

Information Security

Prepared by Dr. Ahmed Omar

IT373

Information Security

Lecture 2



Symmetric Encryption & Standards

Lecture 2

IT373
Information Security

Prepared by
Dr. Ahmed Omar

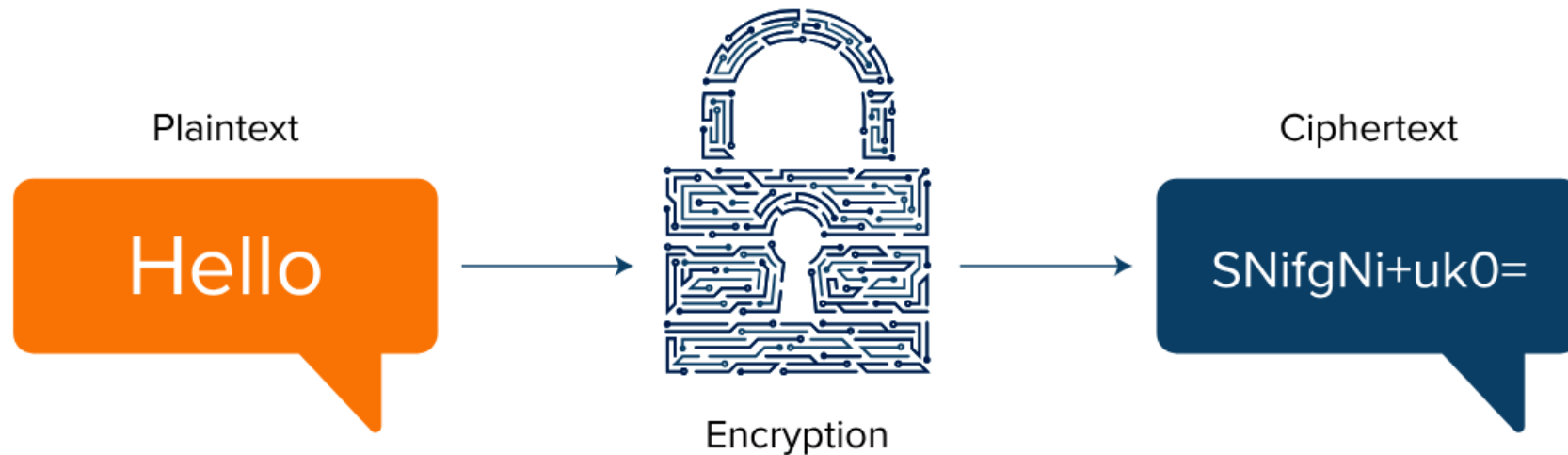
Agenda/Outline

- Cryptography
 - History
 - Modern Cryptology Origins
 - Classification of Cryptography Algorithms
- Symmetric Encryption
 - Requirements for Secure Symmetric Encryption
 - Symmetric Block Encryption Algorithms
 - Data Encryption Standard (D E S)
 - Advanced Encryption Standard (A E S)



Cryptography: Definition and Key Concepts

- Cryptography is the practice of securing communication and information by transforming it into an unreadable format for unauthorized users.



Cryptography vs Encryption

- ❑ **Cryptography** is the broader field (the science); **encryption** is a specific tool within that field (the process)
- ❑ **Cryptography** is about studying methods to keep messages secret; **encryption** is about the actual process of encoding and decoding data
- ❑ **Encryption** is one of several techniques used to achieve **cryptographic** goals

Cryptography Classification

Cryptography is classified along three independent dimensions:

1. The **type of operations** used for transforming plaintext to ciphertext

- ☐ **Substitution:** Each element in the plaintext is mapped into another element.
- ☐ **Transposition:** Elements in plaintext are rearranged.

Cryptography Classification

Cryptography is classified along three independent dimensions:

2. The number of **keys** used

- ☐ **Symmetric:** Sender and receiver use the same key.
- ☐ **Asymmetric:** Sender and receiver each use a different key.

Cryptography Classification

Cryptography is classified along three independent dimensions:

3. The **way** in which the plaintext is processed

- ☐ **Block cipher:** Processes input one block of elements at a time.
- ☐ **Stream cipher:** Processes the input elements continuously.

