References:

* Douglas R Stinson -
  Cryptography: Theory & Practice (CRC press)

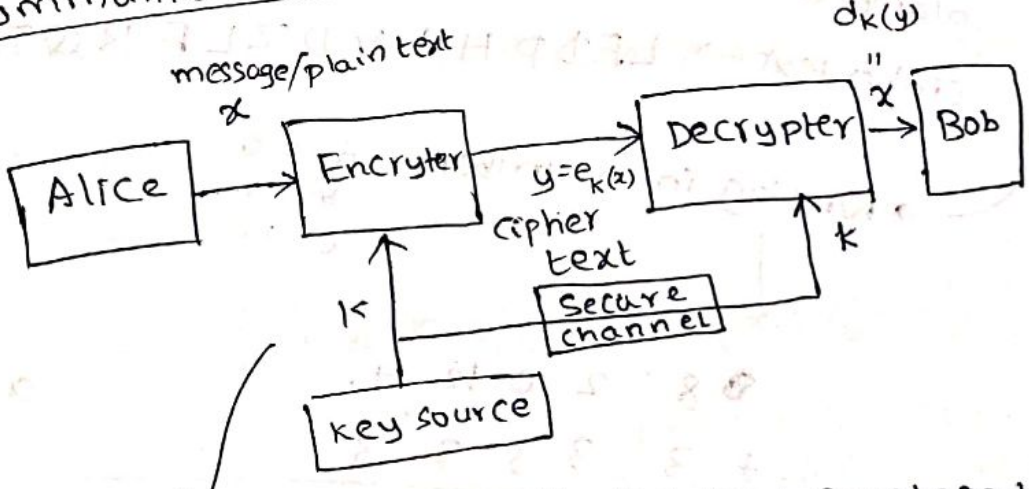
* W. Stallings -
  Cryptography and Network Security - Principles & Practice, Prentice Hall.

* Menezes, Oorschet, Vanstone
  - Hand book of Applied Cryptography

* A. Stranoyvitch
  - Introduction to Cryptography with mathematical foundations & computer implementation.

* Cryptography
  → art or science of secret writing

Communication channel



⇒ Symmetric key or Secret key Cryptography

* ~~asymmetric key or public~~ key Cryptography

* Cryptosystem :-

A cryptosystem is a five tuple

$(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$

- $\mathcal{P}$ → plaintext space
- $\mathcal{C}$ → Ciphertext space
- $\mathcal{K}$ → key space
- $\mathcal{E}$ → Encryption rules
- $\mathcal{D}$ → Decryption rules

for each $k \in \mathcal{K}$, $\exists$ an encryption rule $e_K \in \mathcal{E}$ and a corresponding decryption rule $d_K \in \mathcal{D}$

$$e_K : \mathcal{P} \to \mathcal{C}$$

$$d_K : \mathcal{C} \to \mathcal{P}$$

$$d_K(e_K(x)) = x$$

* The Ceaser Cipher → shift each plaintext letter '3' letters down

Ex: i came, i saw, i conquered ← plaintext

ciphertext → LFDPH LVDZLFRQTXHUHG

→ Writing in numbers

a → 0
b → 1
c → 2
⋮

```
  8   2   0   12   4  . . . . . .     add mod 26
+ 3   3   3    3   3  . . . . . .
-----------------------------------
 11   5   3   15   7  . . . .          cipher text
```

* The shift cipher:

$Z_{26} = \{0, 1, \ldots\ldots, 25\}$

$\mathcal{P} = \mathcal{C} = K = Z_{26}$ ~~english Alphabet~~

For $k \in K$, $0 \le k \le 25$

$e_k(x) = (x + k) \bmod 26$

$d_k(y) = (y - k) \bmod 26$

Ex: $k = 11$

plaintext → ordinary english text

correspandance b/w alphabet characters & integers.

Plaintext → We will meet at midnight

Corresponding seq. of integers → 22 4 22 8 11 11 12 4 4 19 0 19 12 8 13 8 6 7 19

Add 11 mod 26 → 7 15 7 19 22 22 ? ..... .

Cipher text → H P H T W W ..... .

Ex: Cipher text →

↳ JBCRCLQRWCRVNBJENBWRWN

* The Affine Cipher :

$\mathcal{P} = \mathcal{C} = Z_{26}$

$K = \{(a, b) \in Z_{26}^2 \mid \gcd(a, 26) = 1\}$

↓ needed for $a \in Z_{26}$ to have multiplicative inverse mod 26

For "$k \in K$" (a, b).

$e_k(x) = (ax + b) \bmod 26$, $x \in \mathcal{P} = Z_{26}$

$d_k(y) = (a^{-1}(y - b)) \bmod 26$, $y \in \mathcal{C} = Z_{26}$

Above, $y \equiv ax+b \pmod{26}$, $y, x \in Z_{26}$

$\Rightarrow y-b \equiv ax \pmod{26}$

~~$a^{-1}(y-b)$~~

* Theorem:

The congruence $ax \equiv b \pmod{m}$ has a unique soln $x \in Z_m$ for every $b \in Z_m$ iff $\gcd(a, m) = 1$

* In the Affine cipher above,

$|K| = \phi(26) \times 26 = 12 \times 26 = 312$

$\phi(m)$ → No. of integers $< m$ which are co-prime to m.

* Theorem:

Suppose $m = p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_n^{e_n}$, p_i's are distinct primes,

$$\phi(m) = m \prod_{i=1}^{26} \left(1 - \frac{1}{p_i}\right), \quad e_i > 0, \ 1 \le i \le n$$

* Ex:

$K = (7, 3)$.

$y = e_k(x) = (7x+3) \bmod 26$

$d_k(y) = 7^{-1}(y-3) \bmod 26$

$7^{-1} \bmod 26 = 15 \quad [\because 7 \times 15 \bmod 26 = 1]$

$\therefore d_k(y) = 15(y-3) \bmod 26 = (15y-45) \bmod 26$

$= (15y-19) \bmod 26$

→ plaintext: hot

↓

7 14 19

Encryption: $(7 \times 7 + 3) \bmod 26 = 0$

$(14 \times 7 + 3) \bmod 26 = 23$

$(19 \times 7 + 3) \bmod 26 = 6$

Cipher text: A X G

Decryption:

A	X	G
0	23	6

A : $15 \times 0 - 19 \bmod 26 = 7 \rightarrow h$

X : $15 \times 23 - 19 \bmod 26 = 14 \rightarrow o$

G : $15 \times 6 - 19 \bmod 26 = 19 \rightarrow t$

* The Substitution Cipher :-

$\mathcal{P} = \mathcal{C}$ = set of 26-letter English Alphabet

$\mathcal{P} = \{a, b, \ldots, z\}$, $\mathcal{C} = \{A, B, C, \ldots, Z\}$

K = Set of all possible permutations of 26 alphabet characters

$|K| = 26! \approx 2^{88}$ → exhaustive search is infeasible

→ For each permutation $\Phi \in K$,

$e_\Phi(x) = \Phi(x)$ for $x \in \mathcal{P}$

$d_\Phi(y) = \Phi^{-1}(y)$ for $y \in \mathcal{C}$

where Φ^{-1} is the inverse permutation of Φ

Example:

Φ :

a	b	c

Encryption func^n Φ :

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
X	N	Y	A	H	P	O	G	Z	Q	W	B	T	S	F	L	R	C	V	M

u	v	w	x	y	z
U	E	K	J	D	I

Decryption func^n Φ^{-1} :

A	B	C	D	. . .
d	l	r	y	- - -

key, $k = \Phi$

Ciphertext : MGZVYZLGHCMHJMYXSNHA
.H YCDLMHA

plain text : this cipher text can be decrypted

→ Substitution cipher is vulnerable to frequency analysis.

→ Given a large cipher text
→ Calculate the frequency of each symbol in that ciphertext.

alphabet	probability
e	0.127
t	0.091
a	0.082
⋮	⋮
j	0.002
x, q, z	0.001

* Monoalphabetic cipher:
Each alphabet character is mapped to a unique alphabetic character

* Polyaphabetic cipher:
Uses different monoalphabetic substitutions while ~~making~~ moving through the plain text
→ Vigenere Cipher
→ Hill Cipher
→ Transposition / permutation cipher.

* Vigenere Cipher:

$P = C = K = (Z_{26})^m$. m → a fixed positive integer

For $K = (K_1, K_2, \ldots, K_m) \in K$

$e_K(x) = (x_1 + K_1, x_2 + K_2, \ldots, x_m + K_m)$

$d_K(y) = (y_1 - K_1, y_2 - K_2, \ldots, y_m - K_m)$

all operations are mod 26.

Example:

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

→ m = 5

→ keyword is 'money' = (12, 14, 13, 4, 24)

→ plaintext: vive la france

key : mone ymoneymo

Encryption: add mod 26

→ ciphertext: 7 22 8 8 9 12 | 9 4 4 11 14 18

HWI I J M T EE L O S

→ Can still crack by calculating the probability of digrams or trigrams (two consecutive letters (th high prob.) — example)

* The Hill Cipher:

→ m → some fixed positive integer.

$P = C = (Z_{26})^m$.

$K = \{ m \times m \text{ invertible matrix} \}$

For a key $k \in K$, we define

$e_k(x) = xK$, $x \in P$

$d_k(y) = yK^{-1}$, $y \in C$

all operations are mod 26

Example:

Plaintext → code blue alert

encoding matrix, $K = \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}$

code blue alert t n ← added to make it even (our wish)

2 14 3 4 1 11 20 4 0 12 4 17 19 13

Cipher text in Z_{26} →

$$\begin{pmatrix} 2 & 14 \\ 3 & 4 \\ 1 & 11 \\ 20 & 4 \\ 0 & 12 \\ 4 & 17 \\ 19 & 13 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}$$

= 16 20 7 18 12 9 24 0 11 7 21 7 6 25

Ciphertext → Q U H S M J Y A L H V H G Z

→ If Hill cipher is used

ciphertext only attack { and we know only 'y'
↳ difficult cyptanalize

known plaintext attack { x (known 'x'), y (known 'y') & m known
↳ very easy to crack.

* Excercise:

y, x known → ~~$k = x^{-1} y$~~

friday → plain text
m = 2

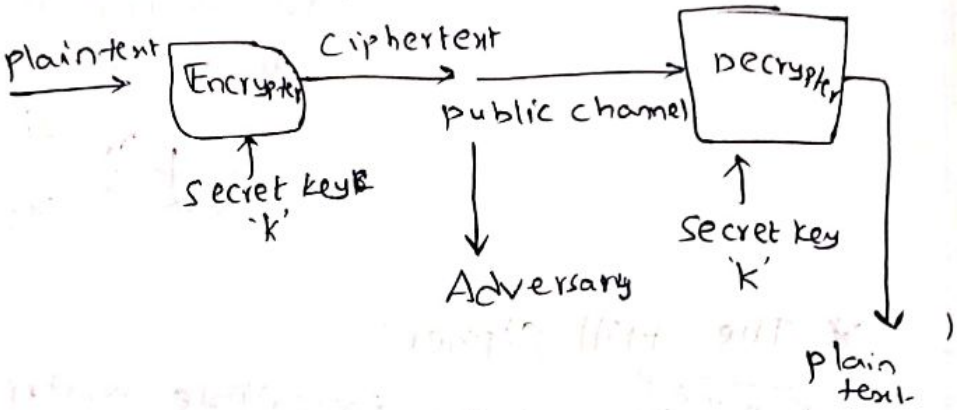
PQCFKU → Cipher text

Ans: $\begin{pmatrix} 7 & 19 \\ 2 & 5 \end{pmatrix}$

* Cryptology → Cryptography
→ Cryptanalysis
↓
analyzes how powerful a cryptosystem is

* Cryptographic Security:

Kirchoff's principle: Assume that the adversary knows the algorithm that is used. The secret is only the secret key.



→ Adversary → passive adversary
→ Active adversary

Active adversary:
- can attack alter messages (delete, replay, insert, modify)
- can see Ciphertext (those that are available in Public channel)

passive adversary:
- Only can eavesdrop i.e listen to/view the traffic

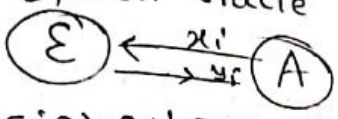
* Passive attacks
→ ciphertext only attack (opponent possesses a string of cipher text, y)
→ known plaintext attack (opponent possesses a string of plaintext x & the corresponding cipher text, y)

→ chosen plaintext attack

(x_i, y_j, $1 \le i \le n$ are known)

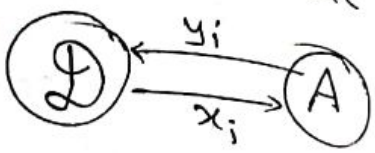
(x_i's are chosen by the adversary)

opponent has obtained temporay access to the encryption oracle



→ Chosen ciphertext attack

(opponent has obtained Temporary access to the decryption oracle



* The Hill Cipher :-

Fix $m \in Z^+$

$K = m \times m$ invertible matrix

Encryption: $y = xK$, $x \in Z_{26}^m$

(y: $1 \times m$, x: $1 \times m$, K: $m \times m$)

Decryption: $x = yK^{-1}$

→ known plaintext attack

(x, y) is known

Ex: friday → PQCFKU

(x: friday, y: PQCFKU)

$m = 2$ $\quad y = xK$

fr → PQ :⇒ $(15\ \ 16) = (5, 17)K$

$(2, 5) = (8, 3)K$

$(10, 20) = (0, 24)K$

$$\begin{pmatrix} 2 & 5 \\ 10 & 20 \end{pmatrix} = \begin{pmatrix} 8 & 3 \\ 0 & 24 \end{pmatrix} K$$

Y $\quad X$

det X

$\begin{pmatrix} 15 \\ 2 \end{pmatrix}$

K =

k

k

* Tr

r

o

$\det X = |X| = 8 \times 24$ is not coprime to 26
$\Rightarrow$ not invertible.

$$\begin{pmatrix} 15 & 16 \\ 2 & 5 \end{pmatrix} = \begin{pmatrix} 3 & 17 \\ 8 & 3 \end{pmatrix} K$$
Y_1 X_1

$|X_1| = 15 - 136 = -121$

$-121 \equiv 9 \pmod{26}$ (9 coprime to 26)

$K = 9^{-1} \begin{pmatrix} 3 & -17 \\ -8 & 5 \end{pmatrix} \begin{pmatrix} 15 & 16 \\ 2 & 5 \end{pmatrix}$ invertible

$K = 3 \begin{pmatrix} 3 & -17 \\ -8 & 5 \end{pmatrix} \begin{pmatrix} 15 & 16 \\ 2 & 5 \end{pmatrix}$ $[\because 9 \times 3 \equiv 1 \pmod{26}]$
$9^{-1} = 3$

$$K = \begin{pmatrix} 9 & -51 \\ -24 & 15 \end{pmatrix} \begin{pmatrix} 15 & 16 \\ 2 & 5 \end{pmatrix}$$

$$K = \begin{pmatrix} 9 & 1 \\ 2 & 15 \end{pmatrix} \begin{pmatrix} 15 & 16 \\ 2 & 5 \end{pmatrix}$$

$$K = \begin{pmatrix} 137 & 149 \\ 60 & 109 \end{pmatrix} = \begin{pmatrix} 7 & 19 \\ 8 & 3 \end{pmatrix}$$

* Transposition/permutation technique:

→ rail fence technique

Ex: meet me after the party.

rail fence of depth 2 →

m e m a t r h p r y
e t e f e t e a t (z) ← added by me.

MEMATRHPRYETEFETEATZ

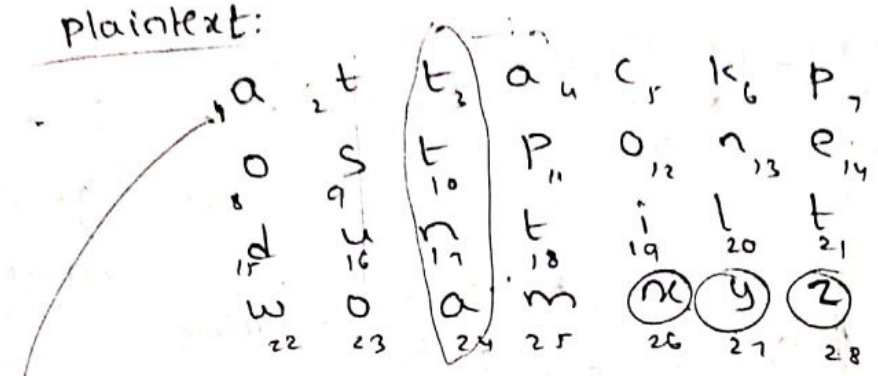
More generally,

Example: attack postponed until two am

(4 × 7 rectangle)

Key: 4 3 1 2 5 6 7

Plaintext:



Ciphertext:-

TTNAAPTM TSUO AODW COIX
KNLY PETZ

Concept of round (round 1, round 2, ...)

→ original plaintext → 1, 2, 3, 4, ..., 28

→ after 1st transposition → 3, 10, 17, 24, ...

→ take 2nd transposition → 17, 9, 5, 27, 24, 16, 12, 7 .....

*DES (Data Encryption Standard)

* Transposition / Permutation Cipher :-

→ m → a +ve integer

→ $P = C = (Z_{26})^m$

→ K = set of all possible permutations of $\{1, 2, 3, \ldots, m\}$

For each $\pi \in K$

$$e_\pi(x_1, x_2, \ldots, x_m) = (x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(m)})$$

$$d_\pi(y_1, y_2, \ldots, y_m) = (y_{\pi^{-1}(1)}, y_{\pi^{-1}(2)}, \ldots, y_{\pi^{-1}(m)})$$

π^{-1} is the inverse permutation of π

Ex:-

→ m = 6

→ key is the following permutation π:

x	1	2	3	4	5	6
y	3	5	1	6	4	2

⇒ inverse permutation π^{-1}.

x	1	2	3	4	5	6
$\pi^{-1}(x)$	3	6	1	5	2	4

plaintext: defend the hilltop at sunset

1 2 3 4 5 6 1 2 3 4 5 6 1 2 3 4 5 6 1 2 3 4 5 6

defend the hil ltopat sunset

Ciphertext: FNDDEE EIIL HH OALTPTNESTSU

→ The permutation cipher is a particular case of Hill Cipher.

