Introduction to Computer Security

M2 - Symmetric Key Cryptography

Dongfeng (Phoenix) Fang

California Polytechnic State University
San Luis Obispo

Winter, 2025

Contents

About Cryptography

Overview of Cryptography in Security

Based on science (mathematics);

An indispensable tool to provide information security;

- Symmetric Key Cryptography
- Public Key Cryptography

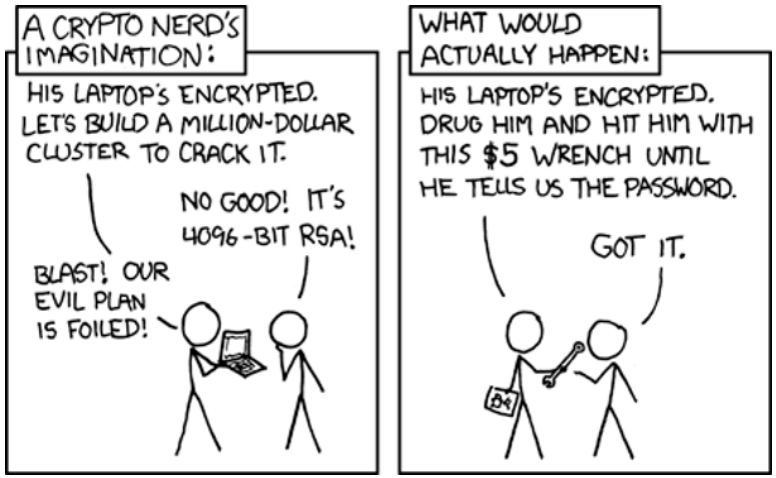


Figure: A thought on cryptography

Cryptographic Issues

In the "Top3" of application flaws;

Data protection regulations have grown increasingly complex;

Implementation of data protection during different phases (transmitting, processing, and storing sensitive data);

Implementation problems (poor password management, weak pseudorandom number generation, use of insecure cryptography).

Cryptanalysis

Goal: Recover key not just messages;

General approaches:

- Cryptanalytic attack: rely on the nature of the algorithm and some knowledge of the general characteristics of the plaintext or even some sample plaintext-ciphertext pairs;
- Brute-force attack: try all possible keys on a piece of ciphertext until an intelligible translation into plaintext is obtained.

What should you do with crypto?

Do

- Understand the tools - not every problem needs a hammer;
- Use tested and trusted implementations;
- Wait for new and exciting improvements to be tested before using it.

Don't

- Try to solve all security problems;
- Use custom implementations.

Classical Encryption Techniques

Symmetric Cipher Model

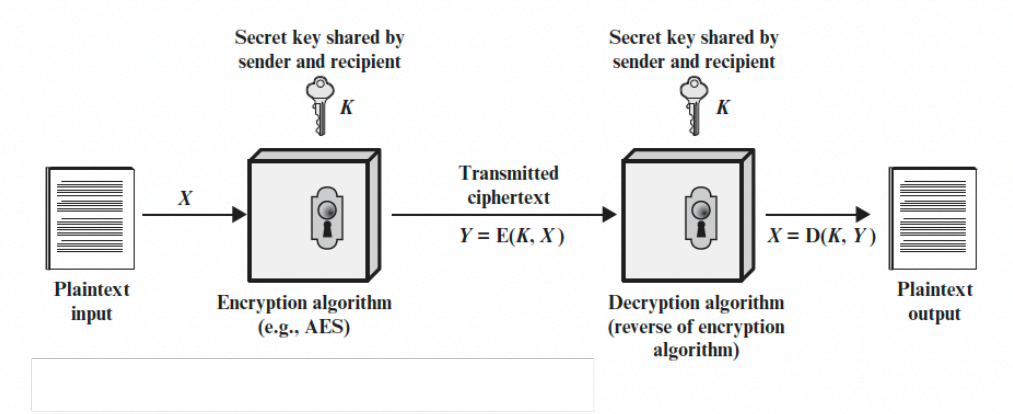


Figure: Simplified Model of Symmetric Encryption/Decryption

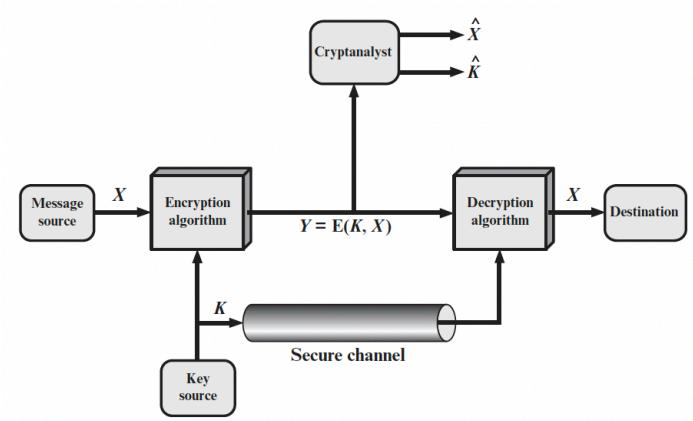


Figure: Model of Symmetric Cryptosystem

Substitution Techniques

One in which the letters of plaintext are replaced by other letters or by numbers or symbols.

