3. Elgamal Scheme

$q = 71$

primitive root : $7\ (e_1)$

a) plaintext $= 30$

$r = 2$

$C_1 = e_1^{r} \bmod q = (7)^2 \bmod 71$

$= \boxed{49}$

$C_2 = (\text{plaintext} * (e_2)^{r}) \bmod q$

$= (30 * (3)^2) \bmod 71$

$= 270 \bmod 71$

$= \boxed{57}$

$C = (49, 57)$

b) r is diff

① $e_1^{r} \% q = C_1$

② $(30 * e_2^{r}) \% q = C_2$

$7^{r} \bmod 71 = 59$

$\Rightarrow \boxed{r = 3}$

by trial & error

$\therefore C_2 = (30 * (3)^3) \% 71$

$= 810 \% 71 = 29$

$\boxed{C_2 = 29}$

4. $C = 10$
iphertext

$e = 5$

$n = 35$

$M = ?$
plaintext

n is a product of two primes p, q
for $n = 35$,

$p = 7$ and $q = 5$

$\phi(n) = (p-1)(q-1) = 6(4) = 24$

$e^* d = 1 \% \phi(n)$

$e = 5$

$5^* d = 1 \% 24$

$\boxed{\therefore d = 5}$ multiplicative inverse of e
pvt key

Plaintext = $(\text{Ciphertext})^d \bmod n$

$= (10)^5 \bmod 35$

$= 100000 \bmod 35$

$\boxed{\text{plaintext} = 5}$

5. Secret number : x public number $- a$

i) If x^a is sent,
let that value be C.

$$C = x^a$$

The hacker can simply get the a^{th} root of this number C to uniquely determine x.

i.e

$$x = \sqrt[a]{C} = C^{1/a}$$

Thus, this encryption would fail as a is known to everybody, and x is nolonger secret

ii) Diffie-Hellman Algo can be used.

Public : (p, g) where p - large prime no.
g - primitive root

say,

Pvt key of Alice : m

Pvt key of Bob : n

Alice sends : $(g^m \bmod p) \rightarrow X_1$

and

Bob sends : $(g^n \bmod p) \rightarrow X_2$

, Then key would be $\boxed{g^{mn} \bmod p}$, which both of them now know without directly transferring key.

Alice receives X_2.
He does $(X_2)^m$ to get g^{mn} % p which is the key.

Similarly Bob receives $X_1 = g^m \bmod p$.
He uses his pvt key n to get $(X_1)^n = g^{mn} \bmod p$ which is the key agreed upon.

iii) No Eve cannot break the system.
Although it can intercept the channel and modify the ciphertext.

iv) No, Eve cannot find the secret key as m and n are private.

1. IV (initial vector)
$\downarrow$
Encrypt with key (permutation)
$\downarrow$
XOR with plaintext
$\downarrow$
Ciphertext$_1$ $\rightarrow$ Next Block

IV = 1010

1010	0010	1111
↓	↓	↓
permute with key	permute	permute
↓	↓	↓
0110	0100	1111
↓ $\oplus$	$\oplus$	$\oplus$
0100	1011	1100
C_1 : 0010	C_2 : 1111	C_3 : 0011

Ciphertext : 001011110011

2. S boxes :

S boxes are substitution boxes. They can be keyless or keyed. In keyed S box, the mapping depends on the key as well.
Keyless ones are static, keyed ones are dynamic.
Static S Box is used in DES.
In some other algos like Blowfish algorithm, the S Box is dynamic.

a) Static | Dynamic

Advantages: (Static)

- no extra hardware is required
- input can be easily mapped to output with the help of lookup table
- much faster than dynamic S box

Disadvantages (Static)

- Vulnerable to attacks, can weaken the algorithm.
- Linear Cryptanalysis can be done and S box can be cracked.

Advantages: (Dynamic)

- not vulnerable to any attacks, unless the key is known.
- dependent on the key.

Disadvantages: (Dynamic)

- extra hardware is required.
- slower than static S box

b) In AES, S-box acts only as a lookup table, thus it is static, and not dependent on the key.

Only the message in each round is mixed with the key. The mapping is the same and does not depend on the key.

AES:

PlainText

↓

Round 1 ← key_1

↓

Round 2 ← key_2

↓

⋮

Round n ← key_n

↓

CypherText

KEY SCHEDULE

Each Round:

- SubBytes → not dependent on key
- ShiftRows
- Mix Columns
- Add RoundKey → dependent on key