π on $\{1, 2, \ldots, m\}$

$K_\pi = (K_{ij})_{m \times m}$

$K_{ij} = 1$ if $i = \pi(j)$

$= 0$ otherwise

$$K_\pi = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \end{array} \begin{array}{c} \begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \end{array} \\ \begin{pmatrix} & & 1 & & & \\ & & & & & 1 \\ 1 & & & & & \\ & & & & -1 & \\ & 1 & & & & \\ & & & 1 & & \end{pmatrix} \end{array}$$

$$\boxed{K_{\pi^{-1}} = (K_\pi)^{-1}}$$

$$K_{\pi^{-1}} = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \end{array} \begin{array}{c} \begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \end{array} \\ \begin{pmatrix} & & 1 & & & \\ & & & & & 1 \\ 1 & & & & & \\ & & & & 1 & \\ & 1 & & & & \\ & & & 1 & & \end{pmatrix} \end{array}$$

* key: (4×7 rectangle)

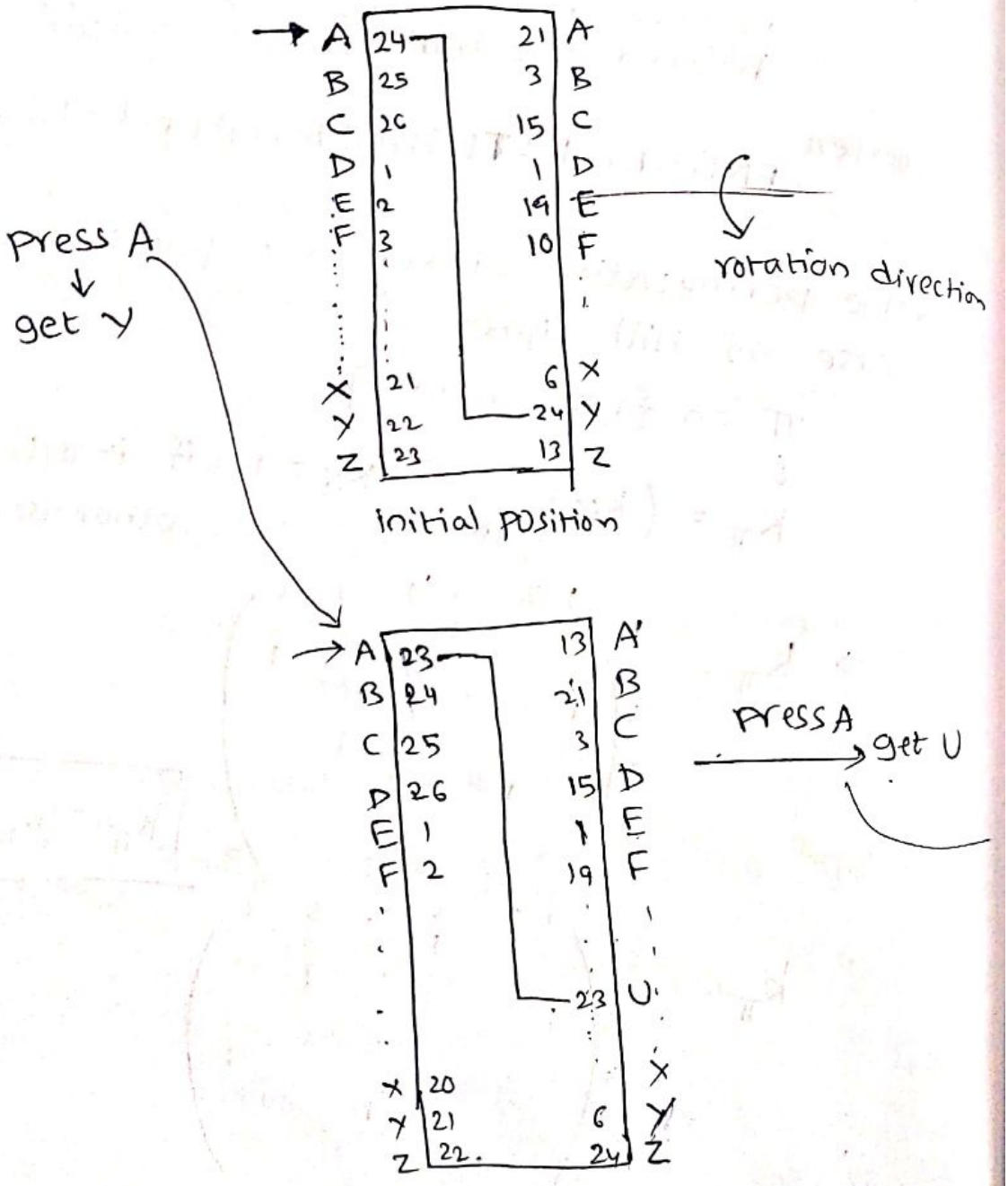
key

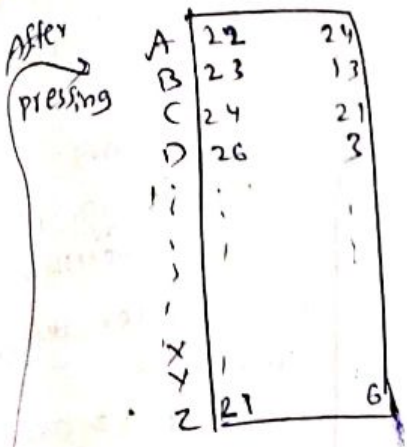
* Rotor Machine:

→ Use multiple stages of encryption

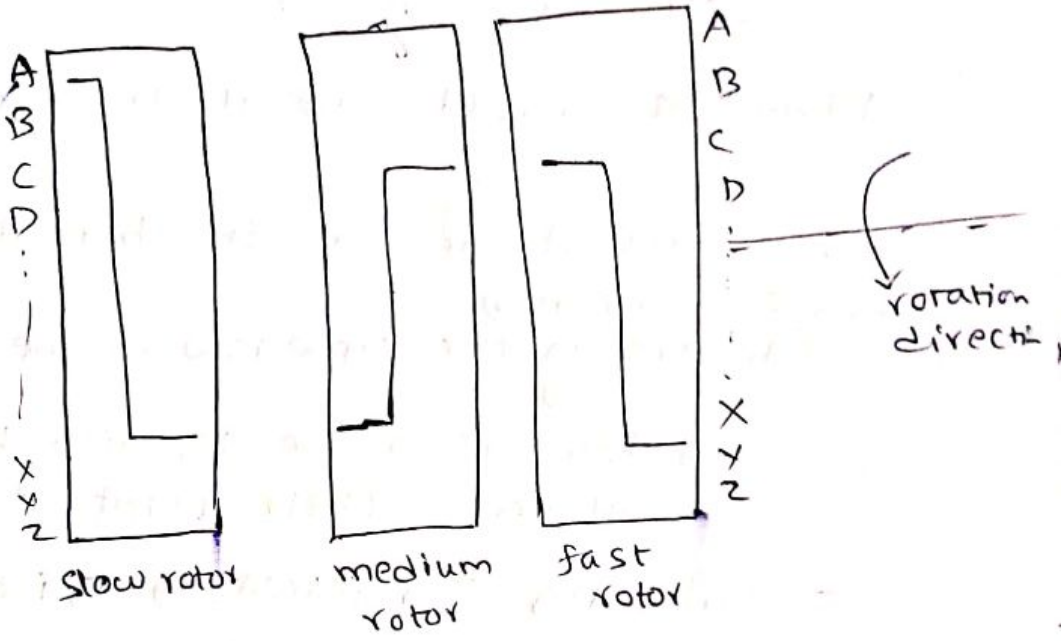
→ Enigma, Purple → based on rotor principle
(Germany) (Japan)

→ Machine consists of a set of independently rotating cylinders through which electrical pulses can flow.





→ 3 rotor



→ After 26 rotations of fast rotor, medium rotor rotates once

→ " " medium rotor, slow rotor " "

↳ The cipher values repeat after 26 X 26 X 26 presses.

* Play fair Cipher

Use the keyword CHARLES (charles wheatstone invented this cipher).

5X5 matrix

c	h	a	r	l
e	s	b	d	f
g	i/j	k	m	n
o	p	q	t	u
v	w	x	y	z

balloon
ba ll oo n
↓ ↓
same letters
use a filler letter such as 'x'
ba lx lo on

Plaintext: meet me at the bridge

me et me at th eb ri dg e(x)

Case I :- (same row)
e, b are in the same row in the matrix
⇓
They are to be replaced by the letters to their right i.e s, d

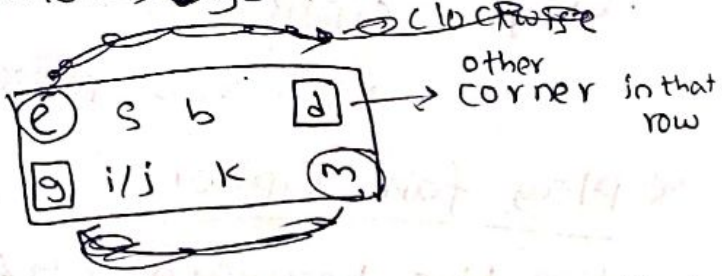
Similarly, ng is replaced by gi (or) gj

Case II :- (same column)

dt → my
ty → yr

Case III :- (Otherwise)

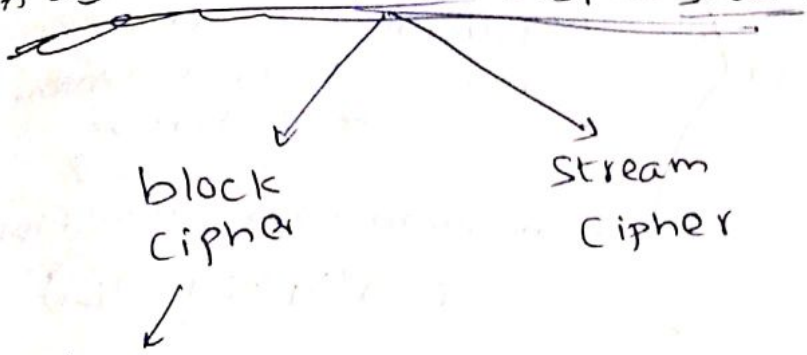
me → gd



∴ Ciphertext → GD DO GD RQ PR SD HM

EM BV

* Symmetric Key Cryptosystem *



eg:
Shift cipher,
Substitution Cipher,
Vigenere Cipher,
Permutation Cipher,
Playfair Cipher etc.

→ Block Cipher (stateless)

block size, $n \geq 64$ bits

block 1 block 2
$x = x_1 x_2 \ldots\ldots$

→ plaintext string $x = x_1 x_2 \ldots\ldots$

→ key 'k'

→ Ciphertext string $\ldots e_k(x_1)\, e_k(x_2) \ldots\ldots$

explain → SPN, DES, Rijndel (AES), IDEA, RC6 & many more

→ stream cipher (state cipher)

→ key: K

→ keystream: $k_1\ k_2\ k_3 \ldots\ldots$

→ plaintext: $x_1\ x_2\ x_3 \ldots\ldots$

→ ciphertext: $e_{k_1}(x_1)\, e_{k_2}(x_2)\, e_{k_3}(x_3) \ldots\ldots$

$k_i = g(k, x_{i-1}, y_{i-1})$

depends on previous state

~~stream~~

* Stream cipher → Synchronous stream cipher (keystream is constructed from the key, independent of plaintext/ciphertext
→ Non-synchronous stream cipher

$K_i = g(K, x_{i-1}, y_{i-1})$

Ex:- (One time pad)

$P = C = K = \{0,1\}^n$

plaintext : $(x_1, x_2 \dots x_n)$

key : $(k_1, k_2 \dots k_n)$

Cipher text : $(x_1 \oplus k_1, x_2 \oplus k_2, \dots x_n \oplus k_n)$

Unconditionally secure provided the key stream is truely random

↓ getting it is very difficult

Vulnerable to known plaintext attack.

* Perfect Secrecy :-

$P(x|y) = P(x)$ ∀ plaintext $x \in P$ &
∀ ciphertext $y \in C$.

$P(x|y)$ ← probability

* Shannon's Theorem :-

Suppose (P, C, K, E, D) is a cryptosystem where $|P| = |C| = |K|$.

Then the cryptosystem provides perfect secrecy iff

(i) every key is used with equal probability $\frac{1}{|K|}$

and (ii) for every $x \in \mathcal{P}$ & $y \in \mathcal{C}$, there is a unique key K st $e_k(x) = y$.

Ex: (perfect Secrecy)

→ One bit encryption

$$C = P \oplus K$$

$$P(k=0) = \frac{1}{2} = P(k=1)$$

let $P(p=0) = 0.6$, $P(p=1) = 0.4$

Show that this ensures perfect secrecy.

$$P(p=0 \mid c=1) = \frac{P(p=0,\ c=1)}{P(c=1)}$$

$$= \frac{P(c=1 \mid p=0)\, P(p=0)}{P(c=1)}$$

$$= \frac{P(k=0)\, P(p=0)}{P(c=1 \mid p=0)\, P(p=0) + P(c=1 \mid p=1)\, P(p=1)}$$

$$= \frac{\frac{1}{2} \times 0.6}{\frac{1}{2} \times 0.6 + \frac{1}{2} \times 0.4} = 0.6$$

$$= P(p=0).$$

Similarly, $P(p=0 \mid c=0) = P(p=0)$

$P(p=1 \mid c=0) = P(p=1)$

$P(p=1 \mid c=1) = P(p=1)$

Ex:- (Vigenere Cipher) ← block cipher with blocks of size 'm' (or) Stream cipher with each letter as x_i

$\mathcal{P} = \mathcal{C} = Z_{26}$, $K = (Z_{26})^m$

if $k = k_1, k_2, \ldots, k_m$, define keystream as

$$K_i = \begin{cases} \alpha_i, & 1 \le i \le m \\ K_{i-m}, & i \ge m+1 \end{cases}$$

$k_1 k_2 k_3 \ldots k_m$ $k_1 k_2 \ldots k_m$ $k_1 k_2 \ldots k_m$

↓

Periodic keystream with period 'm'.

Plaintext → $x_1 x_2 \ldots$

Key stream → $k_1 k_2, \ldots$

Ciphertext → $x_1 + k_1, x_2 + k_2, \ldots \mod 26$.

→ periodic keystream with period 'd':

$$K_{i+d} = K_d \quad \forall i \ge 1$$

d → period.

→ Key streams with large periods are desirable.

→ PRSG / PRNG → Pseudo Random Sequence (or) Number Generator.

→ Another method of generating synchronous keystream is

→ Use linear recurrence relation.

→ $K = (\alpha_1, \alpha_2, \ldots \alpha_m)$ → Initial Value / Vector (IV)

→ define keystream

$$K_i = \alpha_i, \quad 1 \le i \le m$$

$$K_{i+m} = \sum_{j=0}^{m-1} c_j K_{i+j} \mod 2, \quad c_j \in Z_2 \quad \forall i \ge 1$$

New key → $(\alpha_1, \alpha_2, \ldots, \alpha_m), c_0, c_1, \ldots (m-1)$

↳ 2m values

Take, $c_0 = 1$

$(\alpha_1, \alpha_2 \ldots \alpha_m) \neq (0, 0, \ldots 0)$

max. period → $2^m - 1$

Illustration:

$m = 4$ key stream : 1000110

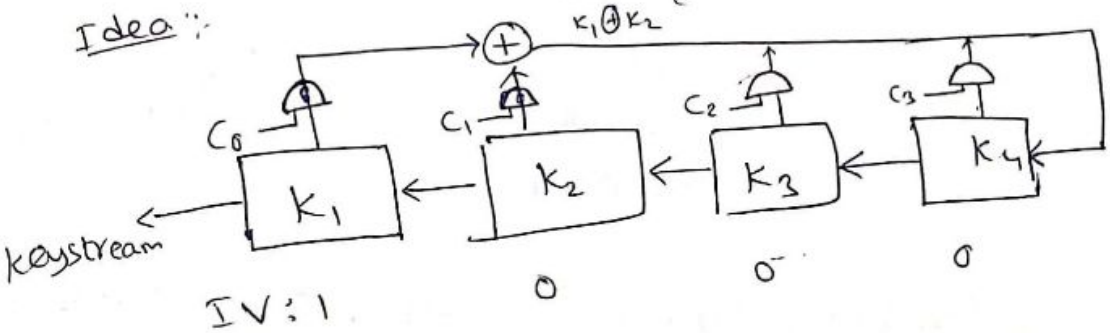
$k_{i+4} = k_i + k_{i+1} \bmod 2 \quad , i \geq 1$

IV = (1,0,0,0)

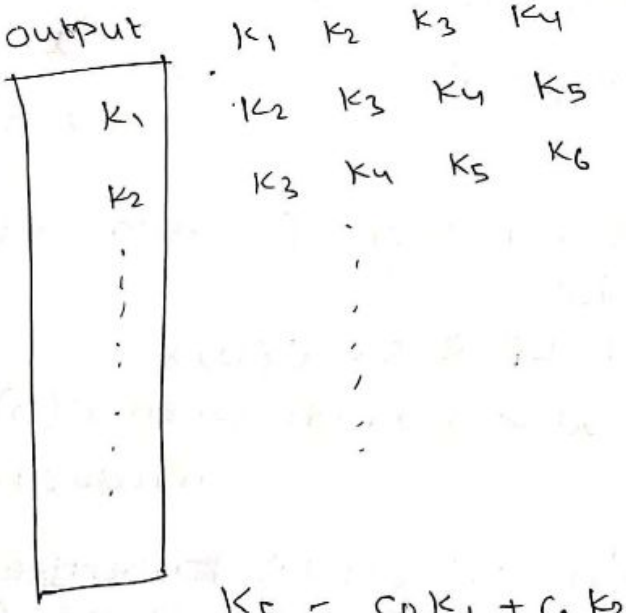
* PRNG (LFSR) → $\langle 4, C(x) \rangle$ LFSR (max. period $2^n - 1$)
  ↳ Connection Polynomial

Linear Feedback Shift Register

Idea:



$k_5 = (k_1 + k_2) \bmod 2$



$k_5 = c_0 k_1 + c_1 k_2 + c_3 k_3 + c_4 k_4$

$C(x) = 1 + c_3 x + c_2 x^2 + c_1 x^3 + c_0 x^4$

Fact: LFSR $\langle L, C(D) \rangle$
↳ $c_0, c_1, \ldots, c_{L-1}$

$C(D) = 1 + c_{L-1} D + c_{L-2} D^2 + \cdots + c_0 D^L, c_0 \neq 0$

Every output sequence of an LFSR $\langle L, C(D) \rangle$ is

periodic iff the connection polynomial has degree 'l'.

Fact: N = period of an LFSR $\langle l, C(D) \rangle$

If C(D) is irreducible then $N \mid 2^l - 1$

If C(D) is primitive, then $N = 2^l - 1$

* $GF(2^l) = Z_2[x] / \langle C(D) \rangle - \{(0,0,\dots 0)\}$ (modulo)

Set of all polynomials with coefficients 0 or 1

$2^l - 1$ elements

→ $(Z_2[x]/\langle C(D) \rangle - \{(0,\dots 0)\}, *)$ forms a cyclic group. (* : multiplication)

↓

α is generator of this cyclic group, then $\{\alpha^0, \alpha^1, \dots \alpha^{2^l-2}\}$ is the whole group

If 'α' is a root of C(D), then C(D) is primitive

If N = period of LFSR $\langle l, C(D) \rangle$

* $N \mid 2^l - 1$ always holds when C(D) irreducible.