Cryptography: Definition and Key Concepts

- **Plaintext:** This is the original message or data that is fed into the algorithm as input.
- **Encryption algorithm:** The encryption algorithm performs various substitutions and transformations on the plaintext.
- **Secret key:** The secret key is also input to the algorithm. The exact substitutions and transformations performed by the algorithm depend on the key.
- **Ciphertext:** This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts.
- **Decryption algorithm:** This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the same secret key and produces the original plaintext.



History of Cryptography

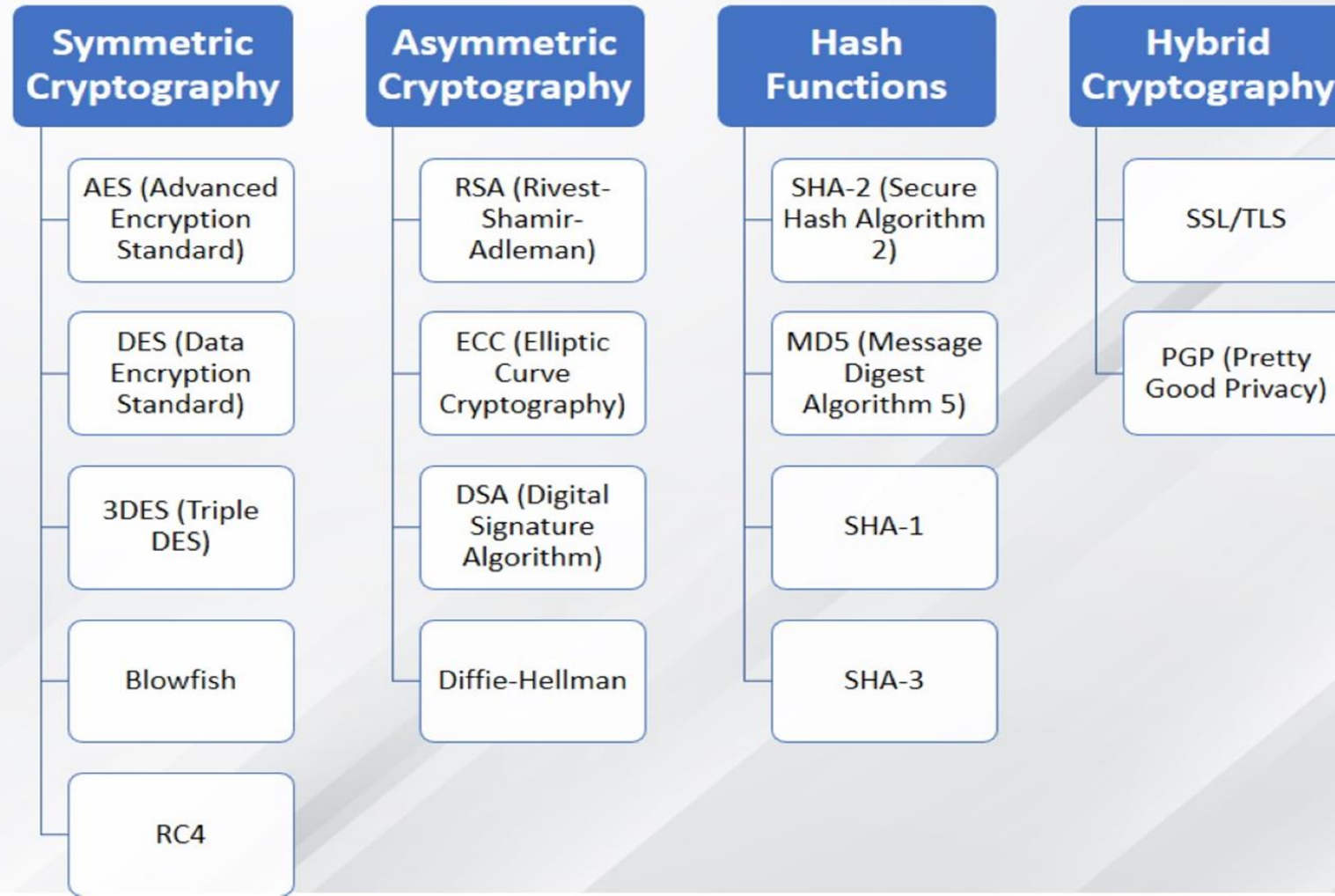
- **Ancient Egypt (circa 1900 BC)**
- **Mesopotamia (circa 1500 BC)**
- **India (400 BC – 200 AD)**
- **Ancient Greece**
- **Roman Empire**



A Scytale, an early device for encryption.



