HOMEWORK 2

Problem 1 - Simplified DES

K = 1001100010 (10 bits)
P = 10011100 (8 bits)

Round 1:

P10 (permutation):

input:	1	2	3	4	5	6	7	8	9	10
output:	3	5	2	7	4	10	1	9	8	6

K = 1001100010
P10 = 0100101100
LS1 = 1001011000

P8 (select & permutate)

input:	1	2	3	4	5	6	7	8	9	10
output:	6	3	7	4	8	5	10	9		

LS1 = 1001011000
P8 = 10110000

So, $K_1 = 10110000$

Round 2:

LS1 = 1001011000
LS2 = 0101000011
P8 = 00010011

So, $K_2 = 00010011$

Encryption:

IP (initial permutation):

input:	1	2	3	4	5	6	7	8
output:	2	6	3	1	4	8	5	7

P = 10011100
IP = 01011010

EP (expand and permutate)

input:	1	2	3	4				
output:	4	1	2	3	2	3	4	1

IP = 0101 10 10
EP = 01011010
$\oplus K_1$ = 10110000
11101010

$$S0 = \begin{bmatrix} 01 & 00 & 11 & 10 \\ 11 & 10 & 01 & 00 \\ 00 & 10 & 01 & 11 \\ 11 & 01 & 11 & 10 \end{bmatrix} \qquad S1 = \begin{bmatrix} 00 & 01 & 10 & 11 \\ 10 & 00 & 01 & 11 \\ 11 & 00 & 01 & 00 \\ 10 & 01 & 00 & 11 \end{bmatrix}$$

EP ⊕ K = 1 1 1 0 0 1 0 1 (1 2 3 4 | 1 2 3 4)

r: 10 → S0 → 11 ; r: 01 → S1 → 01

c: 11 ↓ ; c: 10 ↓

P4 (permutate)
input: 1 2 3 4
output: 2 4 3 1

SOS1 = 1 1 0 1 (1 2 | 3 4)
P4 = 1 1 0 1
⊕ IP (left) = 0 1 0 1
1 0 0 0 | 1 0 1 0 (IP (right))

SW = 1 0 1 0 | 1 0 0 0 (1 2 | 3 4)
EP = 0 1 0 0 0 0 0 1
⊕ K2 = 0 0 0 1 0 0 1 1
0 1 0 1 0 0 1 0

r: 01 → S0 → 01 ; r: 00 → S1 → 01

c: 10 ↓ ; c: 01 ↓

P4 = 1 1 0 0
⊕ SW (left) = 1 0 1 0
0 1 1 0 | 1 0 0 0 (SW (right))

IP⁻¹:
input: 1 2 3 4 5 6 7 8
output: 4 1 3 5 7 2 8 6

P4 ⊕ SW = 0 1 1 0 | 1 0 0 0 (1 2 3 4 | 5 6 7 8)
IP = 0 0 1 1 0 1 0 0

C = 00110100

Problem 2 - DES

M = 44 69 72 74 62 61 67 73
K = 43 57 53 31 39 39 28 21

C = 53 97 E0 17 62 32 86 24

Problem 3 - RSA

$p = 11,\ q = 3,\ e = 3,\ M = 8$

Generate the key:

$n = pq = 11 \times 3 = 33$

$\varphi(n) = (p-1)(q-1) = 10 \times 2 = 20$

Let $d = 7$ because $de = 7 \times 3 = 21 = (1 \times 20) + 1$ and $d = 7 < 20$

So, public key $PU = \{e, n\} = \{3, 33\}$

private key $PR = \{d, n\} = \{7, 33\}$

Encryption:

$C = M^e \bmod n$

$= 8^3 \bmod 33$

$8 \bmod 33 = 8$

$8^2 \bmod 33 = 8 \cdot 8 \bmod 33 = 64 \bmod 33 = 31$

$8^3 \bmod 33 = 31 \cdot 8 \bmod 33 = 248 \bmod 33 = 17$

So $C = 17$

Decryption:

$M = C^d \bmod n$

$= 17^7 \bmod 33$

$17 \bmod 33 = 17$

$17^2 \bmod 33 = 17 \cdot 17 \bmod 33 = 289 \bmod 33 = 25$

$17^4 \bmod 33 = 25 \cdot 25 \bmod 33 = 625 \bmod 33 = 31$

$17^7 \bmod 33 = 17 \cdot 25 \cdot 31 \bmod 33 = 29 \cdot 31 \bmod 33 = 8$

So $M = 8$

Problem 4 - Diffie-Hellman

common prime $q = 11$

primitive root $\alpha = 2$

a. Public key $Y_a = 9$, find A's private key X_a?

n	0	1	2	3	4	5	6	7	8	9	10
$2^n \bmod 11$	1	2	4	8	5	10	9	7	3	6	1

$Y_a = \alpha^{X_a} \bmod q$

$9 = 2^{X_a} \bmod 11$

From the table above,

we can see that $X_a = 6$

b. $Y_b = 3$, find shared secret key K?

$K = (Y_b)^{X_a} \bmod q$

$K = 3^6 \bmod 11$

$3 \bmod 11 = 3$

$3^2 \bmod 11 = 9$

$3^4 \bmod 11 = 9 \cdot 9 \bmod 11 = 4$

$3^6 \bmod 11 = 9 \cdot 4 \bmod 11 = 3$

So, $K = 3$