* $C(D) \mid D^N + 1$ (a) $D^N - 1$ · if C(D) is ~~primitive~~ irreducible

* C(D) is primitive if it is max length LFSR, $N = 2^l - 1$

→ m-sequences → sequences generated by a max-length LFSR.

* Nonsynchronous Stream Cipher

Ex: (Autokey cipher)

$P = C = K = Z_{26}$, $k \in K$

key stream: $K_1 = k$, $K_i = x_{i-1}$ $\forall i > 1$

$e_{K_i}(x_i) = (x_i + K_i) \bmod 26$

$d_{K_i}(y_i) = (y_i - K_i) \bmod 26$

Illustration :

key $k = 8$

plaintext : rendezvous

17, 4, 13, 3, 4, 25, 21, 14, 20, 18

key stream:

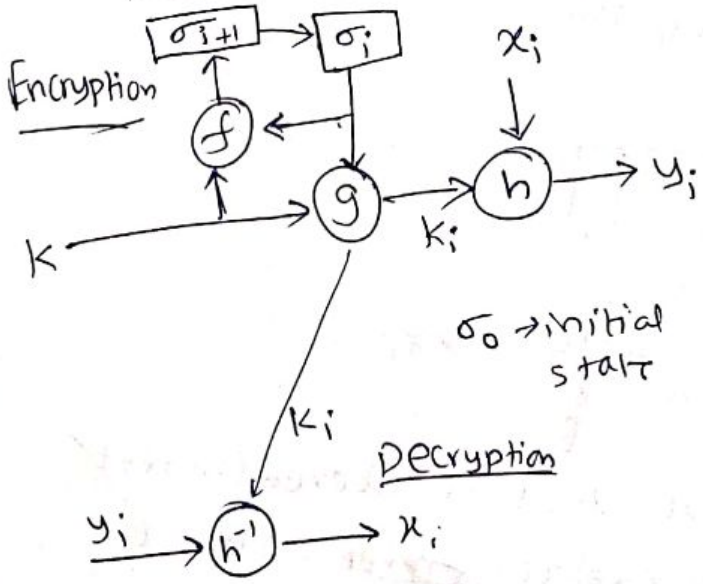
8, 17, 4, 13, 3, 4, 25, ...

Ciphertext:

25, 21, 17, 16, 7, ...

Z V R Q H D U . . . . . .

* General model of Synchronous Stream Cipher



~~$\sigma_{i+1} = f(\sigma_i, k)$~~

$\sigma_{i+1} = f(k, \sigma_i)$

$k_i = g(k, \sigma_i)$

f = next state func^n

g = keystream generator

σ_0 → initial state

h = output func^n

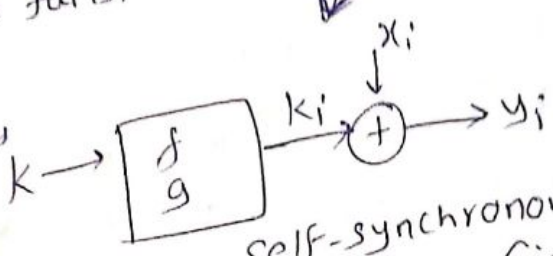
$y_i = h(x_i, k_i)$

Ex: LFSR, Binary additive Stream Cipher

decryption fails if synchronization fails.

↓ detecting active attacks

> cannot detect if adve changes one le of cipher tex



* General Model for xstream Cipher : self-synchronous

~~Synchr~~

$\sigma_i = (y_{i-t}, y_{i-t+1}, \ldots, y_{i-1})$

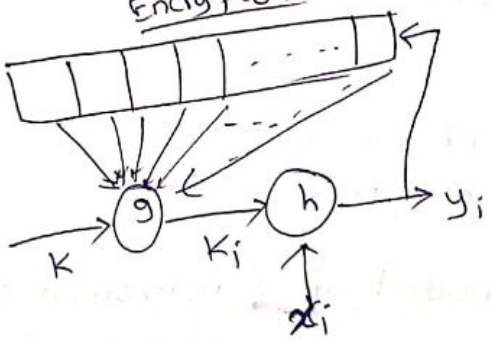
$k_i = g(k, \sigma_i)$

$y_i = h(k_i, x_i)$

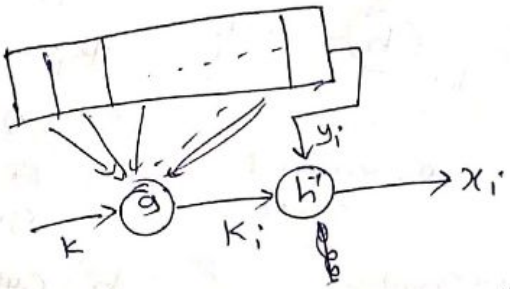
$K \Rightarrow$ key

$\sigma_0 = (y_{-t}, y_{-t+1}, \ldots, y_{-1})$

Encryption



Decryption



→ If a ciphertext digit is altered (insert/ modify/ replay/ delete), ~~cipher~~ after 't' consecutive ciphertext digits correct decryption resumes.

↳ detecting active attacks is difficult

* limited error propagation
  ↳ helps to detect active attacks

* $x_1 x_2 x_3 \cdots x_i \cdots x_j \cdots$
  ↳ (i) uniform distribution (#0's ≈ #1's) — frequency of each digit is same
  (ii) independence (x_j is independent of x_i $\forall i, j$)
  definition of a random sequence

* Golomb's Randomness Postulates:
  (Necessary condition for a periodic pseudo random sequence to look random).

$S = s_0, s_1, s_2, \cdots s_{N-1}, s_N, \cdots$ ($s_N = s_0$) (periodic of period 'N')

R_1: $\left| \sum_{i=0}^{N-1} (-1)^{s_i} \right| \leq 1 \Rightarrow |\#0's - \#1s| \leq 1$

R_2: In every period, $\frac{1}{2}$ of the runs have length '1', $\frac{1}{4}$ of the runs have length '2', $\frac{1}{8}$ of the runs have length '3'---

R_3: The auto-correlation func^n

$$C(T) = \sum_{i=0}^{N-1} (-1)^{s_i + (s_{i+T})}$$ is two valued

Explicitly, $C(T) = \begin{cases} N & \text{if } T \equiv 0 \pmod N \\ T & \text{if } T \neq 0 \pmod N \end{cases}$ (T is a constant)

Ex: $S^{15} = 0\,1\,1\,0\,0\,1\,0\,0\,0\,1\,1\,1\,1\,0\,1$

$R_1 \rightarrow$ Satisfies

$R_2 \rightarrow$ # runs = 8 (run → a block of same digits)

4 runs of length '1' → ✓
2 runs of length '2' → ✓
1 run of length '3' → ✓
1 run of length '4' → ✓

$R_3 \rightarrow$ $C(0) = 15$, $C(T) = -1$ for $1 \leq T \leq 14$

* Randomness measurement:

* Stream cipher strength → randomness of key stream.

→ Five basic tests (periodic seq. $s_0, s_1, s_2, \ldots$ period n)

→ Frequency Test (mono-bit test)

n_0 = #0's
n_1 = #1's

$$X_1 = \frac{(n_0 - n_1)^2}{n}$$ (n_0: no. of 0's, n_1: no. of 1's)

→ χ^2 distribution

→ Serial test (2-bit test)

00, 01, 10, 11

~~$X_2 = \frac{4}{n-1}\left(n_{00}^2 + n_{11}^2 + n_{10}^2 + n_{01}^2\right)$~~

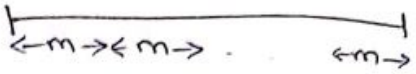
$$X_2 = \frac{4}{n-1}\left(n_{00}^2 + n_{11}^2 + n_{10}^2 + n_{01}^2\right) - \frac{2}{n}\left(n_0^2 + n_1^2\right) + 1$$

→ χ^2-distribution.

→ Run test (not needed) → R_2 → χ^2-distribution (in the postulates before)

→ Poker test

$$k = \left\lfloor \frac{n}{m} \right\rfloor$$



To test whether the no. of each sequence of length 'm' are approximately the same.

$$X_3 = \frac{2^m}{k}\sum_{i=1}^{2^m} n_i^2 - k$$

n_i → # of i^{th} pattern of length 'm'.

↓

χ^2-distribution.

→ Auto Correlation test → R_3 → $N(0,1)$ (in the postulates before)

* max LFSR
  - → m-seq

* eSTREAM project 2004 Completed in 2008.

Profile(SW)	Profile 2 (HW)
HC-128	Grain V1
Rabbit	MICKEY 2.0
Salsa 20/12	Trivium
SOSE MANUK	

Attacks → Algebraic attacks → multivariate non-linear eqns

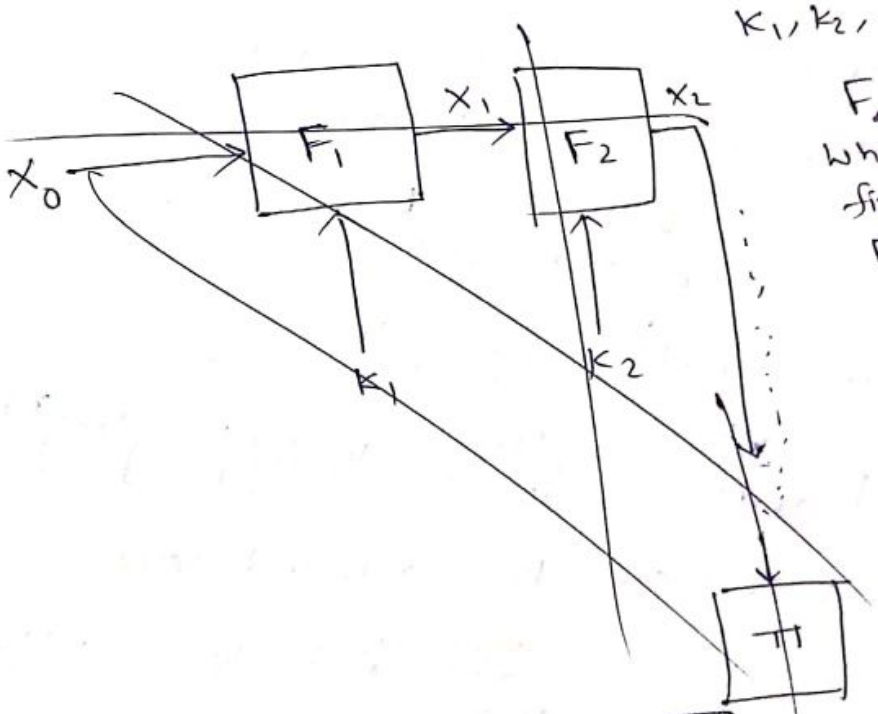
↓

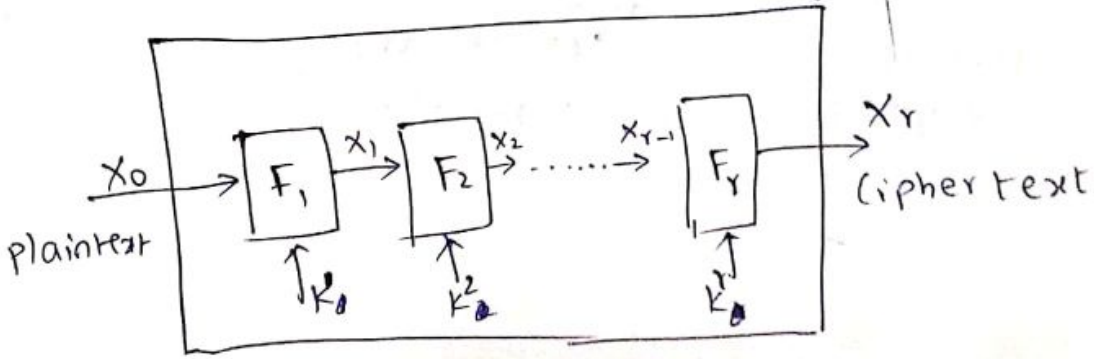
To solve, we use Grabner basics, SAT solvers

* r-round Block Cipher :

K ↓ round keys $k_1, k_2, \ldots, k_r$

$F_k(x, k)$ when k is fixed, $F_k(x)$ is invertible

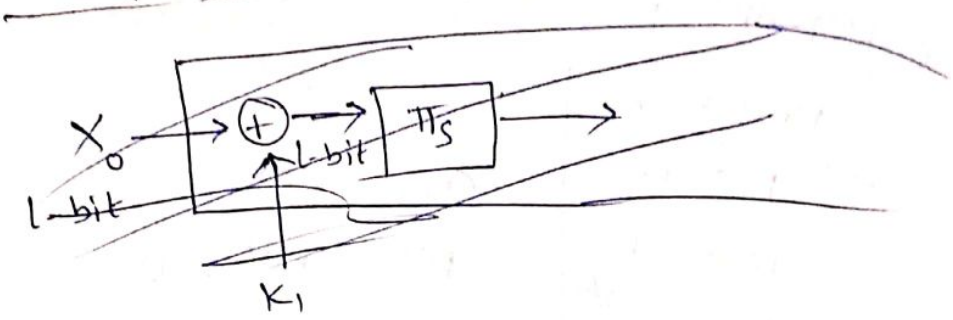


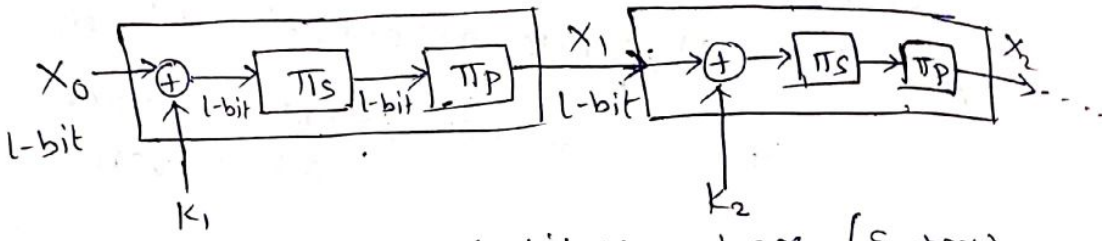


$F(X,K)$ is invertible when K is fixed

$\exists$ a func^n F^{-1} s.t. $F^{-1}(F(X,K),K) = X$

* SPN (Substitution-Permutation Network)





$\pi_S \rightarrow$ Substitution box (S-box)

π_P - permutation box (P-box)

DES → different S-boxes

AES → same S-box

$$\pi_S : \{0,1\}^l \longrightarrow \{0,1\}^l$$

$$\pi_P : \{0,1\}^{lm} \longrightarrow \{0,1\}^{lm}$$

$$P = C = \{0,1\}^{lm}, \quad K \subseteq \left(\{0,1\}^{lm}\right)^{r+1}$$

initial key K → round keys

~~Public key~~ $K^1, K^2, \ldots K^{r+1} \in \{0,1\}^{rm}$

~~Pub~~ ~~Scheduling~~ ~~algorithm~~

Public key scheduling algorithm

e.g. $K \in \{0,1\}^{32}$ 32-bit key

$l = m = r = 4$ → round keys

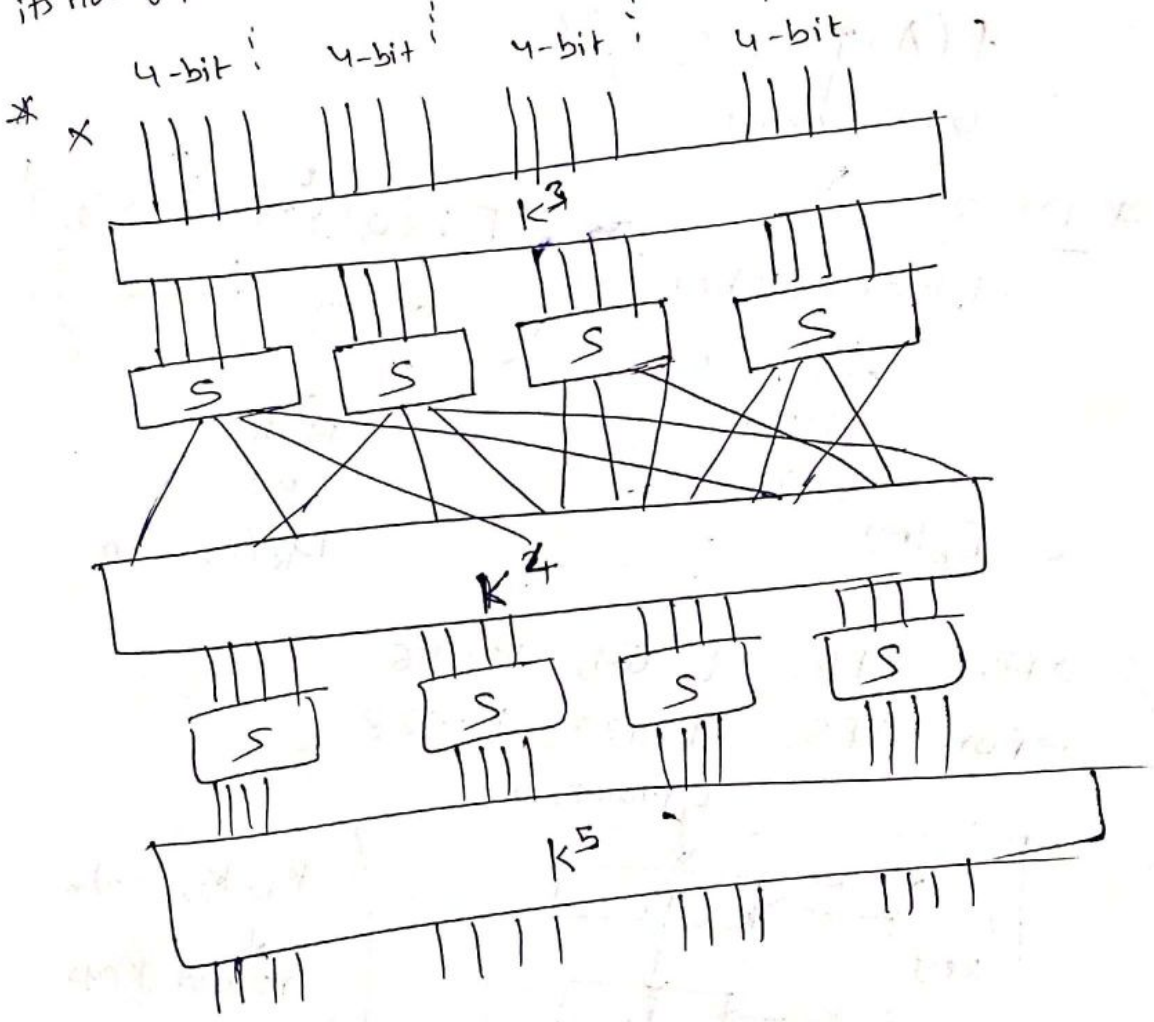
$K_1, K_2, \ldots, K_5 \in \{0,1\}^{16}$