Classification of Cryptography Algorithms



Overview

- Symmetric encryption ensures **confidentiality** for transmitted or stored data.
- Commonly referred to as:
 - **Conventional encryption**
 - **Single-key encryption**
- Historical Use
 - Used by figures like Julius Caesar and during WWII by the German U-boat forces.
 - Still widely employed in diplomatic, military, and commercial communication.



Requirements for Secure Symmetric Encryption

Strong Encryption Algorithm

- Opponents knowing the algorithm and having access to ciphertexts should not be able to:
 - Decipher ciphertext.
 - Discover the key.
- Even with access to both ciphertext and the plaintext used to produce it, the key must remain secure.

Secure Key Management

- Both sender and receiver must securely obtain and protect the secret key.
- If the key is compromised, all communication using it becomes vulnerable.



Symmetric Encryption: An Overview

- **Key Features:**
 - **Single Key:** A shared secret key between sender and receiver.
 - **Efficiency:** Symmetric encryption algorithms are generally faster and more efficient than asymmetric methods.
 - **Common Uses:** Secure communications, file encryption, and protecting sensitive data.



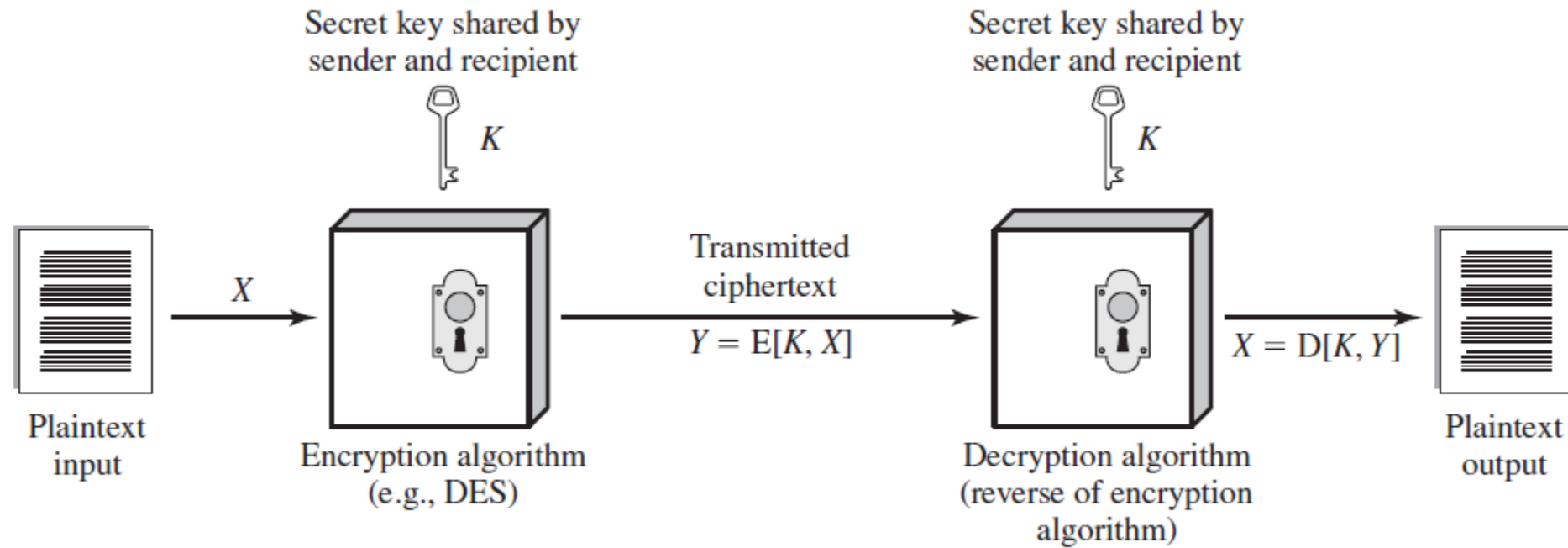


Figure 2.1 Simplified Model of Symmetric Encryption

Caesar Cipher

The Caesar cipher is a classical symmetric-key algorithm that shifts each letter in the plaintext by a fixed number of positions in the alphabet.

