زانکۆی سەلاحەدین - هەولێر
Salahaddin University-Erbil

Information Security II

Lecture 1

Modern Cryptography & Symmetric Cryptography- Part1

Instructor: Newroz N. Abdulrazaq

Science College- Department of Computer Science & I.T.

newroz.abudlrazaq@su.edu.krd

Text Book: Mark Stamp, Information Security: Principles And Practice (Third Edition), 2021. + Educational Websites.

Chapter 4: Symmetric Cryptography

Overview:

- Introduction.
- Types of Modern Cryptography.
- Symmetric Key Cryptography.
- AES Cryptography.
- Example on AES Key Expansion.

Modern Cryptography: Introduction

- Modern cryptography is the cornerstone of computer and communications security.
- Its foundation is based on various concepts of mathematics such as number theory, computational-complexity theory, and probability theory.
- It is classified into two types:
  1. Private key Cryptography (Symmetric).
  2. Public key cryptography (Asymmetric).

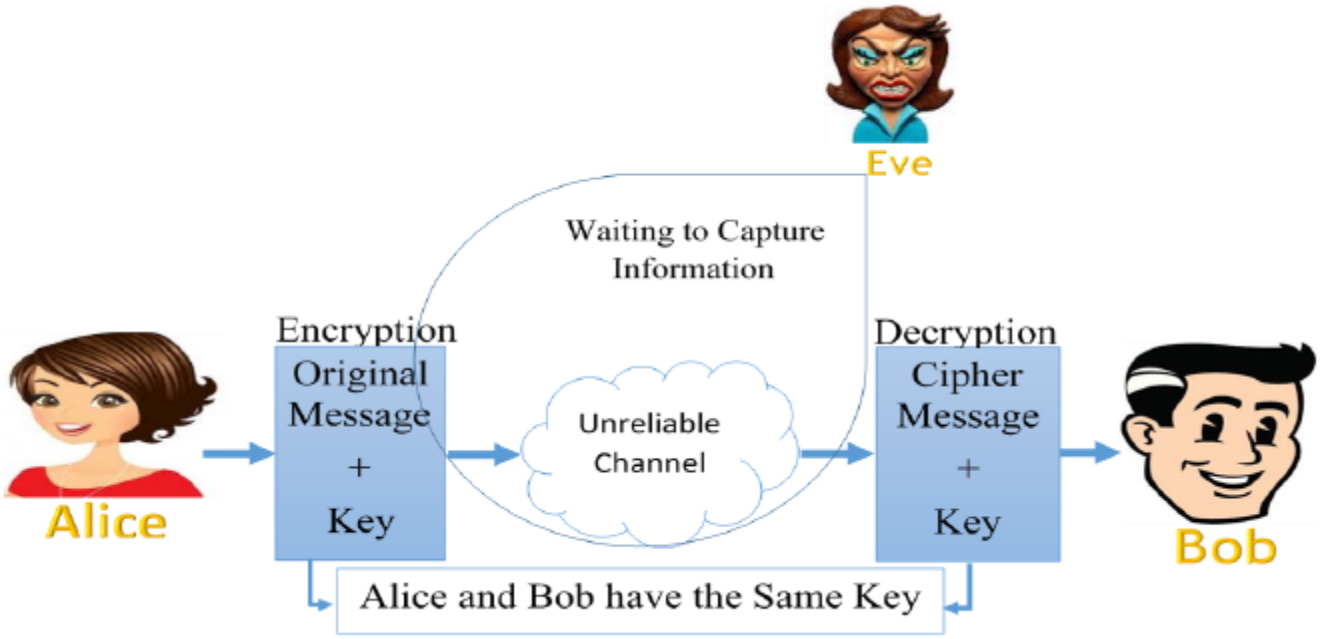
Modern Cryptography:

Private key Cryptography (Symmetric)

- Symmetric-key cryptography are algorithms that use the same cryptographic keys for both encryption of plaintext and decryption of cipher-text.
- Symmetric-key systems are simpler and faster.
- The main drawback is that the two parties must somehow exchange the key in a secure way.

Modern Cryptography:

Private key Cryptography (Symmetric)



Common Techniques of Symmetric key Cryptography:

1) DES (Data Encryption Standard)

- Developed by IBM cryptographers in the early 1970s and has been a U.S. government standard since 1976 for the protection of sensitive but unclassified electronic information.