$k = k_1 k_2 k_3 k_4 k_5 k_6 \ldots \ldots k_{16} k_{17} \ldots \ldots k_{32}$

K_i = 16 consecutive bits of 'k' from $k_{4i-3}, 1 \le i \le 5$

round key 'i'

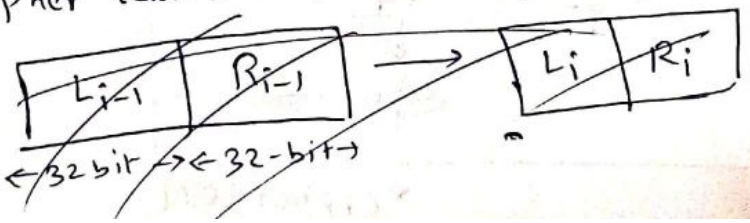
it's not pow(k, i), it is i^{th} round key

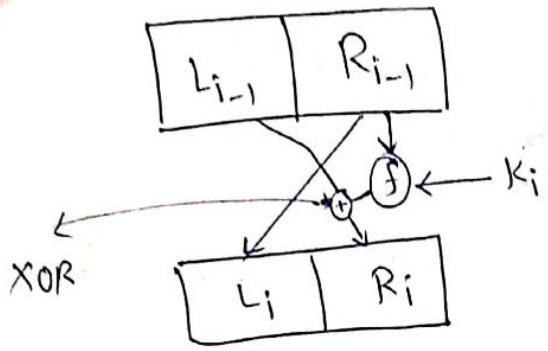


* DES uses Feistel Cipher:

Plaintext → 64 bits Key → 56 bits

Cipher text → 64 bits





One round of DES

$L_i = R_{i-1}$

$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$

$f(A, T) \in \{0,1\}^{32}$

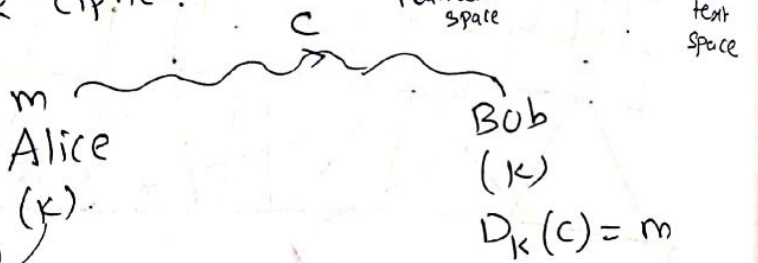
32 bit, 48-bit

* DES

→ Block cipher.

$E: \{0,1\}^l \times \{0,1\}^k \rightarrow \{0,1\}^l$

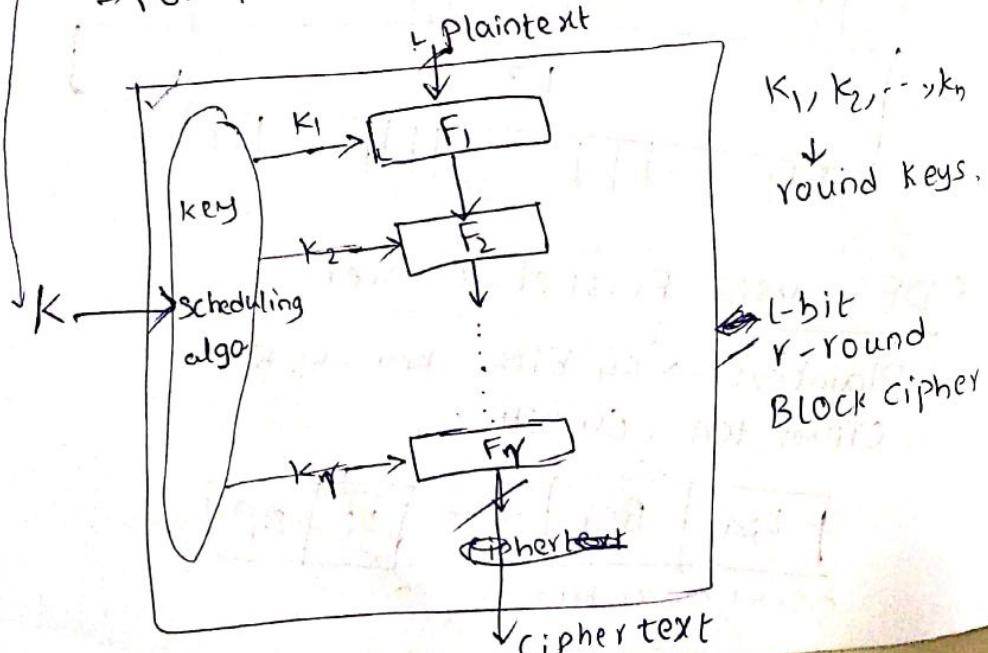
Plaintext space, Keyspace, Ciphertext space



$c = E_K(m)$

→ For DES, $L = 64$, $K = 56$

→ For AES, $L = 128$, $K = 128$



$F_i \rightarrow$ round function.

$$F_i : \{0,1\}^l \times \{0,1\}^\alpha \rightarrow \{0,1\}^l$$

$\alpha \rightarrow$ can be anything.

in i^{th} round, K_i can have any no. of bits.

DES $\rightarrow l = 64$

$k = 56$ bits

But K comes as 64 bits.

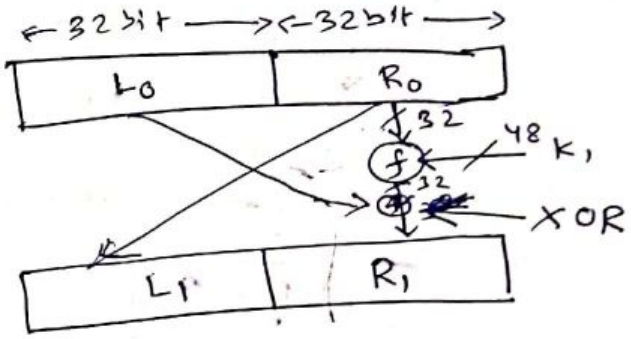
$K = \alpha_1 \alpha_2 \alpha_3 \ldots \alpha_7 \alpha_8 \alpha_9 \ldots \alpha_{16} \ldots \alpha_{64}$

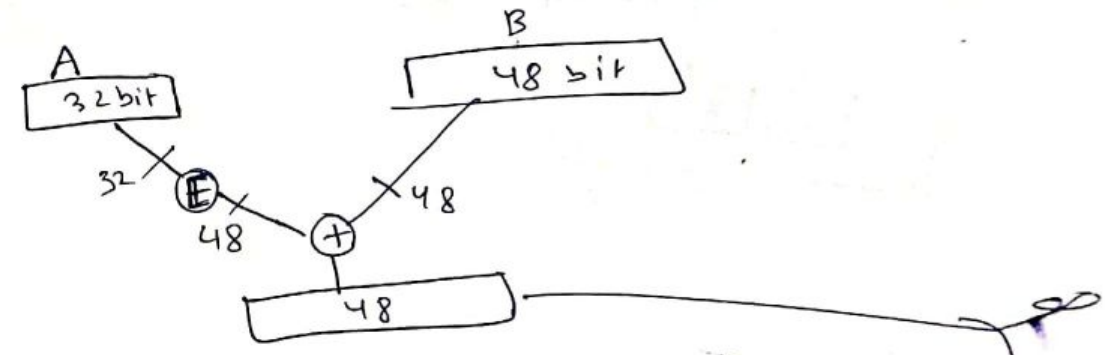
$\alpha_8, \alpha_{16}, \ldots, \alpha_{64}$ used for parity checking.

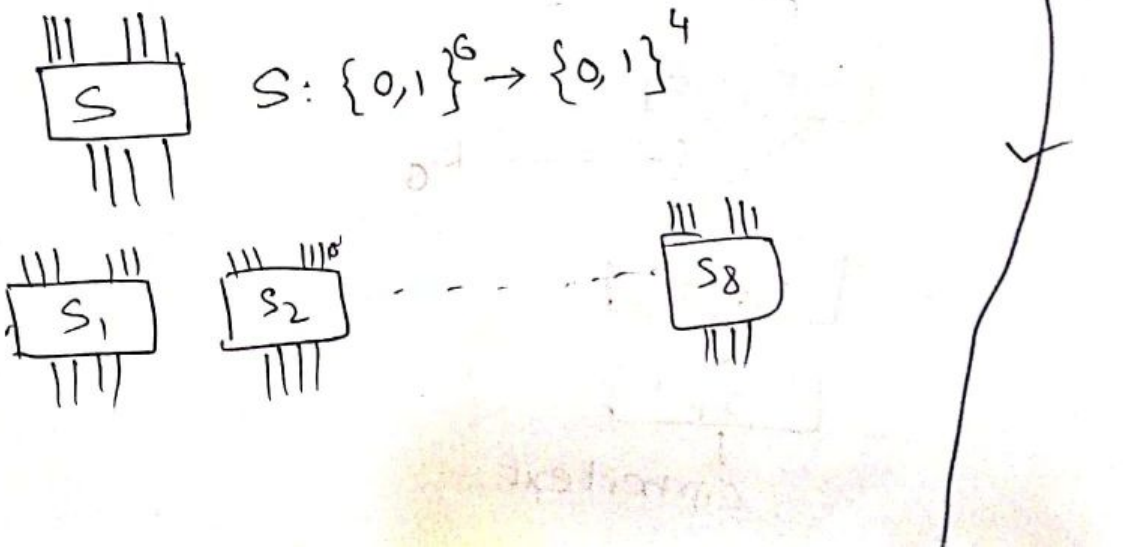
* Feistel cipher :- (a type of Block cipher)

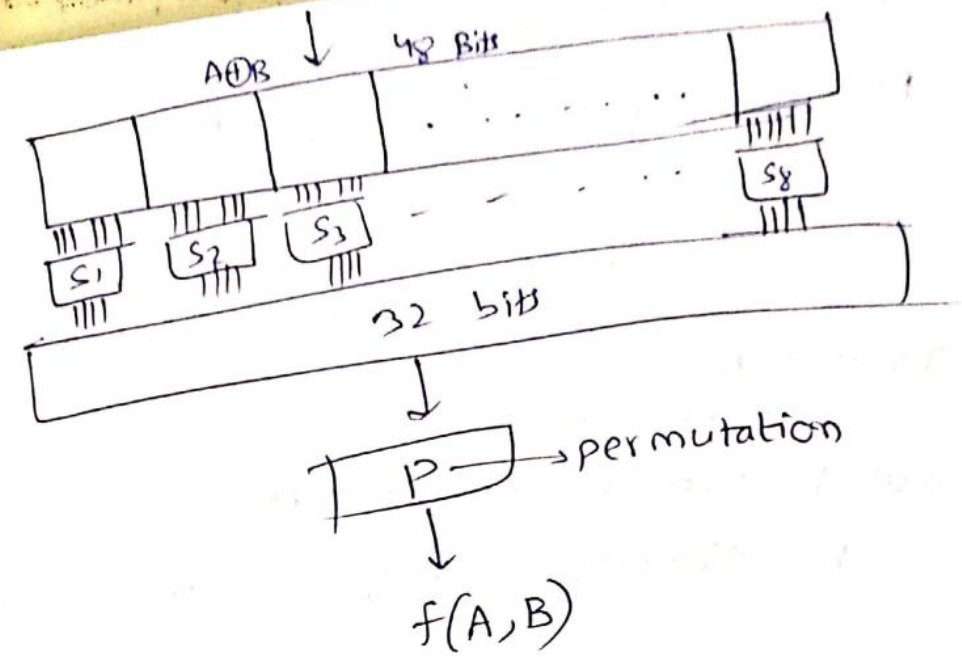
$L_1 = R_0$

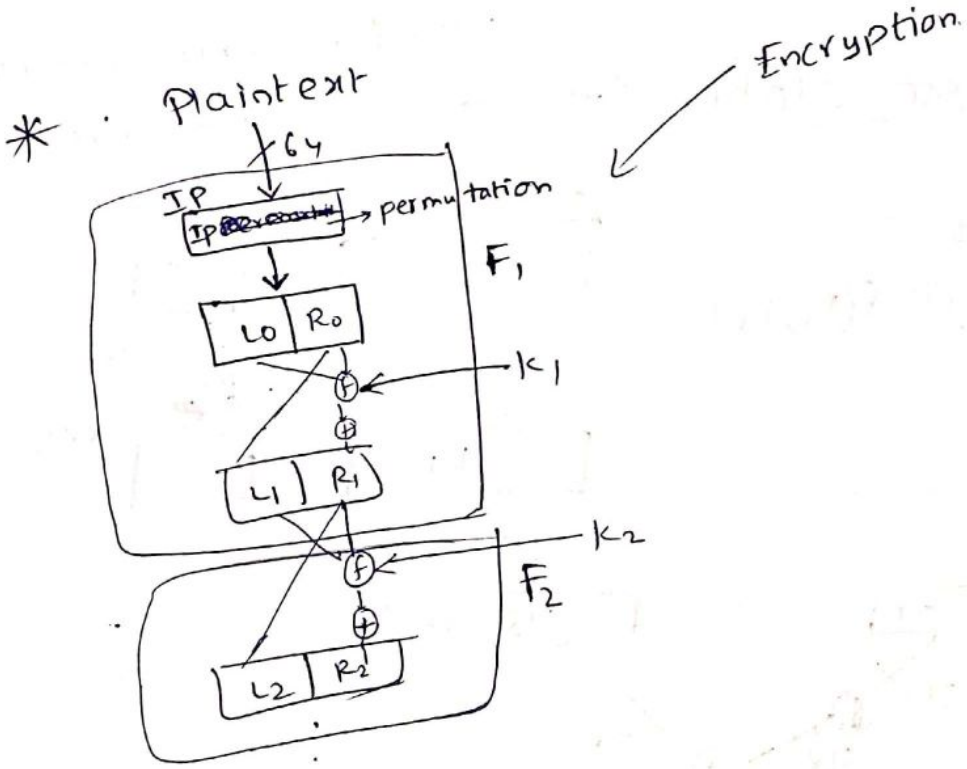
$R_1 = L_0 \oplus f(R_0, K_1)$

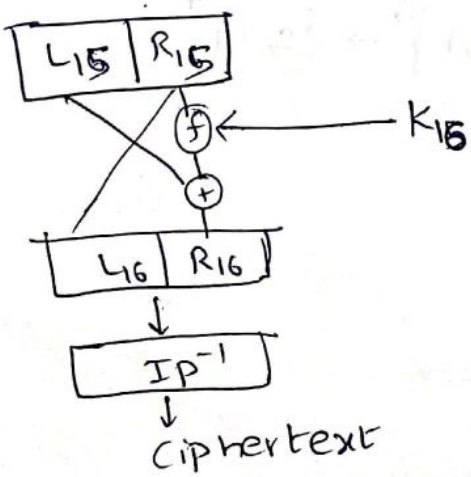




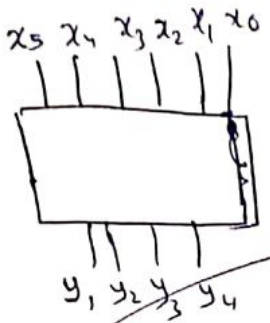








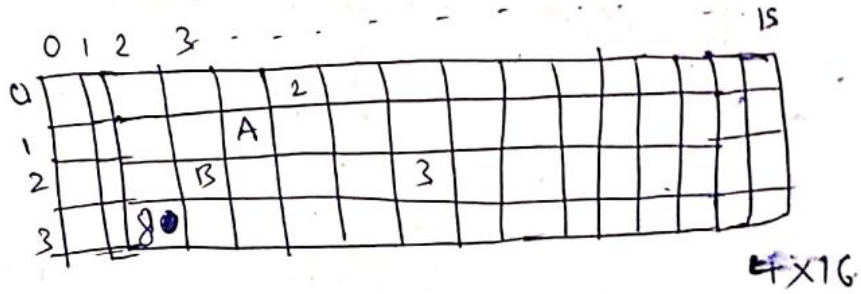
→ DES - S boxes :-



→ $x_0 x_5$ → Row number in the below matrix

→ $x_1 x_2 x_3 x_4$ → column number

each entry is of 4-bits



we go to that element which is 4-bits which is the output

Eg $x_5 x_4 x_3 x_2 x_1 x_0 = 101001$

$\Rightarrow$ row = 11 = 3

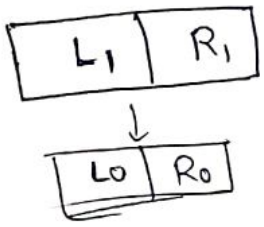
column = 0010 = 2

$\Rightarrow M[3][2] = 8$

$= 1000$

$\Rightarrow y_1 y_2 y_3 y_4 = 1000$

* Decryption of DES :- we have $L_1 = R_0$, $R_1 = L_0 \oplus f(R_0, K_1)$



$R_0 = L_1$

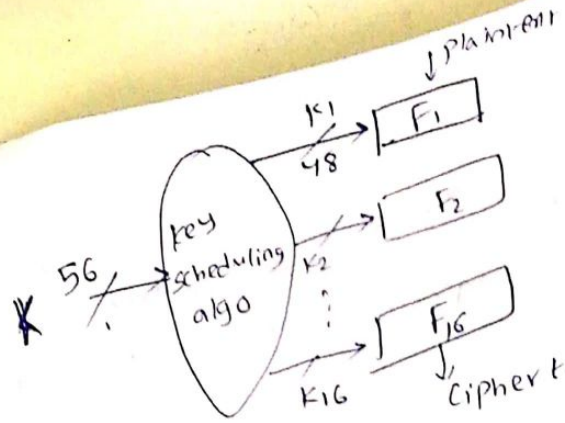
$\Rightarrow R_1 = L_0 \oplus f(R_0, K_1)$

$R_1 \oplus f(R_0, K_1) = L_0$

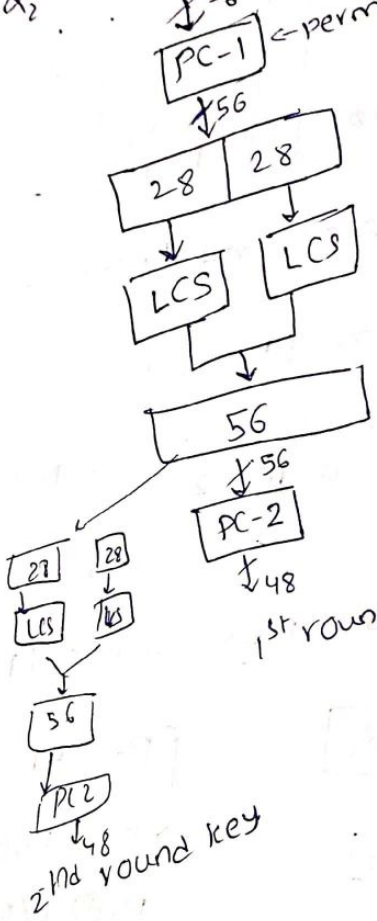
$R_1 \oplus f(L_1, K_1) = L_0$

$\therefore L_0 = R_1 \oplus f(L_1, K_1)$

* Key scheduling algorithm :-

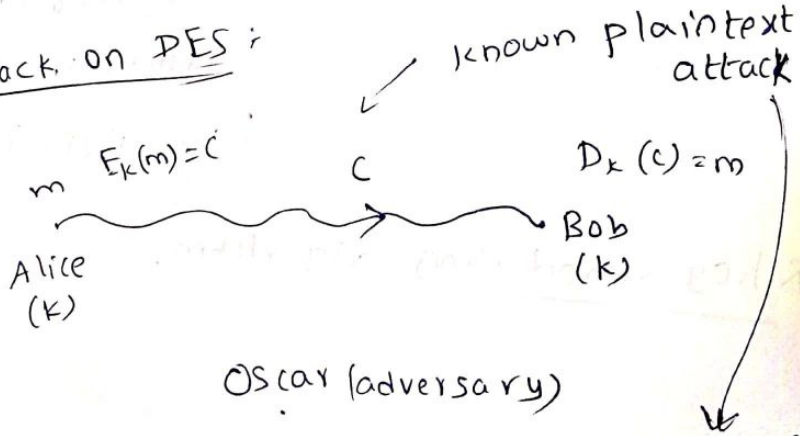


$K = \alpha_1 \alpha_2 \ldots \alpha_7 \alpha_9 \ldots \alpha_{15} \alpha_{17} \ldots \alpha_{64}$ (56 bits)



LCS → Left circular shift

* attack on DES :



(Brute force) Search all over the key space

Oscar knows some ← Plaintext & corresponding Ciphertext

∴ Worst case Time taken = 2^{56} × (DES encryption time)

$= 2^{56}$ sec

1 day = 24 × 60 × 60 s $\approx 2^5 \times 2^6 \times 2^6 = 2^{17}$ s

1 year = $365 \times 2^{17} \approx 2^9 \times 2^{17} = 2^{26}$ s.