Encryption Steps

1.Plaintext: **HELLO**

2.Key (Shift): **3**

3.Encryption Function:

For each plaintext letter with numeric value p ($A = 0, B = 1, \dots Z = 25$), compute

$$C=(p+3) \bmod 26$$

Caesar Cipher

0	1	2	3	4	5	6	7	8	9	10	11	12
A	B	C	D	E	F	G	H	I	J	K	L	M

13	14	15	16	17	18	19	20	21	22	23	24	25
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Caesar Cipher

Plaintext Letter	Numeric Value (p)	$C = (p + 3) \bmod 26$	Ciphertext Letter
H	7	10	K
E	4	7	H
L	11	14	O
L	11	14	O
O	14	17	R

Resulting Ciphertext: **KHOOR**

Caesar Cipher

Decryption Process

- ❑ To recover the original message, subtract the same key (**3**):

$$p = (C - 3) \bmod 26$$

Attacking Symmetric Encryption

Cryptanalytic Attacks

- Rely on:
 - Nature of the algorithm
 - Some knowledge of the general characteristics of the plaintext
 - Some sample plaintext-ciphertext pairs
- Exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or the key being used
 - If successful all future and past messages encrypted with that key are compromised



Symmetric Block Encryption Algorithms

- Symmetric encryption algorithms primarily consist of block ciphers.
- Block ciphers process plaintext in fixed-size blocks, producing an equal-sized ciphertext block for each plaintext block.
- Longer plaintexts are processed as a series of fixed-size blocks.
- Key Algorithms:
 - Data Encryption Standard (DES)
 - Triple DES (3DES)
 - Advanced Encryption Standard (AES)



Table 2.1 Comparison of Three Popular Symmetric Encryption Algorithms

	DES	Triple DES	AES
Plaintext block size (bits)	64	64	128
Ciphertext block size (bits)	64	64	128
Key size (bits)	56	112 or 168	128, 192, or 256

DES = Data Encryption Standard

AES = Advanced Encryption Standard

Data Encryption Standard (DES)

- ❑ DES is a **symmetric-key** block cipher adopted as a U.S. Federal Information Processing Standard (FIPS 46) in 1977
- ❑ It encrypts **64-bit** plaintext blocks using a **56-bit** key over **16 rounds** of ***Feistel structure operations***

Data Encryption Standard (DES)

- Strength concerns:
 - Concerns about the algorithm itself
 - DES is the most studied encryption algorithm in existence
 - Concerns about the use of a 56-bit key
 - The speed of commercial off-the-shelf processors makes this key length woefully inadequate

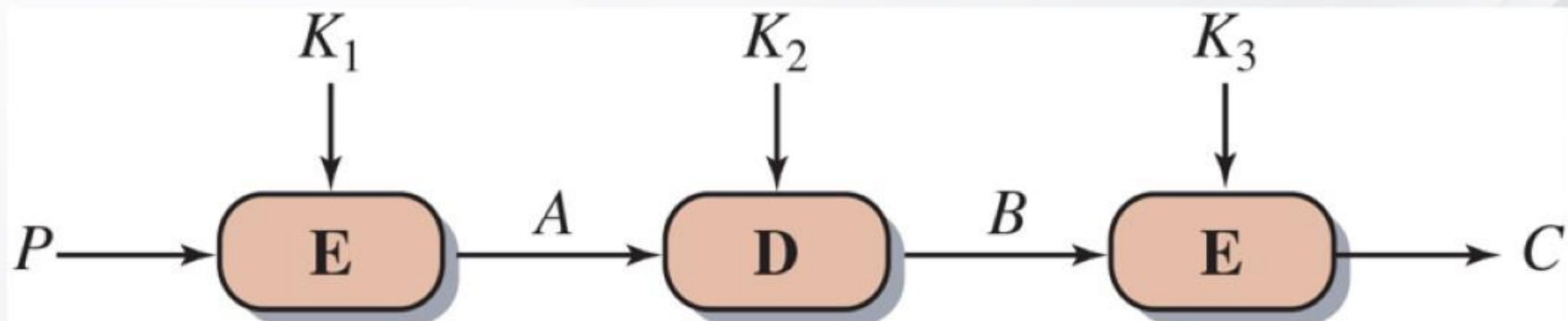


Triple DES (3DES)

