Kenneth Jahnke ≡

Assignment 6 – 01 Mar 2025

CSCI 389 (Online) - Spring 2025

6.4.a.

Original plaintext

00	04	08	0C
01	05	09	0D
02	06	0A	0E
03	07	0B	0F

5/5

Original key

01	01	01	01
01	01	01	01
01	01	01	01
01	01	01	01

6.4.b.

Round 0 Key

w0 = 01 01 01 01

w1 = 01 01 01 01

w2 = 01 01 01 01

w3 = 01 01 01 01

x1 = RotWord(w3) = 01 01 01 01

y1 = SubWord(x1) = 7C 7C 7C 7C

Rcon(1) = 01 00 00 00

z1 = y1 $\oplus$ Rcon(1) = 7D 7C 7C 7C

w4 = w0 $\oplus$ z1 = 7C 7D 7D 7D

w5 = w4 $\oplus$ w1 = 7D 7C 7C 7C

w6 = w5 $\oplus$ w2 = 7C 7D 7D 7D

w7 = w6 $\oplus$ w3 = 7D 7C 7C 7C

Round 1 Key

7C	7D	7C	7D
7D	7C	7D	7C
7D	7C	7D	7C
7D	7C	7D	7C

AddRoundKey --> [Original plaintext] ⊕ [Original key]

Start of Round 1

7C	79	74	71
7C	79	74	71
7F	7A	77	72
7E	7B	76	73

4/5

6.4.c.

After SubBytes

10	B6	92	A3
10	B6	92	A3
D2	DA	F5	40
F3	21	38	8F

4/5

6.4.d.

After ShiftRows

10	B6	92	A3
B6	92	A3	10
F5	40	D2	DA
8F	F3	21	38

4/5

6.4.e.

After MixColumns

9B	69	32	8F
EC	BA	83	CE
DD	AA	ED	54
76	EE	9E	44

4/5

7.1.a.

The three-loop CBC would be best for security because encryption and decryption are distinct steps because they are separated into different units. Long story short – better key mixing.

9/10

7.1.b.

The one-loop CBC would be best for performance because a single unit could handle all processes, i.e., there is reduced latency.

7.4.a.

P1 and P2 will be affected because a ciphertext block will garble the corresponding plaintext block and the subsequent block. In this case C1 will garble P1 and P2, but the ones after those will be fine.

10/10

7.4.b.

C1 and C2 (subsequence) will be changed as a result. For decryption, there will be errors in P1 and P2 (correspondence).

7.5.

Because CBC mode is dependent on the prior ciphertext block via an XOR operation. Encryption must be done sequentially, therefore cannot be done in parallel.

10/10

Decryption can be done in parallel because the previous ciphertext block accompanies the current ciphertext block. Since both inputs from the encryption are available, everything that's needed for decrypting is also available.

7.7.

The motivation for adding a padding block is consistency across iterations of the encryption process and better security. Padding to a consistent size decreases the likelihood of errors and standardizes encryption standards. In adding padding, the exact length of messages is obfuscated, which makes it more difficult for attackers to make assumptions about what's being sent simply by looking at string size.

7.8.

The error propagates over two indexes. A single bit error in a ciphertext byte will have a direct negation effect on the plaintext bit in the corresponding position due to “XOR-ing”. The corrupted ciphertext will be fed back for the next round of encryption and since it’s corrupted the keystream is corrupted. Again, because of “XOR-ing” with the last input, the next plaintext will also be garbled. After this, things return to “normal” and no further errors occur from this particular bit error.