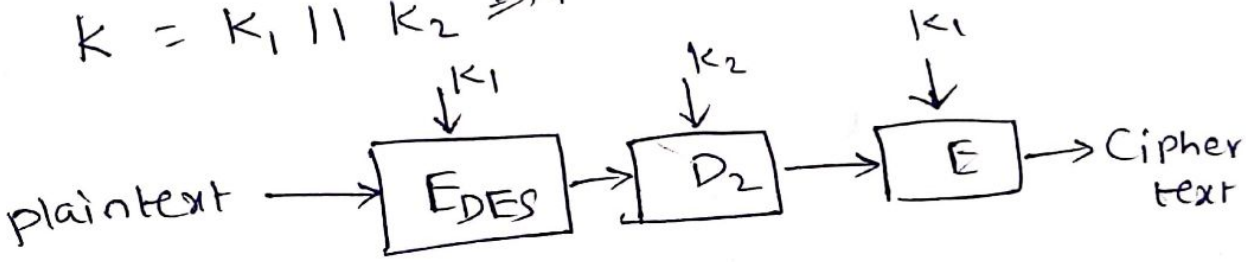
* But If we have 36 processors

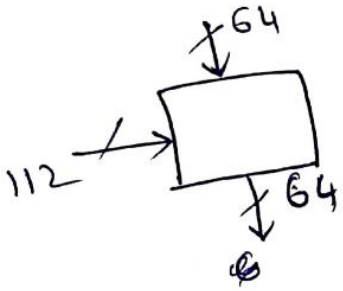
$$\text{time} = \frac{2^{56}}{2^{36}} = 2^{20} = 8 \text{ days}$$

*generic attack → Exhaustive search.

* Triple DES

$K = K_1 \,||\, K_2$ = K_1 concatenate with K_2





∴ Worst case Time taken = 2^{56} × (DES encryption time)

$= 2^{56}$ sec

1 day = $24 \times 60 \times 60$ s $\approx 2^5 \times 2^6 \times 2^6 = 2^{17}$ s

1 year = $365 \times 2^{17} \approx 2^9 \times 2^{17} = 2^{26}$ s.

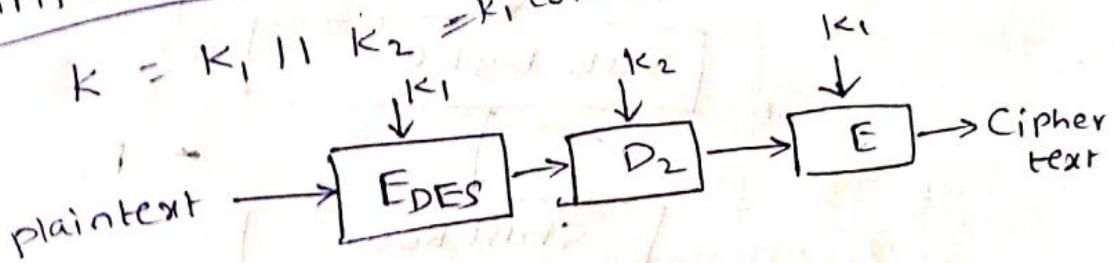
* But If we have 36 processors

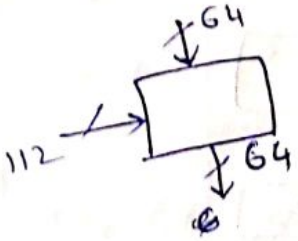
time = $\frac{2^{56}}{2^{36}} = 2^{20}$ = 8 days

*generic attack → Exhaustive search.

* Triple DES

$K = K_1 \,||\, K_2$ = K_1 concatenate with K_2



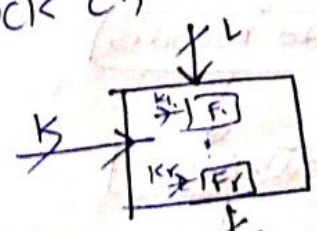


* AES

→ Name is Rijndael

↙ developed by Rijnman, Daeman

Block cipher



→ L = 128 bits

AES-128 ← K = 128 bits, r = 10

AES-192 ← (or) K = 192, r = 12

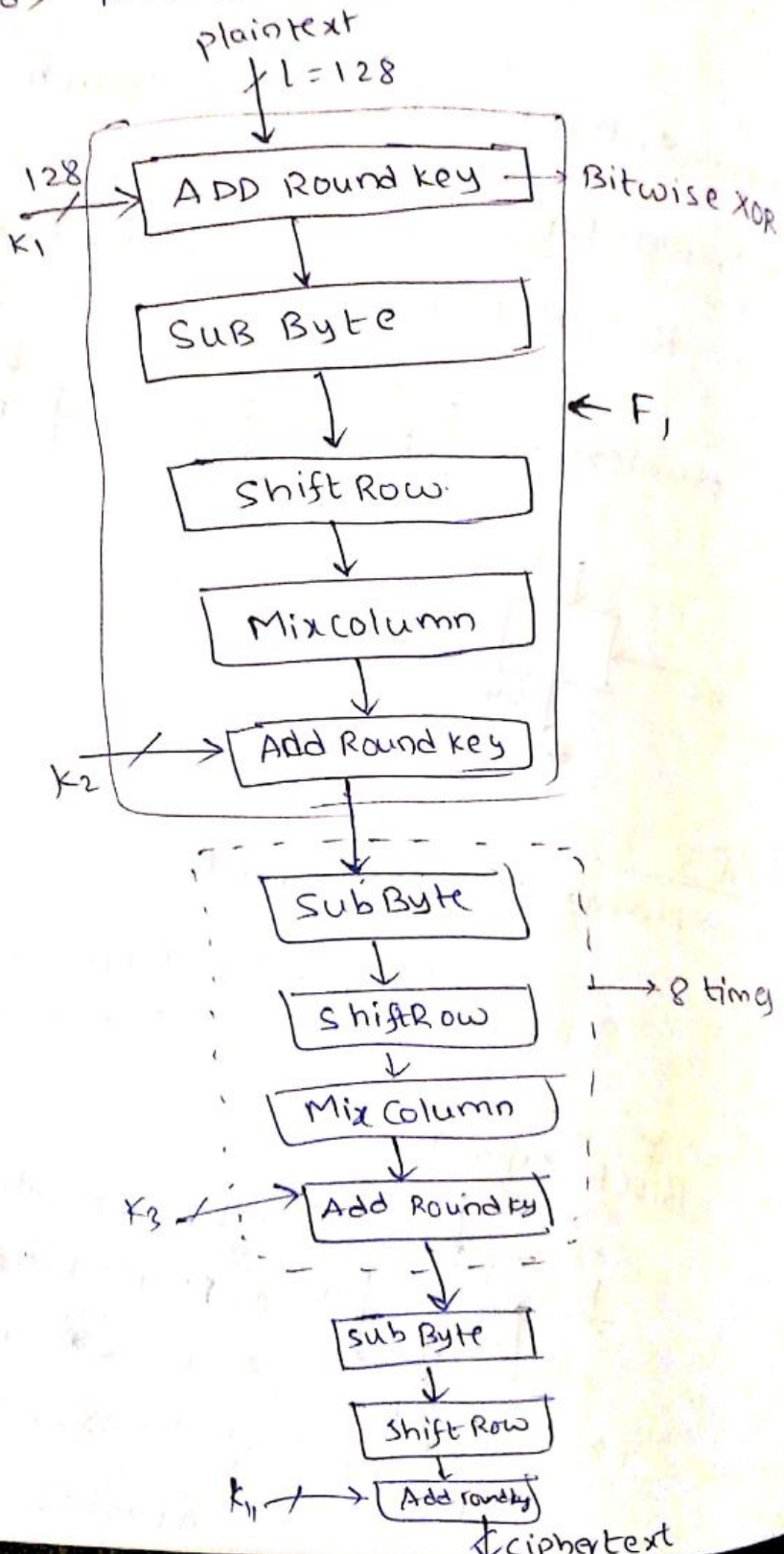
(or) K = 256, r = 14 → AES-256

#rounds

* AES - rounds are based on some funcn
  - → SubByte
  - → Shift Row
  - → Mix Column
  - → Add Round key

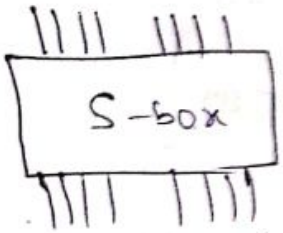
* AES-128

l=128, k=128, r=10



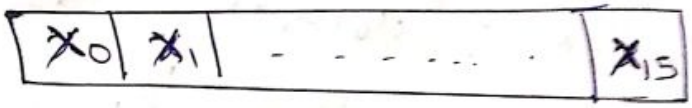
* Sub Byte

≡ S-box.



$\Pi_S : \{0,1\}^8 \rightarrow \{0,1\}^8$

(Π_S ↙ S-box func^n)



→ 128 bit plaintext

$$\begin{pmatrix} s_{00} & s_{01} & s_{02} & s_{03} \\ s_{10} & s_{11} & s_{12} & s_{13} \\ s_{20} & s_{21} & s_{22} & s_{23} \\ s_{30} & s_{31} & s_{32} & s_{33} \end{pmatrix}_{4\times4}$$

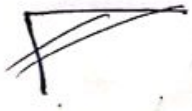
s_{ij} → 8 bit number = 1 byte

~~State~~ ↑ State

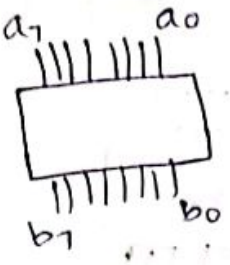
State is initialised to $\begin{pmatrix} x_0 & x_4 & x_8 & x_{12} \\ x_1 & x_5 & x_9 & x_{13} \\ x_2 & x_6 & x_{10} & x_{14} \\ x_3 & x_7 & x_{11} & x_{15} \end{pmatrix}$

it is changed to $\left(\Pi_S(s_{ij})\right)_{4\times4}$

~~S-box~~



S-box,



$$Z_2[x] = \{a_0 + a_1 x + \cdots + a_n x^n \mid n \geq 0,\ a_i \in \{0,1\}\}$$

$$P(x) = x^8 + x^4 + x^3 + x + 1$$

$$Z_2[x]/P(x) = \{a_0 + a_1 x + \cdots + a_7 x^7 \mid a_i \in \{0,1\}\}$$

$Z_2[x]$ → modulo; 2^8 no. of polynomials

Field $\langle +, \cdot \rangle$ mod $P(x)$ (mod $P(x)$)

$\therefore Z_2[x]/P(x) \equiv F_{2^8}$

S-box$(a_7 a_6 \cdots a_0)$

1. $A(x) \equiv a_0 + a_1 x + \cdots + a_7 x^7 \in F_{2^8}$
2. Let $B(x) = (A(x))^{-1}$ under mod $P(x)$ [exists since it's Field]

$$= b'_0 + b'_1 x + b'_2 x^2 + \cdots + b'_7 x^7$$

3. $$\begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_7 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ & & & \vdots & & & & \end{pmatrix} \begin{pmatrix} b'_0 \\ b'_1 \\ \vdots \\ b'_7 \end{pmatrix} \oplus \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_7 \end{pmatrix}$$

for $i \leftarrow 0$ to 7

$$b_i = b'_i + b'_{i+4} + b'_{i+5} + b'_{i+6} + b'_{i+7} + c_i$$

$$(c_7 c_6 \cdots c_0) = (01100011)$$

$$\therefore b_0 = b'_0 + b'_4 + b'_5 + b'_6 + b'_7 + c_0$$

$$b_5 = b'_5 + b'_1 + b'_2 + b'_3 + b'_4 + c_5$$

* Shift Row

assign symbol

$$\begin{pmatrix} s_{00} & s_{01} & s_{02} & s_{03} \\ s_{10} & s_{11} & s_{12} & s_{13} \\ s_{20} & s_{21} & s_{22} & s_{23} \\ s_{30} & s_{31} & s_{32} & s_{33} \end{pmatrix} \leftarrow \begin{pmatrix} s_{00} & s_{01} & s_{02} & s_{03} \\ s_{11} & s_{12} & s_{13} & s_{10} \\ s_{22} & s_{23} & s_{20} & s_{21} \\ s_{33} & s_{30} & s_{31} & s_{32} \end{pmatrix}$$

* Mix Column

$$\begin{pmatrix} s_{00} & s_{01} & s_{02} & s_{03} \\ s_{10} & s_{11} & s_{12} & s_{13} \\ s_{20} & s_{21} & s_{22} & s_{23} \\ s_{30} & s_{31} & s_{32} & s_{33} \end{pmatrix}$$

replace column 'c' $\begin{pmatrix} s_{0c} \\ s_{1c} \\ s_{2c} \\ s_{3c} \end{pmatrix}$ by $\begin{pmatrix} s'_{0c} \\ s'_{1c} \\ s'_{2c} \\ s'_{3c} \end{pmatrix}$

$c = 0$ to 3

$$s'_{0c} = x \cdot s_{0c} \oplus (x+1) s_{1c} \oplus s_{2c} \oplus s_{3c}$$

modulo $p(x)$

$$s'_{1c} = s_{0c} \oplus x \cdot s_{1c} \oplus (x+1) \cdot s_{2c} \oplus s_{3c}$$

$$s'_{2c} = s_{0c} \oplus s_{1c} \oplus x \cdot s_{2c} \oplus (x+1) s_{3c}$$

$$s'_{3c} = (x+1) s_{0c} \oplus s_{1c} \oplus s_{2c} \oplus x \cdot s_{3c}$$

* Modes of operation :-

ECB → Electronic Code Book Mode
CBC → Cipher Block Chaining Mode
OFB → Output Feed Back Mode
CFB → Cipher Feed Back Mode.

* ECB (naive use of block cipher)

$x_1 \; x_2 \; \ldots\ldots$ plaintext blocks
$\downarrow \; \downarrow$
$y_1 \; y_2 \; \ldots\ldots$ ciphertext Blocks

$y_i = E_K(x_i)$

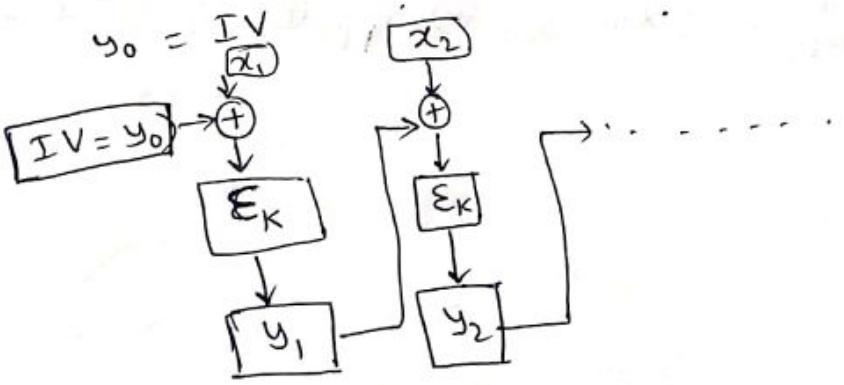
Weakness: Identical plaintext blocks yield identical ciphertext blocks.

⇒ plaintext blocks are chosen from a 'low entropy' plaintext space, this mode is useless.

* CBC

$y_i = E_K((x_i \oplus y_{i-1}), \quad i \geq 1$

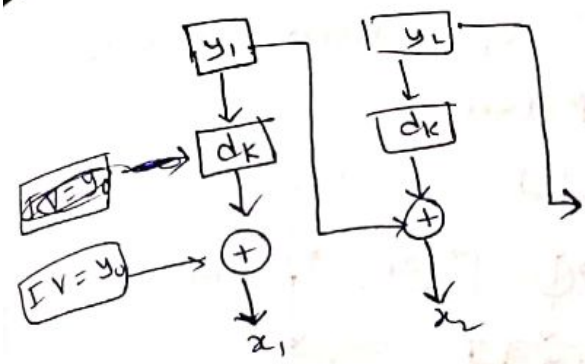
$y_0 = IV$



Decryption.