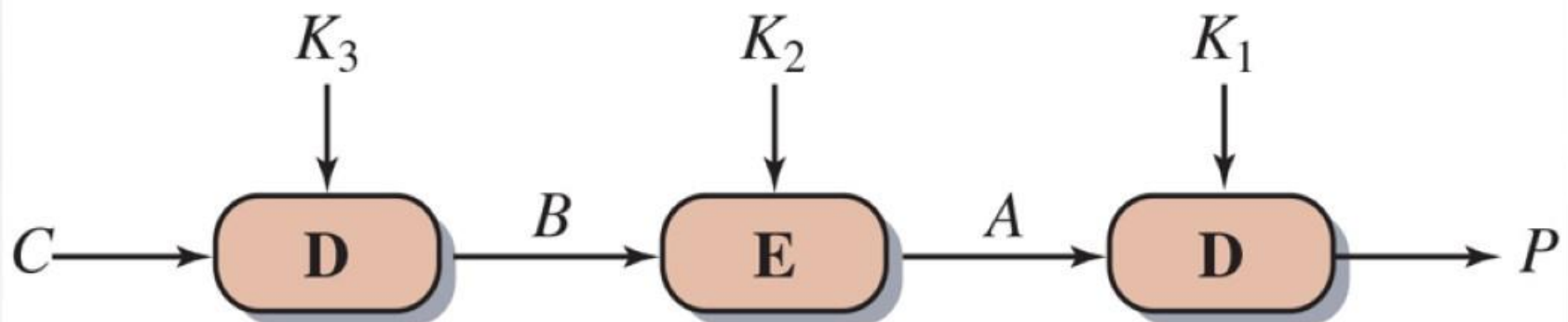
- Repeats basic DES algorithm three times using either two or three unique keys
- First standardized for use in financial applications in ANSI standard X9.17 in 1985
- Attractions:
 - 168-bit key length overcomes DES's vulnerability to brute-force attack
 - Underlying encryption algorithm is the same as in DES
- Drawbacks:
 - Algorithm is sluggish in software
 - Uses a 64-bit block size



Triple DES



(a) Encryption



(b) Decryption



Table 2.2 Average Time Required for Exhaustive Key Search

Key Size (bits)	Cipher	Number of Alternative Keys	Time Required at 10^9 decryptions/ μs	Time Required at 10^{13} decryptions/ μs
56	DES	$2^{56} \approx 7.2 \times 10^{16}$	$2^{55} \mu s = 1.125$ years	1 hour
128	AES	$2^{128} \approx 3.4 \times 10^{38}$	$2^{127} \mu s = 5.3 \times 10^{21}$ years	5.3×10^{17} years
168	Triple DES	$2^{168} \approx 3.7 \times 10^{50}$	$2^{167} \mu s = 5.8 \times 10^{33}$ years	5.8×10^{29} years
192	AES	$2^{192} \approx 6.3 \times 10^{57}$	$2^{191} \mu s = 9.8 \times 10^{40}$ years	9.8×10^{36} years
256	AES	$2^{256} \approx 1.2 \times 10^{77}$	$2^{255} \mu s = 1.8 \times 10^{60}$ years	1.8×10^{56} years

Simplified DES Encryption Process Flow

- **Input:** 64-bit Plaintext
- **Step 1: Initial Permutation (IP)**
- **Step 2: Split into Left (L0) and Right (R0) 32-bit Halves**
- **Step 3: 16 Rounds of Feistel Transformation ($i = 1$ to 16):**
 - $L_i = R_{i-1}$ (The Left half for the current round becomes the Right half from the previous round)
 - $R_i = L_{i-1} \text{ XOR } f(R_{i-1}, K_i)$ (The Right half for the current round is the XOR of the Left half from the previous round and the output of the complex function f applied to the previous Right half and the round's subkey K_i)
 - *(Internal f function details: **Expansion**, **XOR** with Subkey, **S-boxes**)*
- **Step 4: Combine L16 and R16 (without final swap)**
- **Step 5: Final Permutation (FP)**
- **Output:** 64-bit Ciphertext

XOR overview

P=1010

K=1101 $\oplus$



C= 0111

K=1101 $\oplus$

C= 0111

P=1010



2 input XOR gate

A	B	A $\oplus$ B
0	0	0
0	1	1
1	0	1
1	1	0



S Box

minimize

$$S0 = \begin{matrix} & 0 & 1 & 2 & 3 \\ \begin{matrix} 0 \\ 1 \\ 2 \\ 3 \end{matrix} & \begin{bmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{bmatrix} \end{matrix} \quad S1 = \begin{matrix} & 0 & 1 & 2 & 3 \\ \begin{matrix} 0 \\ 1 \\ 2 \\ 3 \end{matrix} & \begin{bmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{bmatrix} \end{matrix}$$