- The algorithm is a block cipher, in which a 64-bit input block is transformed into a corresponding 64-bit output cipher text.

- It employs a 56-bit length key expressed as a 64-bit quantity in which the least relevant bit in each byte is used for parity checking.

Common Techniques of Symmetric key Cryptography:

2) IDEA (International Data Encryption Algorithm)

- the International Data Encryption Algorithm (IDEA) has been classified by some of the contemporary cryptographers as the most secure and reliable block-algorithm.
- Like DES, IDEA encrypts data in 64-bit input blocks; for each it outputs corresponding 64-bit cipher block.
- Unlike DES, IDEA employs 128-bit secret key

Common Techniques of Symmetric key Cryptography:

3) AES (Advanced Encryption Standard)

- The Advanced Encryption Standard (AES), also known by its original name Rijndael. It is chosen by the U.S. government to protect classified information.
- It is implemented in software and hardware throughout the world to encrypt sensitive data.
- Rijndael is an iterated block cipher with a variable block length and a variable key length both of which can independently be 128, 192, or 256 bits.

AES: Rounds Operations

1 Sub Byte

In the Sub Bytes step, each byte aij in the state matrix is replaced with a SubByte $S(aij)$ using an 8-bit substitution box

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Example: B7 ⇒ A9 22 ⇒ 93

AES: Rounds Operations

2 Shift Row

The ShiftRows step operates on the rows of the state; it cyclically shifts the bytes in each row by a certain offset. For AES, the first row is left unchanged. Each byte of the second row is shifted one to the left. Similarly, the third and fourth rows are shifted by offsets of two and three respectively.

Example: B7 A9 22 93 —1 Shift Row→ A9 22 93 B7

AES: Rounds Operations

3 Mix Column

In the MixColumns step, the four bytes of each column of the state are combined using an invertible linear transformation. The MixColumns function takes four bytes as input and outputs four bytes, where each input byte affects all four output bytes.

Example:

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} 63 & EB & 9F & A0 \\ 2F & 93 & 92 & C0 \\ AF & C7 & AB & 30 \\ A2 & 20 & CB & 2B \end{pmatrix} = \begin{pmatrix} BA & 84 & E8 & 1B \\ 75 & A4 & 8D & 40 \\ F4 & 8D & 06 & 7D \\ 7A & 32 & 0E & 5D \end{pmatrix}$$

Matrix used for Mixing Column

Encryption Stage

Result

AES: Rounds Operations

4 Round key Addition

- ✓ In the AddRoundKey step, the subkey is combined with the state.
- ✓ For each round, a subkey is derived from the main key using Rijndael's key schedule; each subkey is the same size as the state.
- ✓ The subkey is added by combining each byte of the state with the corresponding byte of the subkey using bitwise XOR.

AES_128: Key Expansion

Use four byte words called w_i. Subkey = 4 words. For AES-128:

1. First subkey (w3,w2,w1,w0) = cipher key.
2. Other words are calculated as follows: $w_i = w_{i-1} \oplus w_{i-4}$ for all values of i that are not multiples of 4.
3. For the words with indices that are a multiple of 4 (w4k):
   - RotWord: Bytes of w : Bytes of w_{4k-1} are rotated left shift.
   - SubWord: SubBytes f_n is applied to all four bytes.
   - $w4k = rs_k \oplus w_{4k-4} \oplus rcon_k$. Where rs_k is the result of subword

Example*: Generate Round1 key for AES-128 bit where round0 key = That's my Kung Fu.

Example

1

T	h	a	t	s		m	y		K	u	n	g		F	u
54	68	61	74	73	20	6d	79	20	4b	75	6e	67	20	46	75

W_0 W_1 W_2 W_3

2 Calculating $g(w_3)$?

W_3 = 67 20 46 75

RotWord: 20 46 75 67

SubWord: B7 5A 9D 85

2 Calculating $g(w_3)$?

$g(w_3) = rs_1 \oplus Rcon_1$

$g(w_3) =$ B7 5A 9D 85 $\oplus$ 01 00 00 00

	8	4	2	1	8	4	2	1
	1	0	1	1	0	1	1	1
$\oplus$	0	0	0	0	0	0	0	1
	1	0	1	1	0	1	1	0
	B				**6**			