$d_K(y_i) = x_i \oplus y_{i-1}$

$x_i = d_K(y_i) \oplus y_{i-1}$



~~*Useful~~

→ Useful for authentication (data integrity)

↳ to produce Message Authentication Code (MAC).

If x_i is changed in CBC mode, then y_i and subsequent ciphertext blocks will be affected.

*OFB: (operates as a synchronous stream cipher)

→ key stream is generated by repeatedly encrypting an initial vector IV.

$$K_0 = IV$$

→ key = K

→ keystream $K_i = E_K(K_{i-1}), \; i \geq 1$

$i = 1, 2, 3, \ldots$

Blocks

plaintext → $x_1 \; x_2 \; x_3 \ldots$

ciphertext → $y_1 \; y_2 \; y_3 \ldots$

$$y_i = x_i \oplus K_i$$

* CFB (operates as an asynchronous stream cipher)

$$y_0 = IV, \; K_i = E_K(y_{i-1})$$

∴ keystream is produced by encrypting the previous ciphertext block.

key - K

keystream - $K_1 \; K_2 \; K_3 \ldots$

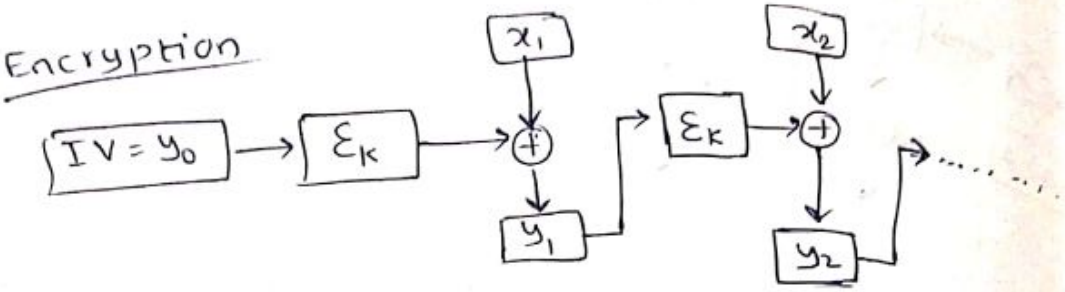
plaintext - $x_1 \; x_2 \; x_3 \ldots$

ciphertext - $y_1 \; y_2 \; y_3 \ldots$

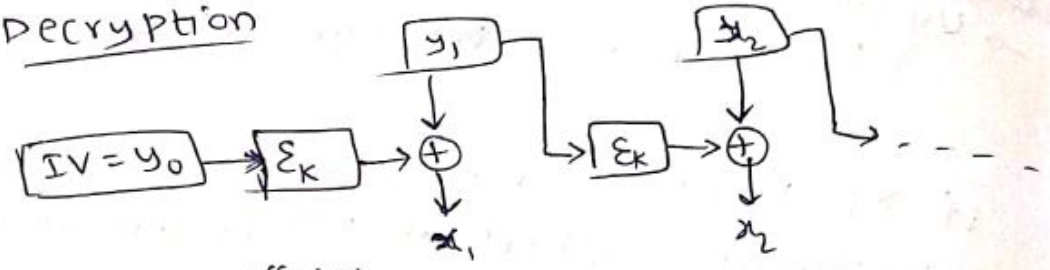
$$y_i = x_i \oplus K_i$$

→ The encryption func^n $\mathcal{E}_K$ is used for both encryption & decryption.

Encryption



Decryption



* Counter Mode (similar to OFB Mode) :- (very efficient)

→ keystream generation is different

→ Construct a seq. of bit strings of length 'm' each. (block size.)

$T_1, T_2, \ldots$

using a counter ctr,

$$T_i = (ctr - i + 1) \bmod 2^m; \quad i \geq 1$$

$$K_i = \mathcal{E}(T_i)$$

Plaintext → $x_1\ x_2 \ldots$

Ciphertext → $y_1\ y_2 \ldots$

$$y_i = x_i \oplus \mathcal{E}_k(T_i)$$

* Key distribution

Alice (K) — Bob (K) → How do they agree on the same key.

* Diffie - Hellman key Agreement

$G = \langle g \rangle$, DLP is hard in G.

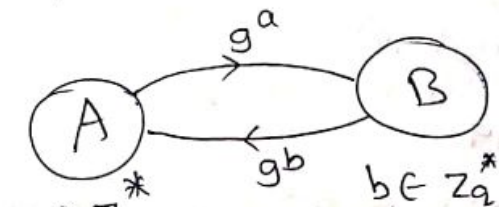
multiplicative group

Discrete Logarithm of p.

$|G| = q$

(Given $\langle g, \beta = g^a \rangle$

$a \rightarrow$ Discrete Logarithm (DL) of β with base g)



$a \in Z_q^*$ (secret) ↑ Random ⇓ $(g^b)^a$ = key → g^{ab}

$b \in Z_q^*$ (secret) ↑ Random ⇓ $(g^a)^b$ = key → g^{ab}

$Z_q^* = \{ a \in Z \mid gcd(a, q) = 1, a < q \}$

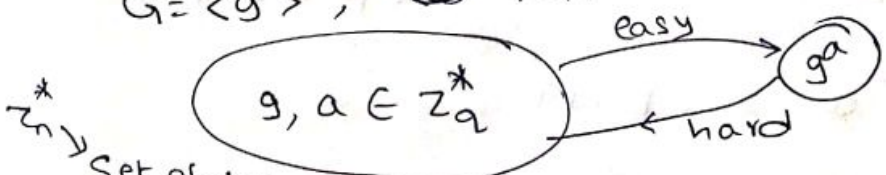
* Public Key Cryptosystem / Asymmetric key Cryptosystem :

→ Encryption schemes
→ Digital signature Schemes
→ Key agreement → Diffie-Hellman.

* Provably secure schemes :

→ Factorization
→ Discrete log problem (DLP)

$G = \langle g \rangle$, $|G| = q$



Z_n^* → Set of integers < n which are coprime to n

they have multiplicative inverse

→ DLP is believed to be hard

→ $Z_n^* = \{a \in Z \mid \gcd(a, n) = 1, a < n\}$

Ex: Compute $2^{1952} \bmod 19$.

Fast modular exponentiation :-

$2^2 \equiv 4 \pmod{19}$

$\Rightarrow 2^4 \equiv 16 \pmod{19}$

$\Rightarrow 2^8 \equiv 16^2 \equiv 9 \pmod{19}$

$2^{16} \equiv 81 \pmod{19}$

$2^{16} \equiv 5 \pmod{19} \Rightarrow 2^{32} \equiv 6 \pmod{19}$

$2^{64} \equiv 17 \pmod{19}$

$2^{128} \equiv 4 \pmod{19}$

$2^{256} \equiv 16 \pmod{19}$

$2^{512} \equiv 9 \pmod{9}$

$2^{1024} \equiv 5 \pmod{9}$

$1452 = [\overset{10}{1}\overset{9}{0}\overset{8}{1}\overset{7}{1}\overset{6}{0}\overset{5}{1}\overset{4}{0}\overset{3}{1}\overset{2}{1}\overset{1}{0}\overset{0}{0}]_2$

$\Rightarrow 1452 = 2^{10} + 2^8 + 2^7 + 2^5 + 2^3 + 2^2$

$2^{1452} = 2^{1024} * 2^{256} \times 2^{128} \times 2^{32} \times 2^8 \times 2^4$

$\therefore 2^{1452} \bmod 19 = (5 \times 16 \times 4 \times 6 \times 9 \times 16) \bmod 19$

$= 11 \bmod 19$

Alternatively : Use Fermat's Little Theorem

$a^{P-1} \equiv 1 \pmod{P}$ if $\gcd(a, P) = 1$ & P is a prime

Here $a = 2$, $P = 19$

$\Rightarrow 2^{19-1} \equiv 1 \pmod{19}$

$2^{18} \equiv 1 \pmod{19}$

$1452 = 18 \times 80 + 12$

$2^{1452} \equiv 2^{18\times 80+12} = 2^{12} \times (2^{18})^{80} \pmod{19}$

$\therefore 2^{1452} \equiv 2^{12} \pmod{19}$

$\equiv 2^8 \times 2^4 \pmod{19}$

$\equiv 9 \times 16 \pmod{19} = 11 \bmod 19$

Compute $18^{802} \pmod{29}$.

Alternatively:- Euler's theorem

$a^{\phi(n)} \equiv 1 \pmod{n}$ $\gcd(a, n) = 1$

$\phi(n)$ = Euler's phi function/totient function

No. of integers less than 'n' coprime to 'n'.

When 'n' is prime, $\phi(n) = n-1$

$\gcd(18, 29) = 1$

$\therefore 18^{28} \equiv 1 \pmod{29}$

$|\mathbb{Z}_n^*|$

Find the last three digits of 13^{2017}.

Question:

1. Existence of primitive roots/generator of $\mathbb{Z}_n^*$.
2. Determine primitive roots if exists.
3. Computing orders $\rightarrow ord_n(a)$, $a \in \mathbb{Z}_n^*$
4. The DLP

Defn:- Let $\alpha \in \mathbb{Z}_n^*$. If $ord_n(\alpha) = \phi(n)$, then 'α' is said to be a generator or primitive element of $\mathbb{Z}_n^*$

[$ord_n(a) = k \Leftrightarrow k$ is the least +ve integer s.t. $a^k \equiv 1 \bmod(n)$]

Fact:
(i) Z_n^* has a primitive element iff $n = 2, 4, p^k$ or $2p^k$ when p is an odd prime, $k \geq 1, k \in Z$

Ex: 1. $n = 20$, primitive root mod n exists?

$20 = 2 \times 2 \times 5 \Rightarrow$ Not of the above forms
$\Downarrow$
primitive root doesn't exist

2. $n = 1250$

$1250 = 2 \times 5^4 \Rightarrow$ primitive root exists

3. $n = 59$, prime $\Rightarrow$ " " "

Fact (ii):- If α is a generator of Z_n^*, then $b = \alpha^i \bmod n$ is also a generator of Z_n^* iff $\gcd(i, \phi(n)) = 1$

Order of power formula

$$\text{ord}_n(\alpha^i) = \frac{\text{ord}_n(\alpha)}{\gcd(i, \phi(n))}$$

(iii) # primitive roots mod n is $\phi(\phi(n))$.

Ex Z_{25}^* is cyclic $\Rightarrow$ primitive root exists
$\because 25 = 5^2$

suppose $\alpha = 2$ is a generator.

#generators = $\phi(\phi(25))$.

$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$

$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)$

$25 = 5^2 \Rightarrow \phi(25) = 25\left(1 - \frac{1}{5}\right) = 20$

$20 = 2^2 \times 5^1$ $\quad \phi(20) = 20\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 20 \times \frac{1}{2} \times \frac{4}{5} = 8$

other generators will be

$2^i \bmod 25$ with $\gcd(i, \phi(25)) = 1$

$\cup$

$\gcd(i, 20) = 1$

$\Rightarrow$ Ans: $\{2, 8, 3, 12, 23, 17, 22, 13\}$

* Determination of primitive roots:-

Finding primitive roots (when they exist)

$\longrightarrow$ (convert to) Determining primitive roots modulo a prime.

* Fact:-

(i) If 'g' is a primitive root modulo an odd prime power p^k, then g or $g + p^k$ (or both) will be a primitive root mod $2p^k$.

(ii) If 'g' is a primitive root mod an odd prime 'p', then g or $g+p$ (whichever is odd) will be a primitive root mod p^2.

(iii) If 'p' is an odd prime & g is a primitive root mod p^2, then g will be a primitive root mod p^k.

* Modular orders of invertible modular integers:-

Defn: For integer $1 \le a < n$, with $\gcd(a, n) = 1$, we define order of 'a' relative to 'n' (or order of a mod n) denoted by $\text{ord}_n(a)$, to be the least +ve integer 'k' for which

$$a^k \equiv 1 \pmod{n}$$

Note:- $\text{ord}_n(a) \le \phi(n)$ by Euler's theorem

*Euler's theorem

If $\gcd(a,n)=1$ then $a^{\phi(n)} \equiv 1 \pmod{n}$

Ex:

$a^k \pmod 8$

	$k=1$	$k=2$	$k=3$	$k=4$	
$a=1$	1	1	1	1	
$a=3$	3	1	3	1	$\Rightarrow ord_8(3)=2$
$a=5$	5	1	5	1	
$a=7$	7	1	7	1	

*Fact: Suppose $a, n > 1$, $\gcd(a,n)=1$

(a) If 'k' is any +ve integer with $a^k \equiv 1 \pmod n$ then $ord_n(a) \mid k$

(b) $ord_n(a) \mid \phi(n)$ (divides)

(c) i, j are non-negative integers with $a^i \equiv a^j \pmod n$ iff $i \equiv j \pmod{ord_n(a)}$

Proof:

(a) let $k = ord_n(a) \cdot q + r \quad 0 \le r < ord_n(a)$.

$$a^k \equiv 1 \pmod n$$

$$\Rightarrow \left(a^{ord_n(a)}\right)^q \cdot a^r \equiv 1 \pmod n$$

$$a^r \equiv 1 \pmod n$$

$\therefore r = 0$ since $ord_n(a) > r$.

Ex: If possible, do each of the following.

(a) Compute $ord_{59}(7)$.

(b) Find an integer between 1 and 59 whose modulo 59 order is 22.

(c) Find a primitive root of 59.

(d) Find an exponent 'j' s.t. $g^j \equiv 7 \pmod{59}$ where g → primitive root of that was found in part (c).

Sol: (a) $ord_{59}(7) \mid \phi(59) = 58$

$\Rightarrow ord_{59}(7) \mid 58$

$\Rightarrow ord_{59}(7) \mid 2 \times 29$

$\therefore ord_{59}(7) = 2$ or 29 or 58

$7^2 \bmod 59 = 49$

$7^{29} \bmod 59 = 1 \Rightarrow ord_{59}(7) = 29$

(b) whether $\exists a$, $1 < a < 59$ → no

s.t $ord_{59}(a) = 22$

(c) $2^2 \equiv 4 \pmod{59}$

$2^{29} \equiv 58 \pmod{59}$

$2^{58} \equiv 1 \pmod{59}$

} → 2 is a primitive element

(d) $2^j \equiv 7 \pmod{59}$

$$ord_{59}(2^j) = \frac{ord_{59}(2)}{gcd(j, \phi(59))}$$

order of power formula.

We have $ord_{59}(2^j) = ord_{59}(7) = 29$

$$\therefore 29 = \frac{58^2}{\gcd(j, \phi(59))}$$

$\therefore \gcd(j, 58) = 2$

$\Rightarrow$ j must be even.

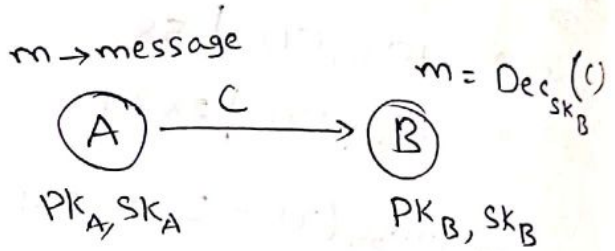
We have to check for all possible values of j.

- Here, $\boxed{j = 18}$

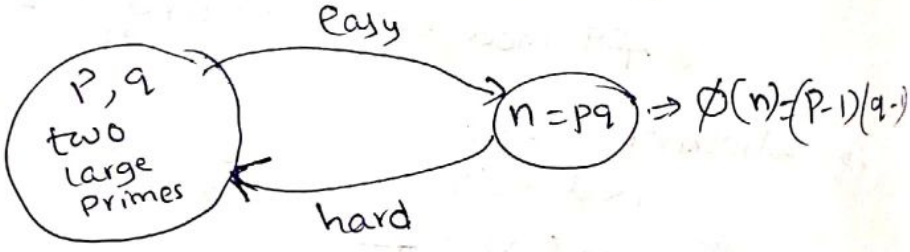
* RSA cryptosystem :-

→ Rivest, Shamir, Adleman.

PK : public key
SK : secret key



$c = Enc_{PK_B}(m)$



Hardness of factorization

Key Gen.	Encryption	Decryption
→ P, q Large primes → n = pq → choose e, $1 < e < \phi(n)$ s.t $\gcd(e, \phi(n)) = 1$ → $ed \equiv 1 \pmod{\phi(n)}$ $\Downarrow$ $ed = k\phi(n) + 1$ k is an integer	$x \in Z_n^*$ $Enc_{Pk}(x) = x^e \bmod n$	$Dec_{Sk}(y) = y^d \bmod n$ $y^d = (x^e)^d = x^{ed}$ $= x^{1 + k\phi(n)}$ $= x(x^{\phi(n)})^k$ $\therefore y^d \bmod n$ $= x \bmod n$

$PK = (n, e)$, $SK = (p, q, d)$

(n, e) are public.

⇒ If we can easily factorize n into $p \times q$, p, q are primes,

$$\phi(n) = (p-1) \times (q-1)$$

$$\Rightarrow \phi(n) = pq - p - q + 1$$

$$\phi(n) = n - p - q + 1$$

$$p + q = n - \phi(n) + 1$$

* Elgamal encrption scheme is Z_p^*, p is prime

security ⇔ the difficulty of the DLP over Z_p^*

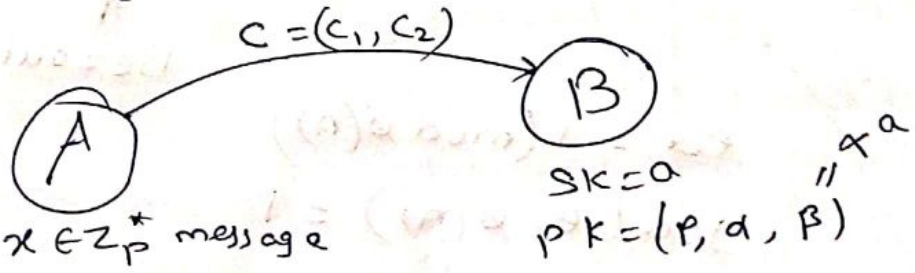
Given p, α, β where $\beta = \alpha^a \bmod p$.

$Z_p^* = \langle \alpha \rangle$.

to find $a \in Z$, $0 \le a \le p-2$

Key Gen.:- ϕ, α generating Z_p^*, $\beta = \alpha^a \bmod p$.

$PK = (p, \alpha, \beta)$, $SK = a$.



