1. Explain the main features of DES algorithm .
2. You have 20 block of 64-bit how many times will implement DES to encrypt the 20 block?
3. Explain the main features of Public key cryptography .
4. How many key(s) does Public key cryptography has ? Detect the type of this key(s).
5. How to find **n** in polling-hellman algorithm ?
6. How to find **n** in RSA algorithm ?
7. What is the encryption process between plaintext and key in stream cipher?
8. What are the two parameters that is a key generation LFSR has ?
9. Why the Gaffe generator is nonlinear key generation ?
10. In DES the encryption and decryption completely the same , but what are the minor differences?
11. What is table that is used with Feastil cipher to divide the plaintext to two equal halves (left and right) before ciphering/deciphering?
12. List the DES algorithm sequence.
13. What is the length of the 16-subkeys in DES ?
14. Explain the main features of Exponential cipher.
15. Write the relation of public key (e) and private key (d) in RSA .
16. Detect the basic condition to select e of RSA encryption algorithm.
17. What is the main condition of Stream cipher first must do of the plaintext ?
18. What are the main two types of stream ciphers ?
19. Detect the main feature of Synchronous stream cipher.
20. **What are the differences of self- synchronous** key generation and **synchronous** key generation ?.

Note2: according table of character coding below encrypt and decrypt.

a =0	***b=1***	***c =2***	***d=3***	***e=4***	***f=5***	***g=6***	***h=7***	***i=8***	***j=9***
k=10	***l=11***	***m=12***	***n=13***	***o=14***	***p=15***	***q=16***	***r=17***	***s=18***	***t=19***
u=20	***v=21***	***w=22***	***x=23***	***y=24***	***z=25***				

1. Answer the following :
   - **a.** In DES a 16th key generation is a process of generate 16 sub-keys of (48-bits); explain with figure how to generate the16th keys.
   - **b.** Explain the rules and steps of the two phases of RSA (key generation and encryption/decryption). Support your answer with example.

c. Explain with figures the encryption and decryption of DES algorithm and then list the two differences between the encryption and decryption.

d. In DES algorithm, if key (64 bit) = 00010011 00110100 01010111 01111001 10011011 10111100 11011111 11110001. Find key (56) using PC-1 table;

PC-1 table

57,	49,	41,	33,	25,	17,	9,	1,	58,	50,	42,	34,	26,	18,
10,	2,	59,	51,	43,	35,	27,	19,	11,	3,	60,	52,	44,	36,
63,	55,	47,	39,	31,	23,	15,	7,	62,	54,	46,	38,	30,	22,
14,	6,	61,	53,	45,	37,	29,	21,	13,	5,	28,	20,	12,	4.

2. Encrypt and decrypt the plaintext (5); using Polling-Hellman, where p = 11, e= 3, d= 7.
3. Encrypt and decrypt the plaintext (***mr***); using Pohlig-Hellman cipher, where p = 7, choose *e*= 11 and *d* you can compute it by d = (1 + n Φ (p)) / e.
4. In DES draw the diagram of key generation process to generate 16 sub-keys.
5. List all steps of RSA -key generation with example.
6. Explain encryption/decryption of RSA cipher system with example.
7. Draw all steps of the encryption and decryption of DES algorithm.
8. List the differences between the encryption and decryption in DES algorithm..
9. Find key (56) using follow table If you have DES algorithm with key = 00000001 00000000 01010100 01111001 10000011 10111100 11011111 11110001.

PC-1 table

57,	49,	41,	33,	25,	17,	9,	1,	58,	50,	42,	34,	26,	18,
10,	2,	59,	51,	43,	35,	27,	19,	11,	3,	60,	52,	44,	36,
63,	55,	47,	39,	31,	23,	15,	7,	62,	54,	46,	38,	30,	22,
14,	6,	61,	53,	45,	37,	29,	21,	13,	5,	28,	20,	12,	4.

10. Given p = 13, e=7, d= 3. Use the Polling-Hellman to encrypt the plaintext (03); using, where.
11. Encrypt and decrypt the plaintext (*h*); using RSA cipher, where p = 11 and q= 3, find n, Φ (n), *e, and d.*
12. Just create a linear feedback shift register with 5 cells in which; $F(x) = x^5 + x^2 + 1$. Show LFSR and the value of output for 7 transitions (shifts) if the seed is (10101).

13. Create a linear feedback shift register with 6 cells in which; $F(x) = x^6 + x^3 + 1$. Show LFSR and the value of output for 7 transitions (shifts) if the seed is (101100). Then encrypt and decrypt the text (1000100010010010).
14. Explain in details with figure how to convert the 64-bit key to generate the16^{th} keys.
15. Explain with figures the encryption and decryption of DES algorithm .
16. If Plaintext = (1101); then encrypt and decrypt it using Stream Cipher. Where the key is generated using the *LFSR with 6 cells; (b6= b5 xor b3 xor b1 xor b0)*, Show LFSR and the value of output for 4 transitions (shifts) if the Initial Key, seed (101011).
17. Given n = 35; e = 3; C = 10.
    1) Compute d .
    2) By using RSA , find the plaintext
    3) Find p and q
    4) Validate (e*d mod Φ (n) =1)
    5) How RSA advanced Polling-Hellman by cancelling the condition GCD (m, n) =1.
18. Explain the Geffe generator. Write the LFSRs function.
19. What are the advantages and disadvantages of using a stream cipher.
20. Explain the stream cipher vs. block cipher.