- Caesar Cipher
- Monoalphabetic Cipher

```
plain:  a b c d e f g h i j k l m n o p q r s t u v w x y z
cipher: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
```

Figure: Plaintext and Ciphertext

Can we break them easily?

Transposition Techniques

Achieved by performing some sort of permutation on the plaintext letters.

```
Key:          4 3 1 2 5 6 7
Plaintext:    a t t a c k p
              o s t p o n e
              d u n t i l t
              w o a m x y z
Ciphertext:   TTNAAPTMTSUOAODWCOIXKNLYPETZ
```

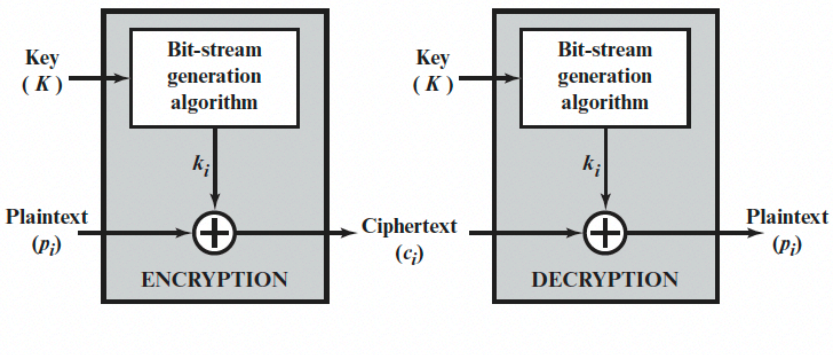
Figure: An Example of Transposition Techniques

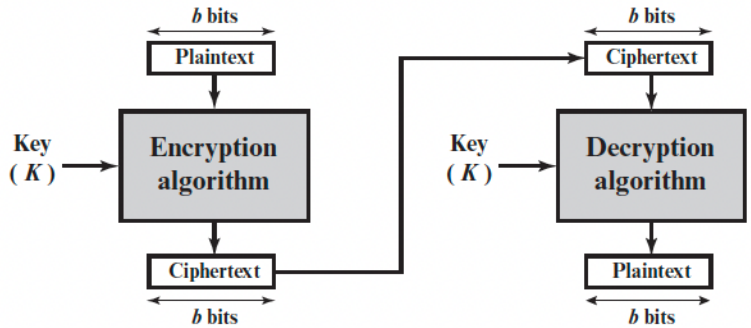
Can we break them easily?

Block Cipher

Modern Symmetric Cipher

- Stream Cipher: encrypts a digital stream one bit or one byte at a time.
- Block Cipher: a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length.





Claude Shannon and Substitution-Permutation Ciphers

Claude Shannon introduced the idea of substitution-permutation (S-P) networks in the 1949 paper;

Form basis of modern block ciphers;

S-P ciphers are based on the two primitive cryptographic operations seen before:

- Substitution (S-box);
- Permutation (P-Box).

Provide confusion and diffusion of messages and keys:

- Diffusion: The statistical structure of the plaintext is dissipated into long-range statistics of the ciphertext.
- Confusion: the relationship between the statistics of the ciphertext and the value of the encryption key is as complex as possible.

About Block Ciphers

Unique mapping from Plaintexts to Ciphertexts;

Block cipher parameters and desired features:

- Block size;
- Key size;
- Fast software encryption/decryption;
- Ease of analysis.

The Data Encryption Standard

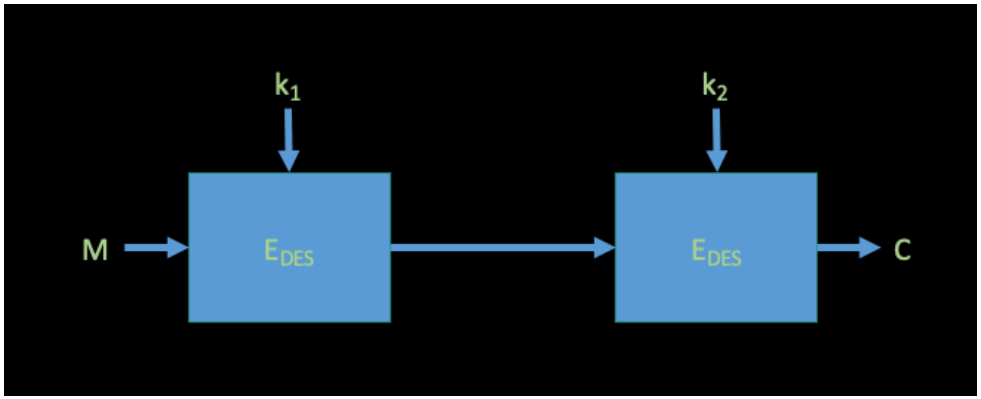
DES was issued in 1977 by NIST as a federal information processing standard;