Encryption:-

$$Enc_{PK}(x) = (\alpha^k \bmod p,\ \beta^k \cdot x \bmod p)$$

where k is chosen randomly from Z_{p-1}.

$$= (c_1, c_2)$$

Decryption: $c = (c_1, c_2)$

$$Dec_{SK}(c) = c_2 / c_1^a$$

$$= \frac{\beta^k \cdot x}{(\alpha^k)^a} = \frac{\alpha^{ak} \cdot x}{\alpha^{ka}} = x \bmod p.$$

* Euclidean Algorithm:-

Input: a, b two non-negative integers, $a \geq b$.

output: $\gcd(a, b)$

$a \; b) a \; (q$

$r) b \; ($

⋮

* Extended Euclidean algorithm:-

Input: a, b $a \geq b$ non-negative integers

output: $\gcd(a,b)$, x, y integers s.t

$$ax + by = \gcd(a,b).$$

↑ Bezoul's identity.

$$ed \equiv 1 \pmod{\phi(n)}$$

$$\gcd(e, \phi(n)) = 1$$

$$xe + y\phi(n) = 1$$

$$\Rightarrow 1 \equiv xe \pmod{\phi(n)}$$

$$\therefore \boxed{x = d}$$

steps:

1. set $V = [a, 1, 0]$, $V = [b, 0, 1]$

(initialize record keeping vectors)

2. While $(v[1] > 0)$

$$w = u - \left\lfloor \frac{u[1]}{v[1]} \right\rfloor v$$

update: $u = v$

update: $v = w$

end(while).

3. output $gcd = u[1]$, $x = u[2]$, $y = u[3]$.

→ we have $u[1] = a \cdot u[2] + b \cdot u[3]$ ↑ $O((\log n)^2)$

* Ex: (a) compute $d = gcd(148, 75)$ & integers x, y such that $d = 148x + 75y$.

(b) If exists, compute $75^{-1} \bmod 148$.

&

$Q = \left\lfloor \frac{u[1]}{v[1]} \right\rfloor$	$u[1]$	$u[2]$	$u[3]$	$v[1]$	$v[2]$	$v[3]$
	148	1	0	75	0	1
1	75	0	1	73	1	-1
1	73	1	-1	2	-1	2
36	2	-1	2	1	37	-73
2	1	37	-73	0	-75	-148
	= gcd	= x	= y			

$\therefore d = 1 = 148 \times 37 + 75 \times (-73)$

$1 = (75 \times (-73)) \bmod 148$

$\therefore 75^{-1} = -73 = 148 - 73$

$= 75$

$1 = 148 \times (37 + 75) + 75 \times (-73 - 148)$

x & y are not unique

* Miller-Robin Primality Test:

~~Properties~~

Proposition: Suppose p is an odd prime & $1 < a < p-1$.

Let $p-1 = 2^f \cdot m$, m an odd integer,

Then, either $a^m \equiv 1 \pmod p$

(or) $a^{2^j m} \equiv -1 \pmod p$

for some j, $0 \le j < f$

Proof: $a^{p-1} \equiv 1 \pmod p$ [Fermat's Little theorem]

$$(a^{p-1} - 1) \equiv 0 \pmod p$$

$$\left(a^{(p-1)/2} - 1\right)\left(a^{(p-1)/2} + 1\right) \equiv 0 \pmod p$$

$\Rightarrow p \mid a^{\frac{p-1}{2}} - 1$ (or) $p \mid a^{\frac{p-1}{2}} + 1$

$\Rightarrow a^{\frac{p-1}{2}} \equiv \pm 1 \pmod p$

i.e. $a^{2^{f-1} \cdot m} \equiv \pm 1 \pmod p$

Case 1: $a^{2^{f-1} m} \equiv -1 \pmod p \Rightarrow$ Done

~~Case 2~~

Case 2: $a^{2^{f-1} m} \equiv 1 \pmod p \rightarrow$ factor it

$$a^{2^{f-1} \cdot m} - 1 \equiv 0 \pmod p$$

$$\Rightarrow \left(a^{2^{f-2} \cdot m} - 1\right)\left(a^{2^{f-2} \cdot m} + 1\right) \equiv 0 \pmod p$$

$\Rightarrow a^{2^{f-2} \cdot m} \equiv \pm 1 \pmod{p}$

$-1 \Rightarrow$ done, $j = f-2$

$+1 \Rightarrow$ again take square root

can go upto 2 power vanishes.,

$a^m \equiv \pm 1 \pmod{p}$

Let 'n' be an odd integer with $n-1 = 2^f \cdot m$ m is an odd integer. Suppose we can find 'a' with $1 < a < n-1$ s.t.

$a^m \not\equiv 1 \pmod{n}$. and $a^{2^j \cdot m} \not\equiv -1 \pmod{n}$

$\forall j,\ 0 \le j < f$

then, 'n' is composite..

*Algorithm:

Input: n, k ← # iterations

$n-1 = 2^f \cdot m$, m is odd

(*) choose a, $1 < a < n-1$ ← $O((\log n)^3)$

$b \equiv a^m \pmod{n}$

if $b \equiv 1 \pmod{n}$, then

count ++

if count = k, return "n is probably prime"

else goto (*)

for j = 0 to f-1 do

if $b \equiv -1 \pmod{n}$

count ++

if count = k return "n is probably prime"

else

$b \equiv b^2 \pmod{n}$

end do

return "n is composite with witness a".

* Error probability $< \left(\frac{1}{4}\right)^k$
* Solloray-Strassen Primality Test:
* Euler's Criterion

If 'p' is odd prime, then

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \pmod p$$

↗ legendre symbol of a mod p

Legendre's symbol modulo an odd prime 'p'

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{if } a \text{ is square modulo } p \\ -1 & \text{if } a \text{ is not a square mod } p. \\ 0 & \text{if } p \mid a. \end{cases}$$

holds for any odd integer 'n'

Defn (Square mod p / Quadratic residue mod p):

$Z_p^* = \{1, 2, \ldots, p-1\}$ p → odd prime

$a \in Z_p^*$ is a sq. mod p / QR mod p) if $\exists\ x \in Z_p^*$ s.t. $a \equiv x^2 \pmod p$

Ex) $p = 7$ $Z_7^* = \{1, 2, 3, 4, 5, 6\}$

$1^2 \equiv 1 \pmod 7$
$2^2 \equiv 4 \pmod 7$
$3^2 \equiv 2 \pmod 7$
$4^2 \equiv 2 \pmod 7$
$5^2 \equiv 4 \pmod 7$
$6^2 \equiv 1 \pmod 7$

$QR_7 = \{1, 2, 4\}$

* Error probability $< \left(\frac{1}{4}\right)^k$

* Solloray-Strassen Primality Test:-

Euler's Criterion

If 'p' is odd prime, then

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \pmod p$$

↑ legendre symbol of a mod p

Legendre's symbol modulo an odd prime 'p'

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{if } a \text{ is square modulo } p \\ -1 & \text{if } a \text{ is not a square mod } p. \\ 0 & \text{if } p|a. \end{cases}$$

holds for any odd integer 'n'

Defn (Square mod p / Quadratic residue mod p):-

$Z_p^* = \{1, 2, \ldots, p-1\}$ p → odd prime

$a \in Z_p^*$ is a sq. mod p / QR mod p) if $\exists\ x \in Z_p^*$ s.t. $a \equiv x^2 \pmod p$

Ex: $p = 7$ $Z_7^* = \{1, 2, 3, 4, 5, 6\}$

$1^2 \equiv 1 \pmod 7$
$2^2 \equiv 4 \pmod 7$
$3^2 \equiv 2 \pmod 7$
$4^2 \equiv 2 \pmod 7$
$5^2 \equiv 4 \pmod 7$
$6^2 \equiv 1 \pmod 7$

$QR_7 = \{1, 2, 4\}$

$QNR_7 = \{3, 5, 6\}$

Quadratic Not Residue.

* Jacobi Symbol modulo n

$$\left(\frac{a}{n}\right) = \begin{cases} 1 & \text{if } a \in QR_n \\ -1 & \text{if } a \notin QR_n \\ 0 & \text{if } n|a \end{cases}$$

n is composite

* when 'n' is composite, $\left(\frac{a}{n}\right)$ is Jacobi symbol & when 'n' is prime, $\left(\frac{a}{n}\right)$ is Legendre symbol.

* To calculate Jacobi symbol:-

$n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \left(\frac{a}{p_2}\right)^{e_2} \ldots \left(\frac{a}{p_k}\right)^{e_k}$$

→ contrative statement

→ If n is an odd integer, $1 \le a \le n-1$, if $\left(\frac{a}{n}\right) \not\equiv a^{\frac{n-1}{2}} \pmod n$, then n is composite & a is the witness of the compositeness. → $O((\log n)^3)$

→ error probability does not vary significantly if k is increased.

* Quadratic Residues & Quadratic reciprocity law:-

→ p → odd prime

Theorem:- Every residue system mod p contains exactly $\frac{p-1}{2}$ quadratic residues and $\frac{p-1}{2}$ quadratic not residues mod p.

Proof: $1^2, 2^2, 3^2, \ldots \left(\frac{p-1}{2}\right)^2 \bmod p$

Claim: distinct

if not, then $x^2 \equiv y^2 \pmod p$.

$\Rightarrow p \mid (x+y)(x-y)$

$1 \le x, y \le \frac{p-1}{2}$, $x \neq y$

$\therefore x+y < p$

$\Rightarrow p \mid x-y$

$x \equiv y \pmod p$

which is contradiction.

$\therefore$ they are all distinct

Also, $(p-k)^2 \equiv k^2 \pmod p$

Legendre's Symbol $p \to$ odd prime

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a \\ 1 & \text{if } a \in QR_p \\ -1 & \text{if } a \in QNR_p \end{cases}$$

QR_p ← Quadratic residue mod p

QNR_p ↑ Quadratic not residue mod p

* **Euler's Criterion:** $p \to$ odd prime

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$$

Proof:

Case (1): $p \mid a$ → trivial

Case (2): $a \in QR_p \Rightarrow \left(\frac{a}{p}\right) = 1$

$\exists\, x \in Z_p^*$ s.t $a \equiv x^2 \pmod p$

By Fermat's Little Theorem (FLT),

$x^{p-1} \equiv 1 \pmod p$ $\quad [\because x \in Z_p^*, \gcd(x,p) = 1]$

$\therefore a^{\frac{p-1}{2}} \equiv 1 \pmod p$

$\therefore 1 \equiv a^{\frac{p-1}{2}} \pmod p$

$\left(\frac{a}{p}\right) \equiv a^{p-1/2} \pmod p$

case (3): $a \in QNR_p \Rightarrow \left(\frac{a}{p}\right) = -1$

~~let $f(x) = (x^{\frac{p-1}{2}} = 1) \bmod p$~~

let $f(x) = x^{\frac{p-1}{2}} - 1 \equiv 0 \pmod p$

has atmost $\frac{p-1}{2}$ sol^{n}s mod p.

But all $\frac{p-1}{2}$ QRs are sol^{n}s of this eq^n

$\Rightarrow a$ cannot be a solu^n since a is QNR.

$\therefore a^{\frac{p-1}{2}} - 1 \not\equiv 0 \pmod p$

$\Rightarrow a^{\frac{p-1}{2}} \not\equiv 1 \pmod p$. $\longrightarrow$ (1)

But By FLT, since $a \in Z_p^*$, $a^{p-1} \equiv 1 \pmod p$

$(a^{p-1} - 1) \equiv 0 \pmod p$

$(a^{p-1/2} - 1)(a^{p-1/2} + 1) \equiv 0 \pmod p$

$\therefore a^{\frac{p-1}{2}} \equiv 1 \pmod p$ (or) $a^{\frac{p-1}{2}} \equiv -1 \pmod p$ $\longrightarrow$ (2)

$\therefore$ from (1) & (2) $a^{\frac{p-1}{2}} \equiv -1 \pmod p$

$\therefore -1 \equiv a^{\frac{p-1}{2}} \pmod p$

$\Rightarrow \left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$

* properties of Legendre and Jacobi symbol

1. $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p \rightarrow \left(\frac{1}{p}\right) = 1$

$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } p = 4k+1 \\ -1 & \text{if } p = 4k+3 \end{cases}$

2. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ (completely multiplicative)

3. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{if } p = 8k \pm 1 \\ -1 & \text{if } p = 8k \pm 3 \end{cases}$

4. p, q $\rightarrow$ odd distinct primes/integers

$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$ [quadratic reciprocity law]

* Jacobi symbol computation :-

Let 'n' be odd, $a = 2^e \cdot a_1$, a_1 odd

$$\left(\frac{a}{n}\right) = \left(\frac{2^e \cdot a_1}{n}\right) = \left(\frac{2^e}{n}\right)\left(\frac{a_1}{n}\right) = \underbrace{\left(\frac{2}{n}\right)^e}_{\text{Can be calculated using above properties}}\left(\frac{a_1}{n}\right)$$

Eg: Calculate without factoring n, $\left(\frac{158}{235}\right)$

$$\left(\frac{158}{235}\right) = \left(\frac{2 \times 79}{235}\right) = \left(\frac{2}{235}\right)\left(\frac{79}{235}\right)$$

$8k+3$

$$= (-1)\left(\frac{79}{235}\right)$$

$$= (-1)\left(\frac{235}{79}\right)(-1)^{\frac{79-1}{2}\cdot\frac{235-1}{2}}$$

$$= (-1)\left(\frac{77}{79}\right)(-1) = \left(\frac{77}{79}\right) \quad (235 \bmod 79)$$

$$= (-1)^{\frac{77-1}{2}\cdot\frac{79-1}{2}}\left(\frac{79}{77}\right)$$

$$= \left(\frac{79}{77}\right)$$

$$= \left(\frac{2}{77}\right) \rightarrow 8k+3$$

$$= -1$$

* Proof of Property (2) :-

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$ $p \rightarrow$ odd prime

$\rightarrow$ legendre symbol.

Case (1) :- $p|a$ or $p|b \rightarrow$ trivial

Case (2) :- $p \nmid a$ and $p \nmid b$.

$$\left(\frac{ab}{p}\right) = (ab)^{\frac{p-1}{2}} \pmod p$$

$$= a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \pmod p$$

$\Rightarrow \left(\frac{ab}{p}\right) \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod p$

$\left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv 0 \pmod p$

$\because \left(\frac{a}{p}\right) = \pm 1 \Rightarrow \left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ can be $0, -2, 2$

$\therefore \left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = 0 \Rightarrow \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

3. (Legendre symbol) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

Proof : consider $\frac{p-1}{2}$ conguences

$$p-1 \equiv -1 \pmod p \rightarrow (1)$$
$$2 \equiv 2 \pmod p \rightarrow (2)$$
$$p-3 \equiv -3 \pmod p \rightarrow (3)$$
$$4 \equiv 4 \pmod p \rightarrow (4)$$
$$\vdots \qquad \vdots$$
$$r \equiv \left(\frac{p-1}{2}\right)(-1)^{\frac{p-1}{2}} \pmod p \rightarrow \left(\frac{p-1}{2}\right)$$

where r is either $\frac{p-1}{2}$ or $p - \left(\frac{p-1}{2}\right) = \frac{p-1}{2}$

$\therefore r = \frac{p-1}{2}$.

multiply (1), (2), ...

$$\left(2 \cdot 4 \cdot 6 \cdots \frac{p-1}{2} \cdot \frac{p+1}{2} \cdots (p-3)(p-1)\right)$$
$$\equiv \left(\frac{p-1}{2}\right)! (-1)^{1+2+3+\cdots+\frac{p-1}{2}} \pmod p$$

$$2^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)! \equiv \left(\frac{p-1}{2}\right)! (-1)^{\frac{p^2-1}{8}} \pmod p$$

$$2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} \pmod p$$

$\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \pmod p \Rightarrow \boxed{\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}}$

* **Theorem:-** If P is an odd integer, then

(i) $\left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}}$

(ii) $\left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}}$

* **Theorem:** (Reciprocity Law for Jacobi symbol)

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\frac{Q-1}{2}}, \quad \gcd(P,Q)=1,$$
P, Q odd.

(i) **Proof:** $P = P_1 P_2 P_3 \cdots P_m$. P_i's primes not necessarily distinct.

$$P = \prod_{i=1}^{m} P_i$$

$$= \prod_{i=1}^{m} (1 + P_i - 1)$$

$$= 1 + \sum_{i=1}^{m} (P_i - 1) + \sum_{\substack{i=1 \\ i \neq j}}^{m} \sum_{j=1}^{m} (P_i - 1)(P_j - 1) + \cdots$$

$$\cdots\cdots (*) \cdots$$

$$\therefore P \equiv \left(1 + \sum_{i=1}^{m} (P_i - 1)\right) \bmod 4$$

$$\underset{\text{even}}{P-1} \equiv \sum_{i=1}^{m} \underset{\text{even}}{(P_i - 1)} \pmod 4$$

lemma If $ac \equiv bc \pmod m$ & $\gcd(c, m) = d$ then $a \equiv b \pmod{\frac{m}{d}}$.

$$\therefore \frac{P-1}{2} \equiv \sum_{i=1}^{m} \frac{P_i - 1}{2} \pmod{\frac{4}{2}}$$

$$\Rightarrow \frac{P-1}{2} \equiv \sum_{i=1}^{m} \frac{P_i - 1}{2} \pmod 2$$

$$\Rightarrow (-1)^{\frac{P-1}{2}} = (-1)^{\sum_{i=1}^{m} \frac{P_i - 1}{2}}$$

$$\left(\frac{-1}{P}\right) = \prod_{i=1}^{m}\left(\frac{-1}{P_i}\right)$$

$$= \prod_{i=1}^{m}(-1)^{\frac{P_i-1}{2}}$$

$$= (-1)^{\sum_{i=1}^{m}\left(\frac{P_i-1}{2}\right)}$$

$$\therefore \left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}}$$

(ii) Proof:- $\left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}}$

$$P^2 = \prod_{i=1}^{m} P_i^2 = \prod_{i=1}^{m}(1 + P_i^2 - 1)$$

$$P^2 = 1 + \sum_{i=1}^{m}(P_i^2-1) + \sum_{i=1}^{m}\sum_{j=1}^{m}(P_i^2-1)(P_j^2-1) + \cdots$$

$(P_i^2-1) \to 8k'$; $(P_j^2-1) \to 8k'$; $(i \neq j)$; $\to 64k'$

$$P^2 = 1 + \sum_{i=1}^{m}(P_i^2-1) \pmod{64}$$

$[P_i = 4k+1$ or $4k+3$

$\Rightarrow P_i^2 = 16k^2+8k+1$ or $16k^2+24k+9$

$\to 8k'+1$; $\to 8k'+1]$

$$\frac{P^2-1}{8} \equiv \sum_{i=1}^{m}\left(\frac{P_i^2-1}{8}\right) \pmod 8$$

$$\Rightarrow \frac{P^2-1}{8} \equiv \sum_{i=1}^{m}\left(\frac{P_i^2-1}{8}\right) \pmod 8$$

$$\therefore (-1)^{\frac{P^2-1}{8}} = (-1)^{\sum_{i=1}^{m}\left(\frac{P_i^2-1}{8}\right)}$$

$$\left(\frac{2}{P}\right) = \left(\frac{2}{P_1 P_2 \cdots P_m}\right) = \prod_{i=1}^{m}\left(\frac{2}{P_i}\right) = \prod_{i=1}^{m}(-1)^{\frac{P_i^2-1}{8}}$$

$$= (-1)^{\sum_{i=1}^{m}\frac{P_i^2-1}{8}} = (-1)^{\frac{P^2-1}{8}}.$$

(iii) $\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = \prod_{i=1}^{L}\prod_{j=1}^{m}\left(\frac{P_i}{q_j}\right)\left(\frac{q_j}{P_i}\right) = \prod_{i=1}^{L}\prod_{j=1}^{m}(-1)^{\frac{P_i-1}{2}\cdot\frac{q_j-1}{2}}$

$$= (-1)^{\sum_{i=1}^{L}\sum_{j=1}^{m}\frac{P_i-1}{2}\cdot\frac{q_j-1}{2}} = (-1)^{\sum_{i=1}^{L}\frac{P_i-1}{2}\cdot\sum_{j=1}^{m}\frac{q_j-1}{2}}$$

$$= (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}$$

$$= \left((-1)^{\sum_{i=1}^{l} \frac{p-1}{2}}\right)^{\sum_{j=1}^{m} \frac{q_j-1}{2}}$$

$$= \left((-1)^{p-1/2}\right)^{\sum_{j=1}^{m} \frac{q_j-1}{2}}$$

$$= \left((-1)^{\sum_{j=1}^{m} \frac{q_j-1}{2}}\right)^{\frac{p-1}{2}}$$

$$= (-1)^{\frac{p-1}{2}\frac{Q-1}{2}}$$

$$= \left((-1)^{\sum_{i=1}^{t} \frac{p-1}{2}}\right)^{\sum_{j=1}^{m} \frac{q_j - 1}{2}}$$

$$= \left((-1)^{p-1/2}\right)^{\sum_{j=1}^{m} \frac{q_j-1}{2}}$$

$$= \left((-1)^{\sum_{j=1}^{m} \frac{q_j-1}{2}}\right)^{\frac{p-1}{2}}$$

$$= (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

* Rabin Crypto System → problem

e_K is not an injection func^n ⇒ decryption is ambiguous

→ **Setup**:- p, q → large primes, set $n = pq$.