Rcon Constants (Base 16)			
Round	Constant(Rcon)	Round	Constant(Rcon)
1	01 00 00 00	6	20 00 00 00
2	02 00 00 00	7	40 00 00 00
3	04 00 00 00	8	80 00 00 00
4	08 00 00 00	9	1B 00 00 00
5	10 00 00 00	10	36 00 00 00

$g(w_3) =$ B6 5A 9D 85

3 Calculating w_4, w_5, w_6, w_7

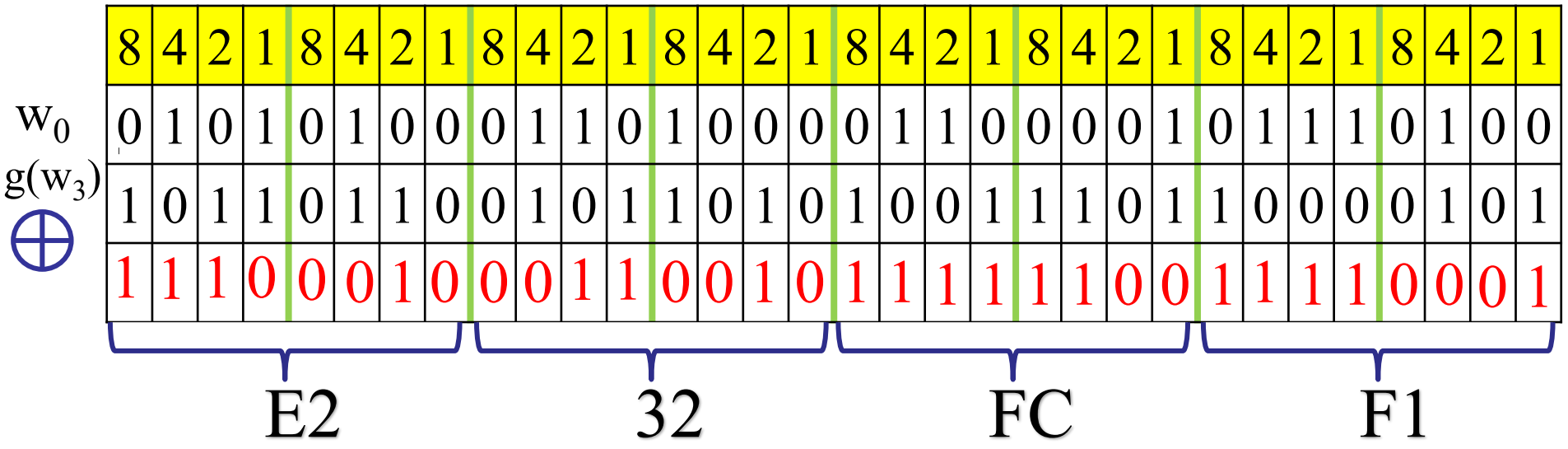
$w_4 = w_0 \oplus g(w_3) =$ 54 68 61 74 $\oplus$ B6 5A 9D 85 = E2 32 FC F1

$w_5 = w_1 \oplus w_4 =$ 73 20 6D 79 $\oplus$ E2 32 FC F1 = 91 12 91 88

$w_6 = w_2 \oplus w_5 =$ 20 4B 75 6E $\oplus$ 91 12 91 88 = B1 59 E4 E6

$w_7 = w_3 \oplus w_6 =$ 43 49 54 59 $\oplus$ B1 79 A2 93 = D6 79 A2 93

w_0 =54 68 61 74 $g(w_3)$ = B6 5A 9D 85



∴ $w_4 = w_0 \oplus g(w_3)$ =54 68 61 74 ⊕ B6 5A 9D 85 = E2 32 FC F1

AES_128: Encryption Process

For 10 round encryption process, we should do the following steps:

