

3. ElGamal Scheme

$$q = 71$$

primitive root : 7 (e_1)

a) plaintext = 30

$$n = 2$$

$$C_1 = e_1^n \bmod q = (7)^2 \bmod 71$$

$$= \boxed{49}$$

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

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

$$= 270 \bmod 71$$

$$= \boxed{57}$$

$$C = \underline{(49, 57)}$$

b) n is diff

$$\textcircled{1} e_1^n \bmod q = C_1$$

$$\downarrow n$$

$$7 \bmod 71 = 59$$

$$\textcircled{2} (30 * e_2^n) \bmod q = C_2$$

$$\Rightarrow \boxed{n = 3}$$

by trial & error

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

$$= 810 \bmod 71 = 29$$

$$\boxed{C_2 = 29}$$

4. $C = 10$
 ciphertext

$$e = 5$$

$$n = 35$$

$$M = ?$$

plaintext

n is a product of two primes p, q

for $n = 35$,

$$p = 7 \text{ and } q = 5$$

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

$$e \cdot d = 1 \pmod{\phi(n)}$$

$$e = 5$$

$$5 \cdot d = 1 \pmod{24}$$

$$\boxed{d = 5} \text{ multiplicative inverse of } e$$

priv Key

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

$$= (10)^5 \pmod{35}$$

$$= 100000 \pmod{35}$$

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

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 no longer 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.

Alice receives X_2 .

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

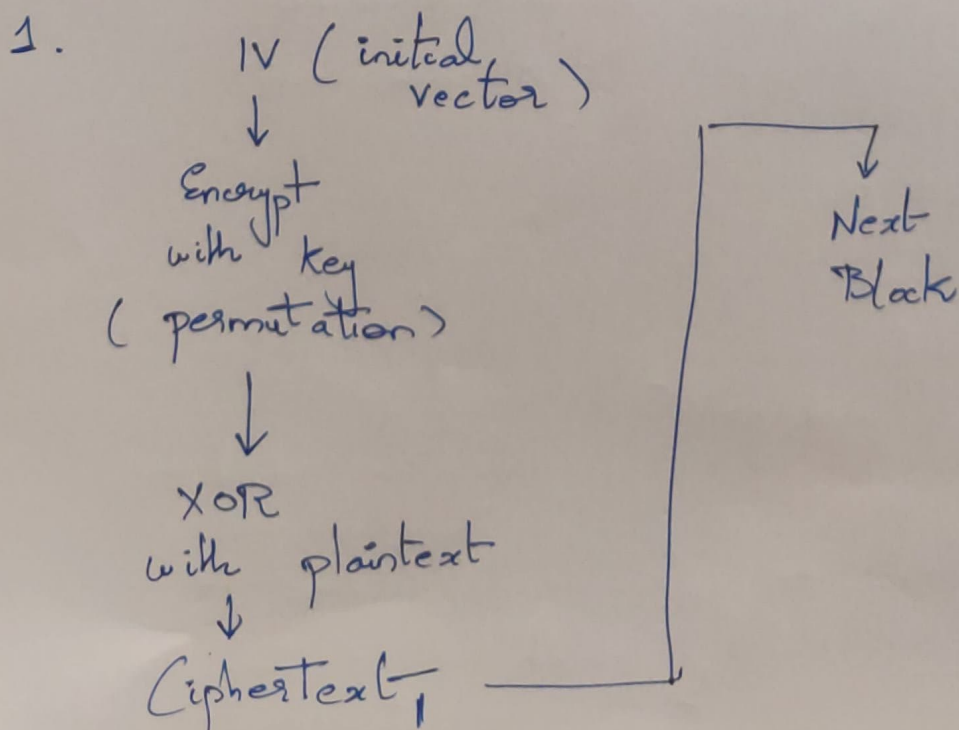
Similarly Bob receives $X_1 = g^m \bmod p$.

He uses his prv 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.



$$IV = 1010$$

1010
↓
permute
with key
↓

0110

↓
⊕

0100

C₁: 0010

0010

↓
permute
↓

0100

⊕

1011

C₂: 1111

1111

↓
permute
↓

1111

⊕

1100

C₃: 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

Advantages:

- 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

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

In AES,

b) 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.

Dynamic

pg 6

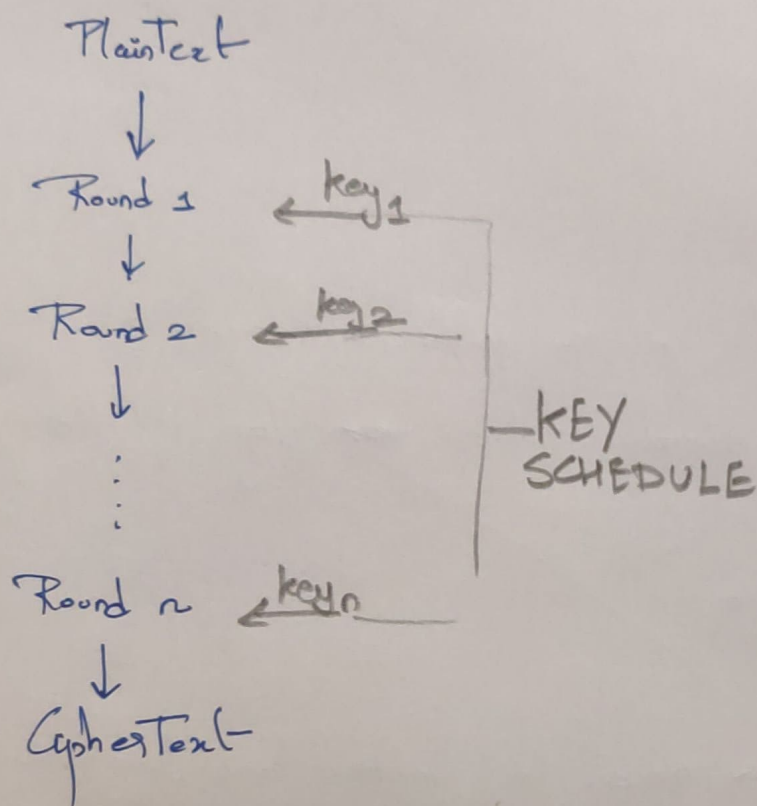
Advantages:

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

Disadvantages:

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

AES:



Each Round:

- SubBytes → not dependent on Key
- Shift Rows
- Mix Columns
- Add Roundkey → dependent on Key