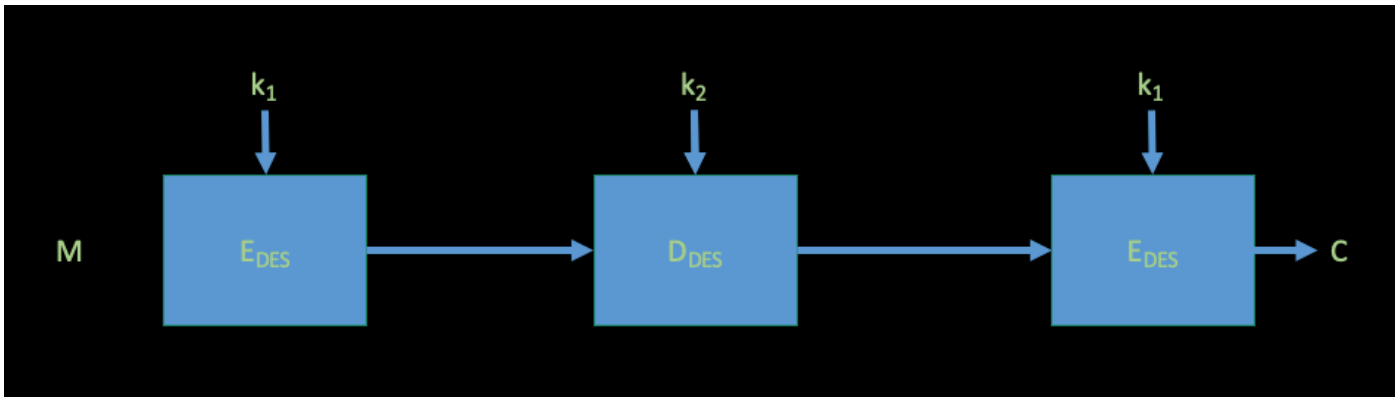
64-bit for each block;

Generally considered broken.

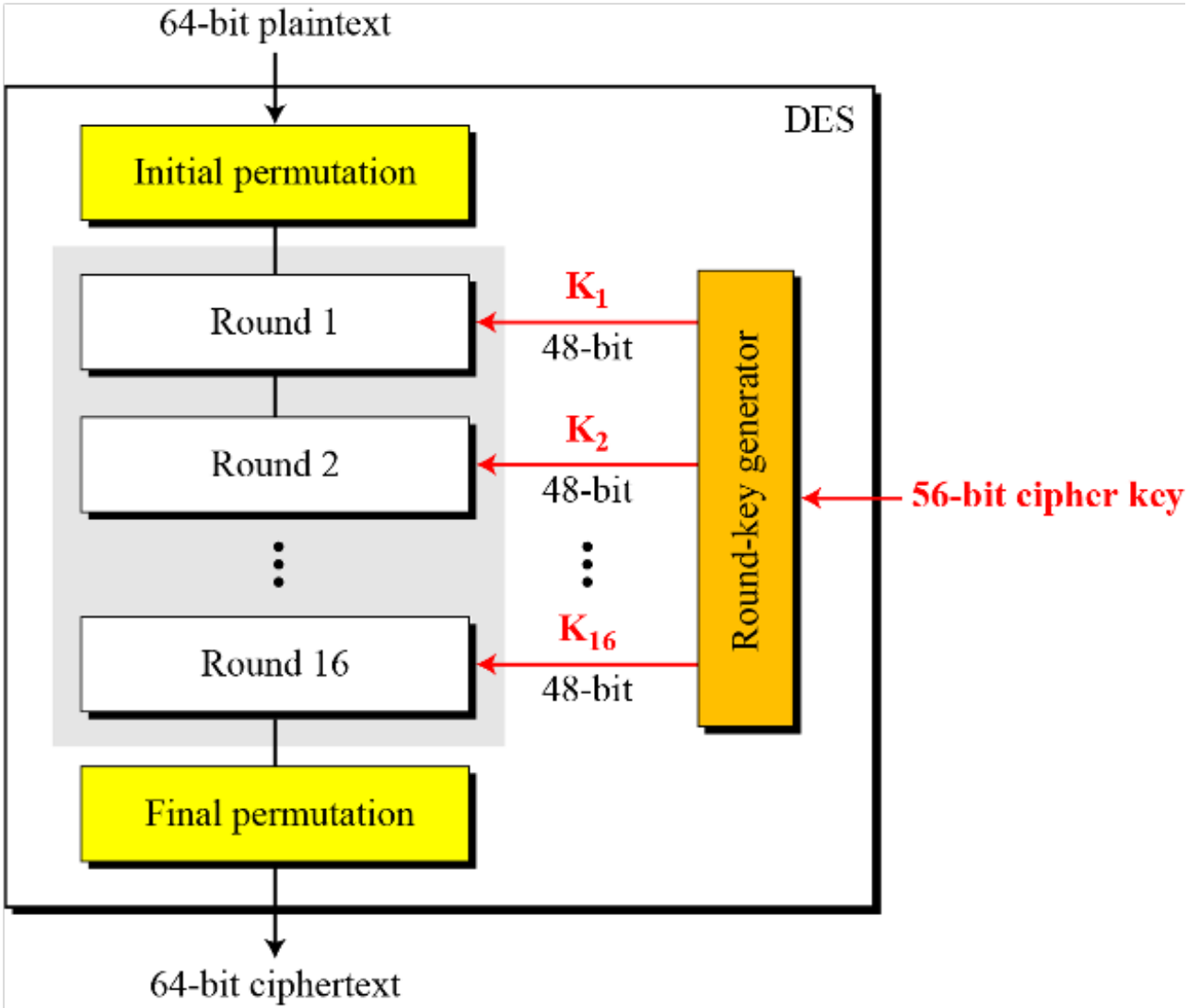
Key Size (bits)	Cipher	Number of Alternative Keys	Time Required at 10^9 Decryptions/s	Time Required at 10^{13} Decryptions/s
56	DES	$2^{56} \approx 7.2 \times 10^{16}$	2^{55} ns = 1.125 years	1 hour

What About Double DES and Triple DES?