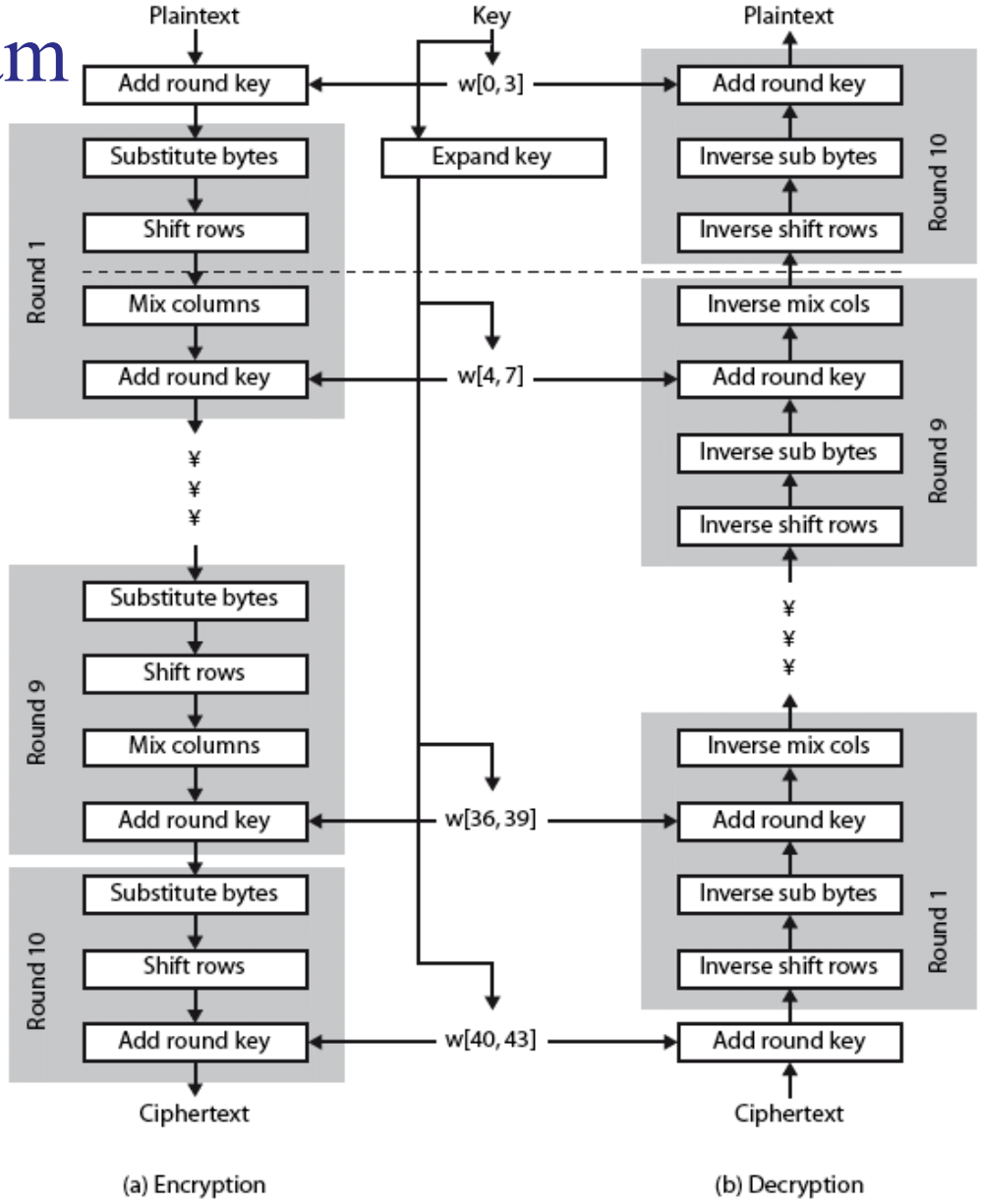
1. Round0: Addition Round key using the zeroth round.
2. Rounds 1 to 9: processed to calculate BS, SR, MC, ARK.
3. Round10: processed without MC.

AES_128: Decryption Process

For 10 round encryption process, we should do the following steps:

1. Addition Round key using the last round.
2. Rounds Last-1 to 1 are processed to calculate:
   IBS, ISR, IMC, IARK.
3. Zeroth round is processed without IMC.

AES Block Diagram



Home Work

Q1: Generate round 2 to round 10 keys for AES- 128 Cryptosystem from example*?

Q2: What is the difference between Classical and Modern cryptography?

Key Point

- Symmetric key Cryptography.
- AES cryptosystem.
  - Key Expansion.
  - Encryption Process.
  - Decryption Process.
- Example on Key Expansion.