Symmetric Key Cryptography

IMPORTANT NOTES: Study lecture materials at least 1 hour and prepare Q1–3 prior to the tutorial session. Those questions will be discussed in the tutorial.

1. What is the difference between an unconditionally secure cipher and a computationally secure cipher?

2. What is a monoalphabetic cipher and what is a key in this cipher?

3. Vigenère cipher is a cipher similar to the one-time pad, uses the values of the letters of a secret key to shift the letters of a plaintext. However, unlike the one-time pad, it repeatedly uses the same short key to encrypt arbitrarily long plaintexts. This is done by repeating the secret key word to create a key which is as long as the message and then adding the values of the letters of the key to the letters of the plaintext. The result will be calculated mod 26 to make sure the ciphertext will also be comprised of letters. Using the Vigenère cipher, encrypt the word *explanation* using the key *leg*.

   Note: You can use the foloowing values assigned for each letter:

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

4. **Block cipher:** The SubBytes in AES round operation is performed as follows. Write the input byte by byte in hexadecimal. For each byte represented in hexadecimal, use the first hexadecimal digit to select the row and uses the second hexadecimal digit to select the column, then replace the input by the corresponding byte from the SBox specified by Table 1. For example, if the input byte is `53` in hexadecimal, then the SubBytes result is `ED` in hexadecimal. Given the input `EA 36 56 78` in hexadecimal, write the result of SubBytes in hexadecimal.

	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

Table 1: S-Box used in AES, in hexadecimal notation

5. **CBC Block Cipher Mode:** For the CBC block cipher mode shown in Figure 6.4:

   (a) Identify which decrypted plaintext blocks P_x will be corrupted if there is an error in the received ciphertext block C_4.

   (b) Assuming that the ciphertext contains N blocks, and there was a bit-flip error in the sender side plaintext block P_3, identify through how many ciphertext blocks this error is propagated.

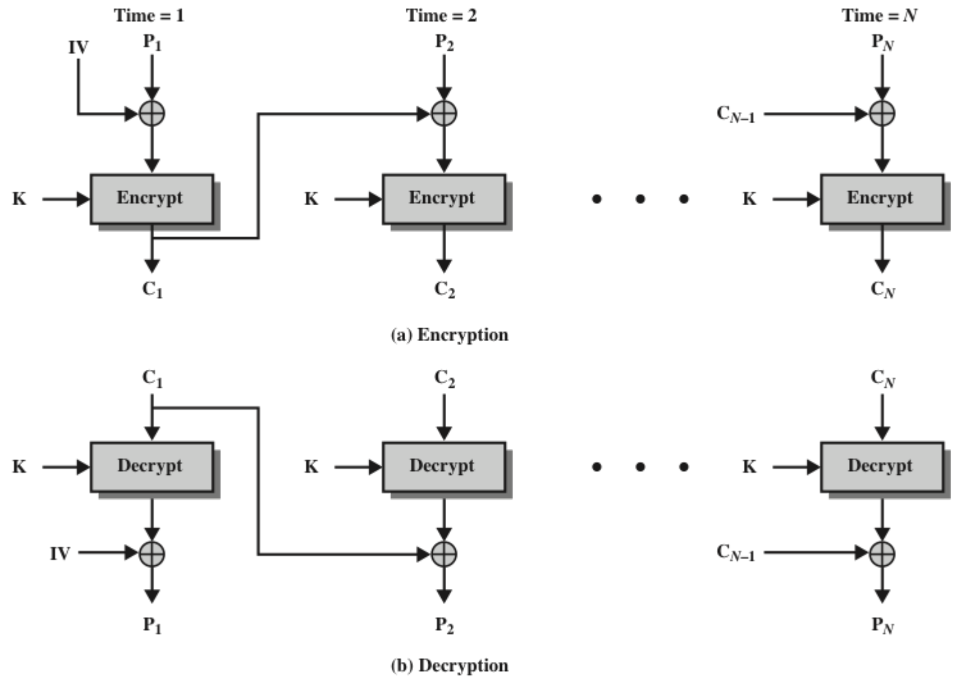

Figure 6.4 Cipher Block Chaining (CBC) Mode