EDE vs EEE


64-bit plaintext
DES
Initial permutation
Round 1
Round 2
Round 16
Final permutation
K_1
48-bit
K_2
48-bit
K_{16}
48-bit
Round-key generator
56-bit cipher key
64-bit ciphertext

AES

The Advanced Encryption Standard;

Symmetric key block cipher;

Published by NIST in 2001;

Security: effort for practical cryptanalysis;

Cost: in terms of computational efficiency;

Implementation

AES Details

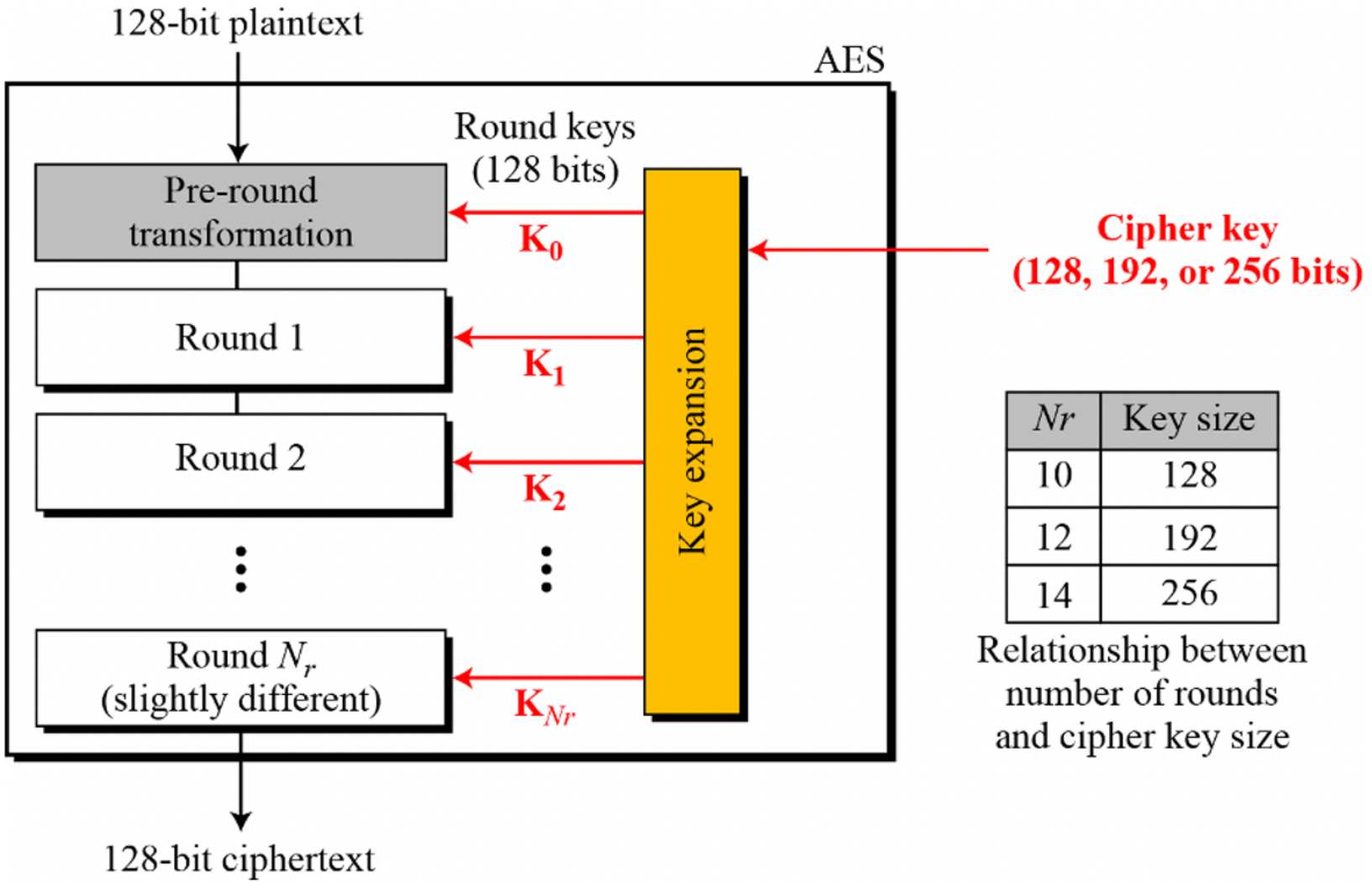
Rijndael: a non-Feistel Cipher;

Blcok size: 128 bits;

Three different key sizes:

- 128 bits (10 rounds)
- 192 bits (12 rounds)
- 256 bits (14 rounds)

General Design of AES Encryption Cipher



Nr	Key size
10	128
12	192
14	256

Relationship between number of rounds and cipher key size

Cryptographic APIs

Cryptlib;

OpenSSL;

Crypt++;

BASFE;

Cryptix;

And more.

