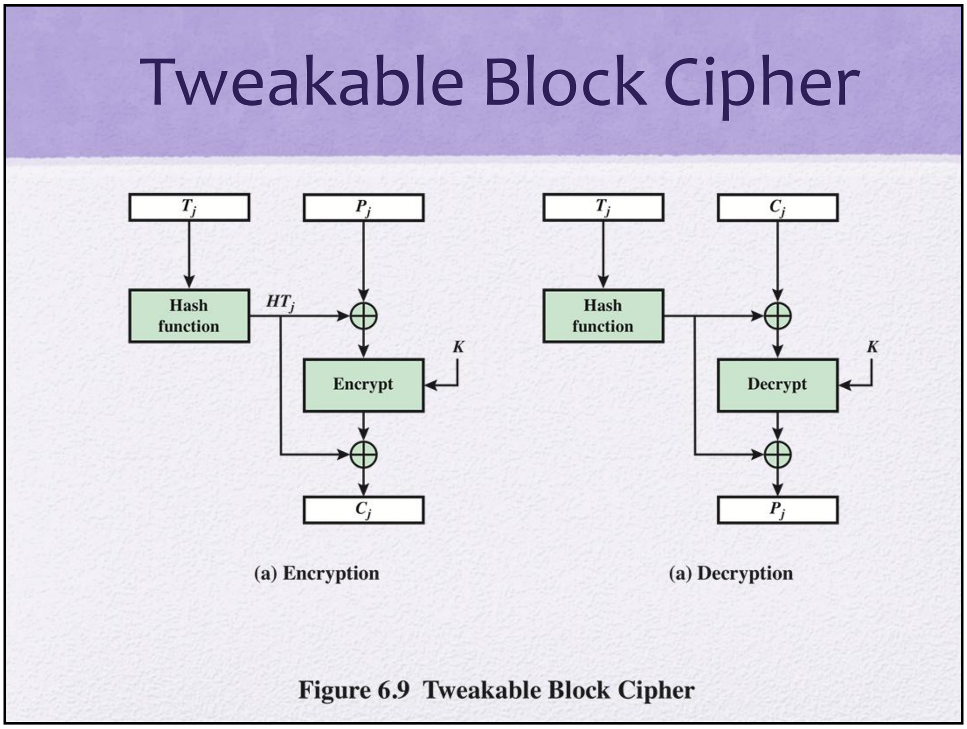


Tweakable Block Ciphers

- XTS-AES mode is based on the concept of a *tweakable block cipher*
- General structure:
  - Has three inputs:

A
plaintext
P
A
symmetric
key
K
A
tweak
T
Produces
a
ciphertext
output
C

- Tweak need not be kept secret
  - Purpose is to provide variability



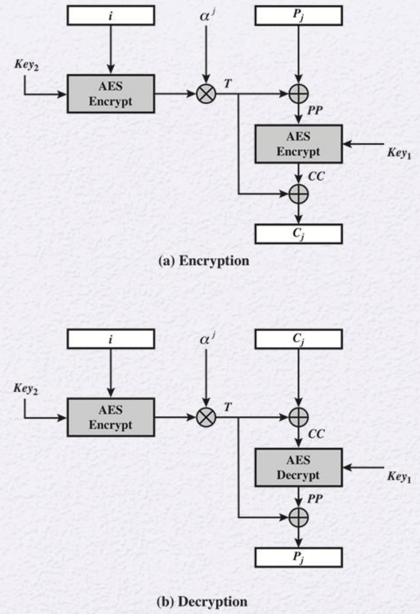
Tweakable Block Cipher

(a) Encryption

(a) Decryption

Figure 6.9 Tweakable Block Cipher

XTS-AES Operation on Single Block

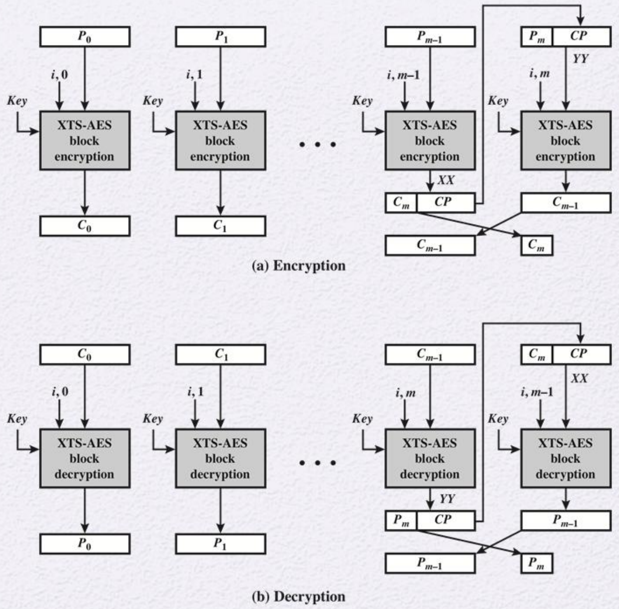


(a) Encryption

(b) Decryption

Figure 6.10 XTS-AES Operation on Single Block

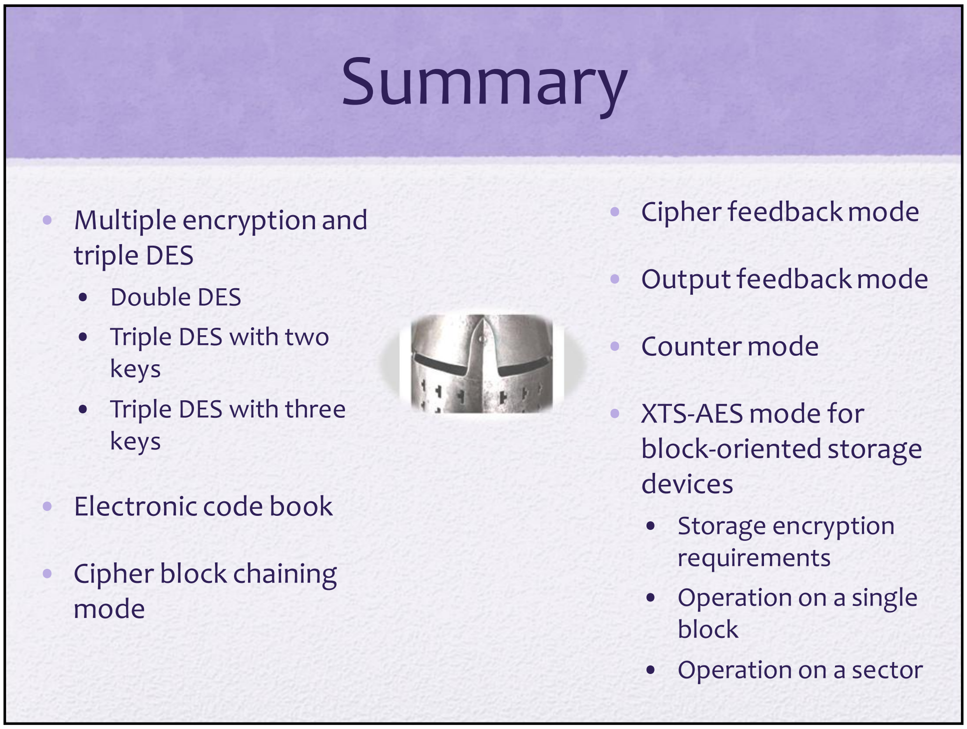
XTS–AES Mode



(a) Encryption

(b) Decryption

Figure 6.11 XTS-AES Mode



Summary

- Multiple encryption and triple DES
  - Double DES
  - Triple DES with two keys
  - Triple DES with three keys
- Electronic code book
- Cipher block chaining mode
- Cipher feedback mode
- Output feedback mode
- Counter mode
- XTS-AES mode for block-oriented storage devices
  - Storage encryption requirements
  - Operation on a single block
  - Operation on a sector