11011111

	1	2	3	4	5	6	7	8
IP	2	6	3	1	4	8	5	7
IP inverse	4	2	3	5	7	2	8	6

Simplified DES Encryption Process Flow

■ Step 1: Initial Permutation

- $M = 11011001 \rightarrow 10011110$
- $K1 = 10100010$ IP = 2 6 3 1 4 8 5 7 S-Box

■ Step 2: Splitting the Data

- $L0 = 1001$ $R0 = 1110$
- $L1 = R0$ $L1 = 1110$
- $R1 = (L0 \text{ XOR } F(R0, K1), R0)$ $F(R0, K1) = R0 \text{ XOR } K1$ $R0 = 4\text{bit}$ $k1 = 8\text{bit} !!!$ (Expand)
- $E = 4 \ 1 \ 2 \ 3 \ 2 \ 3 \ 4 \ 1$
- $E(R) = 01111101$
- $R0 \text{ XOR } K1 = 01111101 \text{ XOR } 10100010 = 11011111$
- $R1 = L0 \text{ XOR } 11011111 = 1001 \text{ XOR } 11011111$ (Sbox) $= 1001 \text{ XOR } 1111 = 0110$
- $R1 = 0110 \text{ XOR } 1110 = 1000$
- $R1 + L1 = 10001110$ apply IP inverse $C1 = 01011001$

Computationally Secure Encryption Schemes

- Encryption is computationally secure if:
 - Cost of breaking cipher exceeds value of information
 - Time required to break cipher exceeds the useful lifetime of the information
- Usually very difficult to estimate the amount of effort required to break
- Can estimate time/cost of a brute-force attack



Advanced Encryption Standard (AES)

- Needed a replacement for 3DES
 - 3DES was not reasonable for long-term use
- NIST called for proposals for a new AES in 1997
 - Would have a security strength equal to or better than 3 DES
 - Would significantly improve efficiency
 - Symmetric block cipher
 - 128 bit data and 128/192/256 bit keys
- Selected Rijndael in November 2001
 - Published as FIPS 197



Key Points of AES

- **Block Cipher:** AES encrypts data in **fixed-size** blocks of 128 bits (16 bytes) at a time
- **Key Sizes:** AES supports key lengths of 128, 192, or 256 bits. The longer the key, the stronger the encryption.
- **Rounds:** The encryption process involves multiple rounds of transformation:
 - ❑ 10 rounds for 128-bit keys
 - ❑ 12 rounds for 192-bit keys
 - ❑ 14 rounds for 256-bit keys