Practical Considerations

Encoding arbitrary length messages;

Encoding messages greater than n-bits;

Different modes of operations.

Modes of Operation - Goals

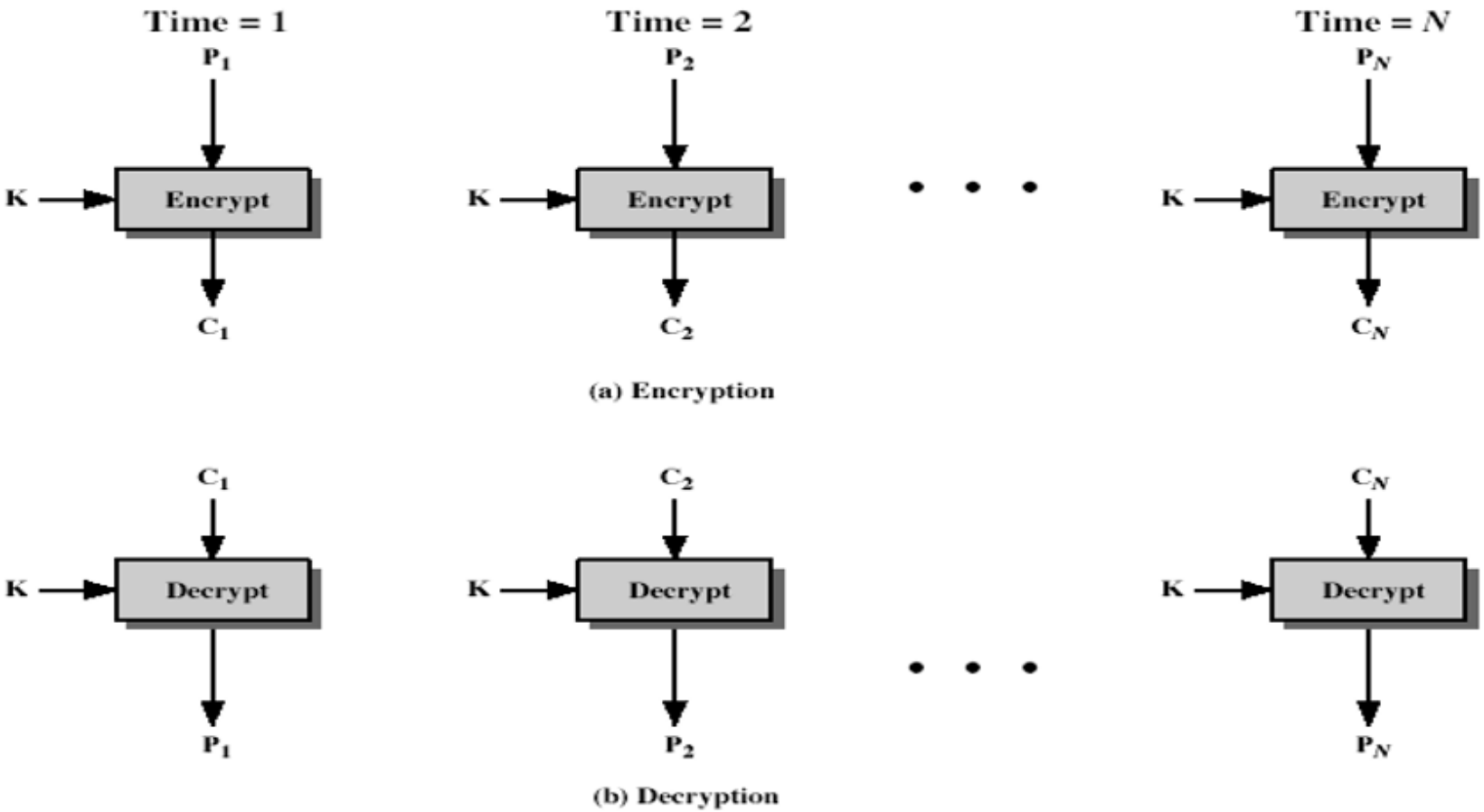
- Information leakage - Should be avoided;
- Ciphertext manipulation - Can a simple change in ciphers cause predictable plaintext changes?
- Parallelization - This is great with modern GPUs;
- Error propagation - Can this be avoided?

