Exercises

1. A Linear Feedback Shift Register is defined as follows:

What will be the state and output bit stream of the register after 10 clock cycles?

Clk	b7	b6	b 5	b4	b 3	b2	b1	b0	Output
0	1	1	1	0	0	0	1	0	0
1	1	1	1	1	0	0	0	1	0
2	0	1	1	1	1	0	0	0	10
3	0	0	1	1	1	1	0	0	010
4	1	0	0	1	1	1	1	0	0010
5	1	1	0	0	1	1	1	1	00010
6	1	1	1	0	0	1	1	1	100010
7	1	1	1	1	0	0	1	1	1100010
8	0	1	1	1	1	0	0	1	11100010
9	0	0	1	1	1	1	0	1	11100010
10	1	0	0	1	1	1	1	0	111100010

2. Explain the key issue that limits the practical application of the one-time-pad(OTP) cipher.

Encryption with the OTP requires a key that is the same length as the plain text. This means the larger the plain text is, the longer would be the key required. As the key is based on the specific plaintext, it can only be used once. As a result, it is impractical to use.

3. For an AES-128 cipher, if K_4 = D6581283 45106552 C02B2F32 563486E1₁₆, and the first word of K_5 is 5621B371₁₆, what would be the fourth word for K_5 ?

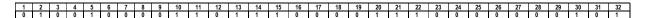
2nd Word of K_5 is given by XOR of 1st word of K_5 with 2nd word of K_4 $5621B371_{16}~\oplus~45106552_{16}$ = $1331D623_{16}$

3rd Word of K_5 is given by XOR of 2nd word of K_5 with 3rd word of K_4 1331d623₁₆ \oplus C02B2F32₁₆ = D31AF911₁₆

4th Word of K_5 is given by XOR of 3rd word of K_5 with 4th word of K_4 D31AF911 $_{16}$ $\,\oplus$ 563486E1 $_{16}$ = 852E7FF0 $_{16}$

4. In DES, if the input to the expansion stage is $486E1C05_{16}$, and the round key, $k_i = D2F865B4C290_{16}$ what will be the input to the S-Box substitution stage.

Expansion Stage



XOR Stage

- 5. In a DES S-Box substitution, if the input is 4597F2D13C3A₁₆, what will be the output?
 - → 010001, 011001, 011111,110010,110100, 010011,110000, 111010
 - → 18, 1C, 1F, 2A, 2C, 1A, 28, 2D,
 - → 10,09, 08,09,03,12,15,10
 - → 1010,1001, 1000, 1001,0011,1100,1111,1010
 - → A9893CFA
- 6. In an AES-128 cipher, if the input to the SubBytes stage is E749039456217663674597F2D13C3A43₁₆, what is the output of the ShiftRows stage?

Block-to-State Conversion

E7	56	67	D1
49	21	45	3C
03	76	97	ЗА
94	63	F2	43

SubBytes Stage Output

94	В1	85	3E
3в	FD	6E	EB
7в	38	88	80
22	FB	89	1A

Shiftrows Stage Output

94	В1	85	3E
FD	6E	EB	3в
88	80	7в	38
1A	22	FB	89

- 7. Maryam is using RSA for sending messages to Fatima. Assuming p=5 and q=7, m=3:
 - (a) Calculate n and $\Phi(n)$.

$$n = 5*7 = 35$$

 $\Phi(n) = 4*6 = 24$

- (b) Choose the exponent (e) that is necessary to satisfy the requirements of key generation. Choose e such that 1<e<24 and gcd(e,24)=1
- (c) Calculate Maryam's private key, d, using the Extended Euclidean Algorithm

$$ex + \Phi(n)y = 1$$

 $5x + 24y = 1$

Gcd(5,24)=1

$$24 = 4(5) + 4$$
 $4 = 24 - 4(5)$ (eq. 1)

 $5 = 1(4) + 1$
 $1 = 5 - 1(4)$ (eq. 2)

Substitute (eq. 1) into (eq. 2)

 $1 = 5 - [24-4(5)] = 5 + 4(5) - 1(24) = 5(5) - 1(24)$
 $d = x = 5$

Private Key, $K_{prv} = 5,35$.

- (d) Calculate the Maryam's public key
 Public key, K_{pub} = e, n = 5,35
- (e) Show the calculations that Fatima will need to make to decrypt the ciphertext

Encryption
$$c = m^e \mod n = 3^5 \mod 35 = 33$$

Decryption $M = c^e \mod n = 33^5 \mod 35 = 3$