Key Points of AES

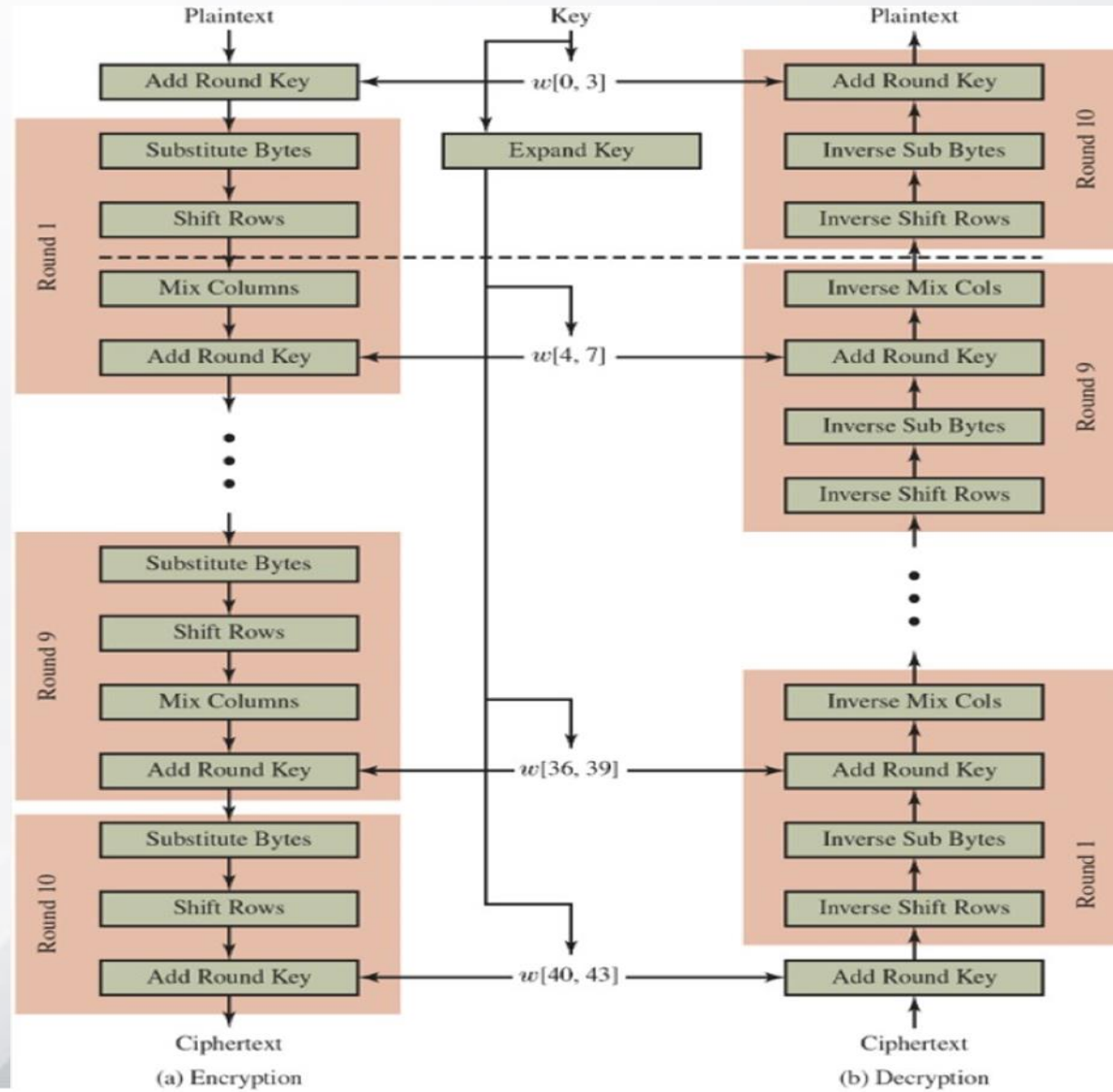
➤ Substitution–Permutation Network:

AES is based on a design called a **substitution–permutation** network, which combines confusion (making the relationship between the key and ciphertext complex) and diffusion (spreading the influence of each plaintext bit over many ciphertext bits)

How AES Works (Simplified)

➤ For each block of data:

1. **Key Expansion:** The original key is expanded into a set of round keys.
2. **Initial Round:** The data is mixed with the first round key (AddRoundKey).
3. **Main Rounds:** Each round consists of:
 - **SubBytes:** **Substitute** each byte using a fixed lookup table (S-box) for non-linearity.
 - **ShiftRows:** Shift rows of the data matrix to the left by different offsets (**permutation**).
 - **MixColumns:** Mix the bytes in each column (**diffusion**).
 - **AddRoundKey:** Combine with the next round key using XOR
4. **Final Round:** Same as a main round, but without the MixColumns step.



DES vs AES

Feature	DES (Data Encryption Standard)	AES (Advanced Encryption Standard)
Key Size	56 bits	128, 192, or 256 bits
Block Size	64 bits	128 bits
Security	Weak (easily broken by brute force)	Strong (no practical attacks known)
Speed	Slower, especially in software	Faster and more efficient in hardware/software
Structure	Feistel network (16 rounds)	Substitution-permutation network (10, 12, or 14 rounds)
Status	Obsolete (retired in 2005)	Current global standard

Why AES Replaced DES

- **Security:** AES's longer keys make it exponentially harder to crack. DES's 56-bit key is vulnerable to brute-force attacks—demonstrated in public challenges where DES was broken in less than a day
- **Performance:** AES is faster and more efficient, making it ideal for large-scale and high-speed applications
- **Flexibility:** AES can use different key lengths for varying security needs, while DES is fixed at 56 bits.

Summary

Cryptography

- History

- Modern Cryptology Origins

- Classification of Cryptography Algorithms

Symmetric Encryption

- Requirements for Secure Symmetric Encryption

- Symmetric Block Encryption Algorithms

- Data Encryption Standard (D E S)

- Advanced Encryption Standard (A E S)





Thank You