Block Cipher Modes of Operation

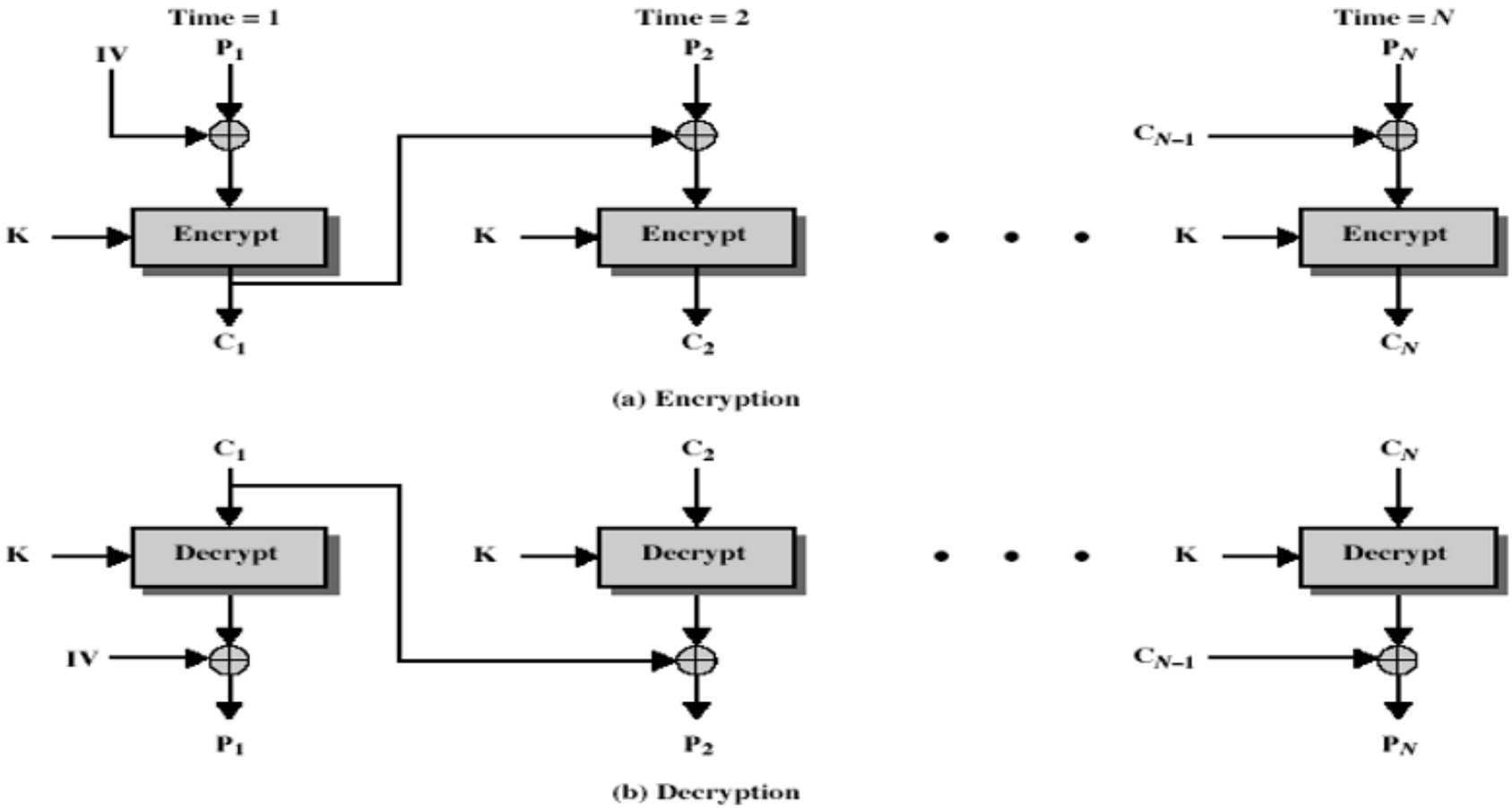
Table 6.1 Block Cipher Modes of Operation

Mode	Description	Typical Application
Electronic Codebook (ECB)	Each block of 64 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 64 bits of plaintext and the preceding 64 bits 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 DES output.	•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

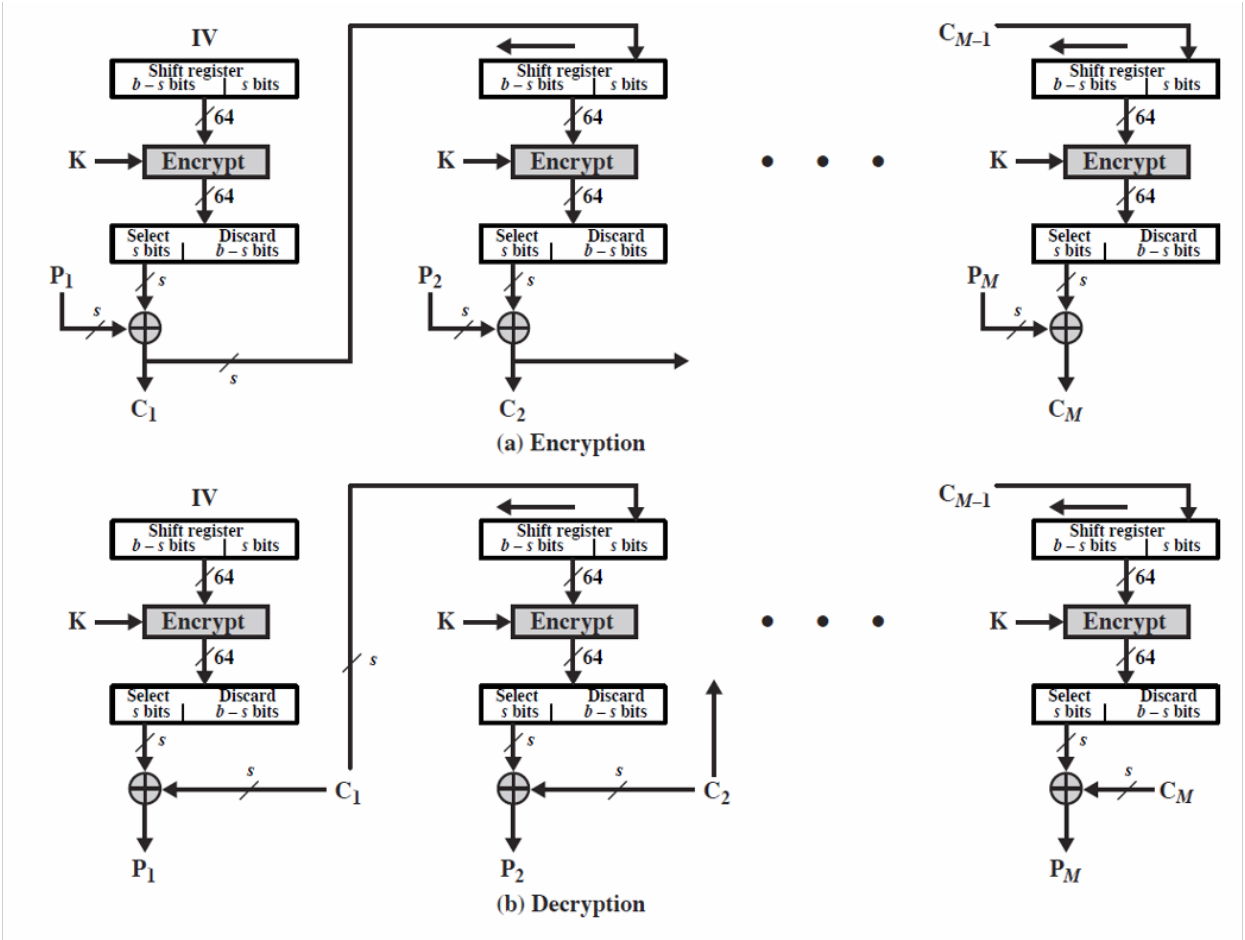
Electronic Code Book (ECB)



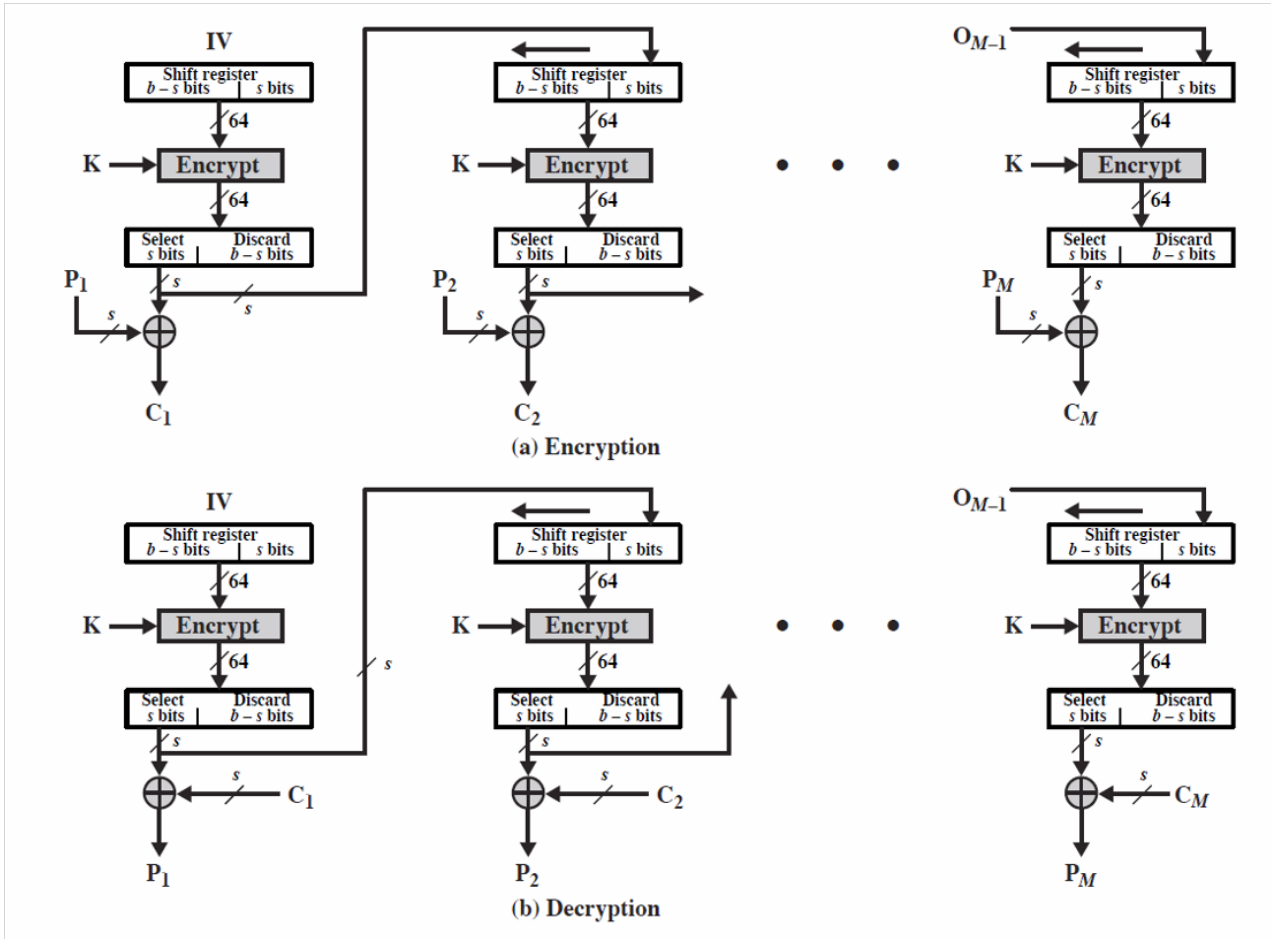
Cipher Block Chaining (CBC)



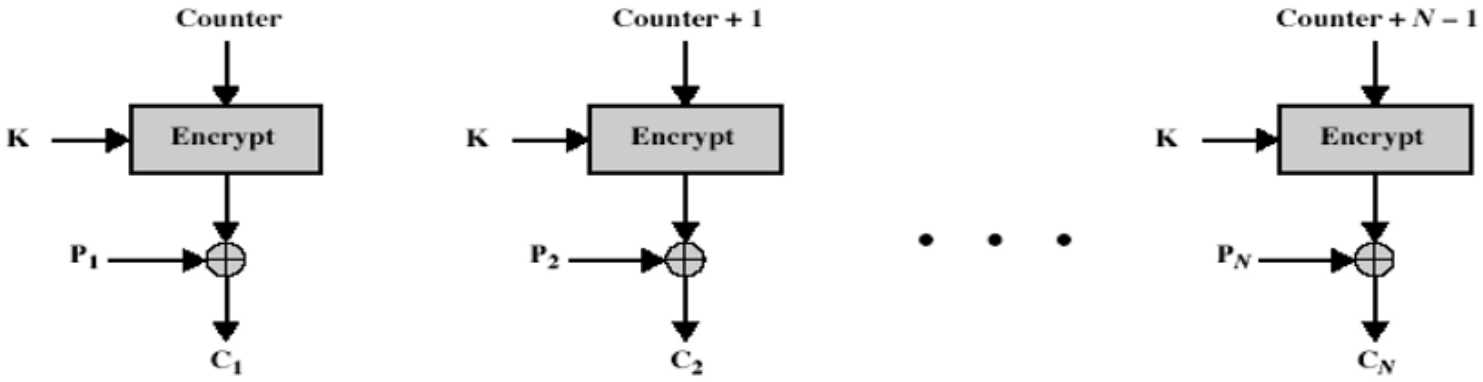
Cipher Feedback (CFB)



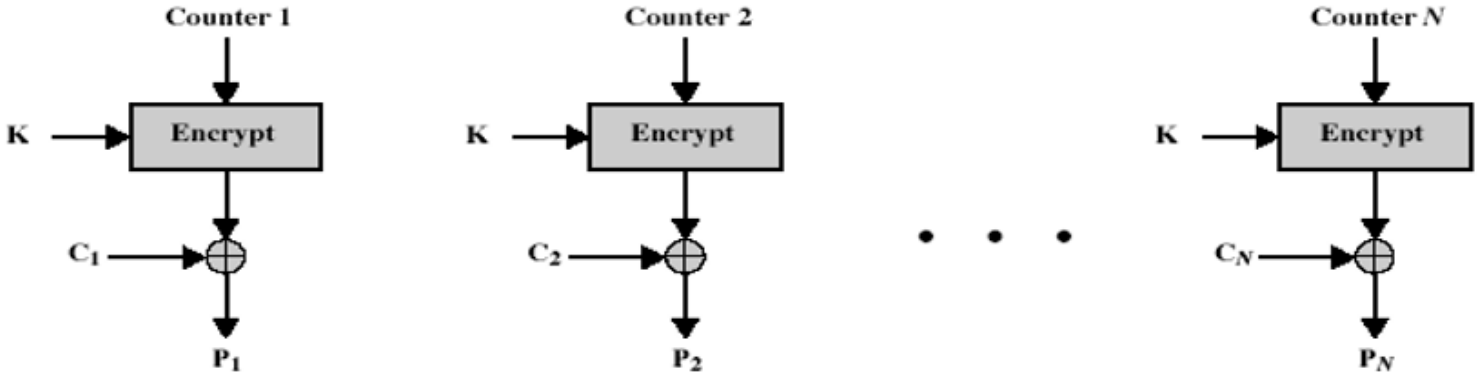
Output Feedback (OFB)



Counter Mode (CTR)



(a) Encryption



(b) Decryption

Conlusion

Conlusion of Symmetric Key Cryptography

- Applications
- Challenges