$PK = n$, $SK = (p, q)$

→ **Encrypt**:- message $x \in Z_n$

$$y \equiv x^2 \pmod n$$

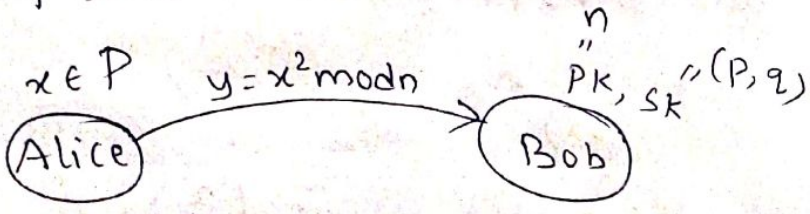
$$\mathcal{E}_{PK=n}(x) = y$$

→ **Decrypt**:- $D_{SK}(y)$.

$\|$

(p, q)

$P = C = Z_n$



$\sqrt{y} \bmod n$

↓ equivalent to

$$y \equiv x^2 \bmod n \Leftrightarrow (y \equiv x^2 \bmod p) \wedge (y \equiv x^2 \bmod q)$$

Chinese Remainder Theorem (CRT)

→ **CRT**

$m_1, m_2, \ldots, m_r$ → pairwise relatively prime.

$a_1, a_2, \ldots a_r \in Z$

$x \equiv a_1 \bmod m_1$
$x \equiv a_2 \bmod m_2$
$\vdots$
$x \equiv a_r \bmod m_r$
→ has unique soln mod M ($M = m_1 m_2 \cdots m_r$) given by

$$x = \sum_{i=1}^{r} a_i M_i y_i \bmod M$$

where $M_i = \frac{M}{m_i}$

& $y_i = M_i^{-1} \bmod m_i$, $1 \le i \le r$

$M_i y_i \equiv 1 \bmod m_i$

$\therefore x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_i M_i y_i + \cdots + a_r M_r y_r$

$\therefore x \bmod m_i = a_i M_i y_i \bmod m_i$ [$\because m_i$ is present in all other M_j's]

$= a_i \bmod m_i$

$\therefore x$ satisfies each of the above equations.

* square root modulo n

If $a \equiv x^2 \bmod n$ $\quad a, x \in Z_n^*$

Then x is sq. root modulo 'n' of a.

* → $y \equiv x^2 \bmod n \iff (y \equiv x^2 \bmod p) \wedge (y \equiv x^2 \bmod q)$ $\quad (n = pq)$

If $p \equiv 3 \pmod 4$ & $q \equiv 3 \pmod 4$

then decryption is easy.

$$\left(\pm y^{\frac{p+1}{4}}\right)^2 = y^{\frac{p+1}{2}} = y^{\frac{p-1}{2}} \cdot y$$

$$= \left(\frac{y}{p}\right) \cdot y \pmod p$$

($\because$ By Euler's criterion; $\left(\frac{y}{p}\right)$ ← legendre symbol)

$$= y \pmod p$$ [$\because y$ is a quadratic residue]

$$\left(\pm y^{\frac{p+1}{4}}\right)^2 \equiv y \pmod p$$

$\therefore x = \pm y^{(p+1)/4}$

$y \equiv x^2 \bmod p \Rightarrow \pm y^{\frac{p+1}{4}}$ $\Rightarrow x \equiv y^{\frac{p+1}{4}} \bmod p$

$y \equiv x^2 \bmod q \Rightarrow \pm y^{\frac{q+1}{4}}$ $x \equiv -y^{\frac{p+1}{4}} \bmod p$

$x \equiv y^{\frac{q+1}{4}} \bmod q$

$x \equiv -y^{\frac{q+1}{4}} \bmod q$

4 values in decryption ⇒ ambiguous

Apply CRT.

Ex: Rabin Cryptosystem:

$n = 77 = 7 \times 11$

$4.1+3$ " $4.2+3$

To decrypt $y = 23$

$(23)^{\frac{7+1}{4}} \equiv 23^2 \bmod 7 \equiv 2^2 \bmod 7 \equiv 4 \bmod 7$

$(23)^{\frac{11+1}{4}} \equiv 23^3 \bmod 11 \equiv 1 \bmod 11$

Apply CRT,

$x \equiv 4 \bmod 7$

$x \equiv -4 \bmod 7$

$x \equiv 1 \bmod 11$

$x \equiv -1 \bmod 11$

$x \equiv 4 \bmod 7$, $x \equiv 1 \bmod 11$ $\Rightarrow x = 4 \times 11 \times (11^{-1} \bmod 7) + 1 \times 7 \times (7^{-1} \bmod 11)$

$x = (4 \times 11 \times 2 + 1 \times 7 \times 8) \bmod 77$

$x = -10 \bmod 77$

Similarly, we get another 3 values for

$x \equiv -4 \bmod 7$, $x \equiv 1 \bmod 11$; $x \equiv 4 \bmod 7$, $x \equiv -1 \bmod 11$; $x \equiv -4 \bmod 7$, $x \equiv -1 \bmod 11$

$\therefore x \equiv (\pm 10, \pm 32) \bmod 77$

* Fact: (number of sq. roots) — Set of Quadratic residues mod p

1. If p is an odd prime and $a \in Q_p$, then a has exactly two square roots mod p.

If $a \equiv x^2 \bmod p \Rightarrow x, p-x$ are its solutions

$y \equiv x^2 \bmod p \Rightarrow y^{\frac{p+1}{4}}$ $\quad x \equiv y^{\frac{p+1}{4}} \bmod p$

$y \equiv x^2 \bmod q \Rightarrow y^{\frac{q+1}{4}}$ $\quad x \equiv -y^{\frac{p+1}{4}} \bmod p$

$x \equiv y^{\frac{q+1}{4}} \bmod q$

$x \equiv -y^{\frac{q+1}{4}} \bmod q$

4 values in decryption ⇒ ambiguous

Apply CRT.

Ex: Rabin Cryptosystem :

$n = 77 = 7 \times 11$

$4 \cdot 1 + 3 \quad 4 \cdot 2 + 3$

To decrypt $y = 23$

$(23)^{\frac{7+1}{4}} \equiv 23^2 \bmod 7 \equiv 2^2 \bmod 7 \equiv 4 \bmod 7$

$(23)^{\frac{11+1}{4}} \equiv 23^3 \bmod 11 \equiv 1 \bmod 11$

Apply CRT,

$x \equiv 4 \bmod 7$

$x \equiv -4 \bmod 7$

$x \equiv 1 \bmod 11$

$x \equiv -1 \bmod 11$

$x \equiv 4 \bmod 7$
$x \equiv 1 \bmod 11$ $\Rightarrow x = 4 \times 11 \times (11^{-1} \bmod 7) + 1 \times 7 \times (7^{-1} \bmod 11)$

$x = (4 \times 11 \times 2 + 1 \times 7 \times 8) \bmod 77$

$x = -10 \bmod 77$

Similarly, we get another 3 values for

$x \equiv -4 \bmod 7$, $x \equiv 4 \bmod 7$, $x \equiv -4 \bmod$
$x \equiv 1 \bmod 11$ $\quad x \equiv -1 \bmod 11$ $\quad x \equiv -1 \bmod$

$\therefore x \equiv (\pm 10, \pm 32) \bmod 77$

* Fact: (number of sq. roots)

1. If p is an odd prime and $a \in Q_p$ (Set of Quadratic residues mod p), the
a has exactly two square
mod p.

2. If $x = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, where p_i are distinct odd primes and $e_i \geq 1$.

If $a \in QR_n$ (Quadratic residues), then a has precisely 2^k distinct square roots mod n.

$$\left[\because a \in QR_n \Rightarrow a \equiv x \bmod n \right.$$
$$a \equiv x^2 \bmod p_1 < \cdot$$
$$a \equiv x^2 \bmod p_2 <$$
$$\vdots$$
$$\left. a \equiv x^2 \bmod p_k < {}_2{}^k \right]$$

* $a \in QR_p$, p odd prime $\Leftrightarrow \left(\frac{a}{p}\right) = 1$

$a \in QR_n$, n composite $\Rightarrow \left(\frac{a}{n}\right) = 1$

2. If $x = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, where p_i are distinct odd primes and $e_i \geq 1$.

If $a \in QR_n$ (Quadratic residues), then a has precisely 2^k distinct square roots mod n.

$$\left[\because a \in QR_n \Rightarrow a \equiv x^2 \bmod n \right.$$
$$a \equiv x^2 \bmod p_1 < ;$$
$$a \equiv x^2 \bmod p_2 <$$
$$\vdots \qquad \vdots$$
$$\left. a \equiv x^2 \bmod p_k < 2^k. \right]$$

* $a \in QR_p$, p odd prime $\Leftrightarrow \left(\frac{a}{p}\right) = 1$

$a \in QR_n$, n composite $\Rightarrow \left(\frac{a}{n}\right) = 1$

Ex: Find $\sqrt{68} \bmod 86$

$86 = 2 \times 43$

$68 \equiv x^2 \bmod 86$, $x = ?$

$\Rightarrow 68 \equiv x^2 \bmod 2$

$68 \equiv x^2 \bmod 43$

$68 \equiv x^2 \bmod 2 \Rightarrow x \equiv 0 \bmod 2$

$68 \equiv x^2 \bmod 43 \rightarrow$ check whether $68 \in \{1^2, 2^2, \cdots \left(\frac{43-1}{2}\right)^2\} \bmod 43$

$43 = 4 \times 10 + 3$ ($4k+3$ form)

exhaustive search

$$\therefore x \equiv \pm (68)^{\frac{43+1}{4}} \bmod 43$$

$$x \equiv \pm (68)^{11} \bmod 43$$

Use fast exponentiation to calculate

$68 \equiv 25 \bmod 43$

$(68)^2 \equiv 625 \bmod 43 = 23 \bmod 43$

$(68)^{22} \equiv (23)^2 = 13 \bmod 43$

$(68)^{23} \equiv (13)^2 = 40 \bmod 43$

$(68)^{11} = (68)(68)^2(68)^8$

$(68)^{11} = (25 \times 23 \times 40) \bmod 43$

$(68)^{11} \equiv 38 \bmod 43$

$\therefore x \equiv \pm 38 \bmod 43$

$x \equiv 0 \bmod 2$

$x \equiv 38 \bmod 43$

↓

Apply CRT

$x \equiv 0 \bmod 2$

$x \equiv -38 \bmod 43$

↓

Apply CRT

* Probabilistic Encryption :-

→ Encryption is made probabilistic

→ many possible encryption of each plaintext.

→ not feasible to test whether a given cipher text is an encryption of a particular plaintext.

→ no information about plaintext should be computable from the ciphertext.

Example:- ELGamal Encryption

* Goldwasser - Micali Bit encryption :-

Setup :- p, q → two distinct large primes

$n = pq$

Choose a pseudo ~~sequence~~ square $m \in \tilde{Q}R_n$

↓

pseudosquare modulo n.

$\left(\frac{m}{n}\right) = \left(\frac{m}{p}\right)\left(\frac{m}{q}\right) = 1$

If $m \in QR_n \Rightarrow \left(\frac{m}{p}\right) = 1 = \left(\frac{m}{q}\right)$

If $m \in \widetilde{QR}_n \Rightarrow \left(\frac{m}{p}\right) = -1 = \left(\frac{m}{q}\right)$

Square mod n

pseudosquare mod n.

(Primary key) $P.K = (n, m)$. $SK = (P, q)$ (secret key)

$\mathcal{P} = \{0,1\}$, $\mathcal{C} = Z_n^*$

*Encryption :- $x \in \{0,1\}$

$\mathcal{E}_{PK}(x) = m^x r^2 \bmod n$

where $r \in Z_n^*$ randomly.

If $x=0 \Rightarrow \mathcal{E}_{PK}(x) = r^2 \bmod n \Rightarrow \boxed{\left(\frac{y}{n}\right) = 1}$

$x=1 \Rightarrow y = \mathcal{E}_{PK}(x) = mr^2 \bmod n$

$[QR_n \times QR_n = QR_n$
$QR_n \times \widetilde{QR}_n = \widetilde{QNR}_n]$

$\widetilde{QNR}_n$ QR_n

$\widetilde{QNR}_n$

But $\boxed{\left(\frac{y}{n}\right) = 1}$ still y is $\widetilde{QNR}_n$ [$\because \left(\frac{y}{n}\right)$ is Jacobi symbol not legendre]

$\therefore x = 0$ or $1 \Rightarrow \left(\frac{y}{n}\right) = 1$

*Decryption :- $SK = (P, q)$

$$D_{SK}(y) = \begin{cases} 0 & \text{if } y \in QR_n \\ 1 & \text{if } y \notin QR_n \end{cases}$$

We just have to check $\left(\frac{y}{p}\right) = 1 \Rightarrow QR_n$

$\left(\frac{y}{p}\right) = -1 \Rightarrow \widetilde{QNR}_n$

Calculate by Euler's —

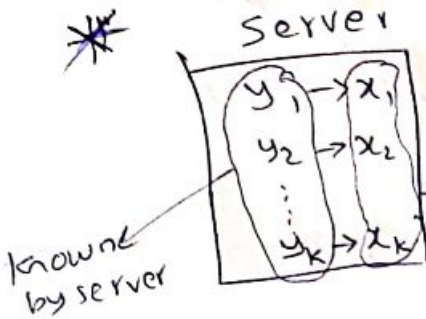
$\left(\frac{y}{p}\right) = y^{\frac{p-1}{2}} \bmod p$

Hardness assumption:-

Security relies on the hardness of DCR (Decision Composite Residuosity) problem.

↓

Decide whether $y \in QR_n$ or not given n & $\left(\frac{y}{n}\right) = +1$



$\rightarrow y_1 y_2 = (m^{x_1} r_1^2)(m^{x_2} r_2^2) \bmod n$

$= m^{x_1 \oplus x_2} (r_1 r_2)^2 \bmod n$

$= \mathcal{E}(x_1 \oplus x_2) \Rightarrow \mathcal{E}(x_1)\mathcal{E}(x_2) = \mathcal{E}(x_1 \oplus x_2)$

additively Homomorphic

Homomorphic encryption:-

Goldwasser-Micali → additively Homomorphic

RSA → $y_1 = x_1^e \bmod n$

$y_2 = x_2^e \bmod n$

$y_1 y_2 = (x_1 x_2)^e \bmod n$

$\mathcal{E}(x_1)\mathcal{E}(x_2) = \mathcal{E}(x_1 x_2)$

↳ multiplicatively homomorphic

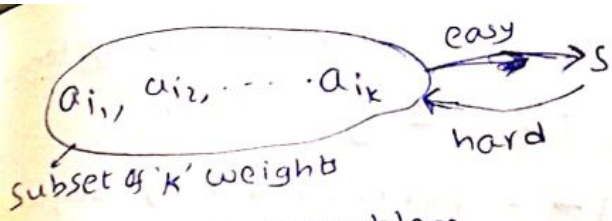
If we have fully homomorphic encryption, any arithmetic expression's (in $x_1, x_2, \ldots x_k$) can be calculated.

* Markle Hellman Knapsack Cryptosystem:-

Knapsack problem (0/1 knapsack) (or) Subset sum problem

$[a_0, a_1, \ldots a_n]$ → a vector of distinct +ve integers

→ object weights



Subset sum problem

Problem instance : $I = (a_1, a_2, \cdots a_n, S)$

where $a_1, a_2, \cdots, a_n$ & S are +ve integers.

a_i's → sizes/weights

S → target sum.

Question: Is there a 0-1 vector $x = (x_1, x_2, \cdots, x_n)$ such that $\langle x, a \rangle = x_1 a_1 + x_2 a_2 + \cdots + x_n a_n = S$

where $x_i \in \{0, 1\}$

Ex: $[a_1, a_2, a_3, a_4, a_5, a_6] = [3, 4, 6, 8, 10, 12]$

$S = 28$. find all soln's.

$x = [0, 0, 1, 0, 1, 1]$

(or)

$x = [0, 1, 1, 1, 1, 0]$

* If $[a_1, a_2, \cdots, a_n]$ is superincreasing

i.e if $a_i > a_1 + a_2 + \cdots + a_{i-1}$

for $i = 1, 2, 3, \cdots, n$

Proposition:

A knapsack problem with superincreasing weights can have atmost one soln

Ex) $[a_1, a_2, a_3, a_4, a_5, a_6] = [1, 2, 4, 9, 20, 48]$

$S = 27$.

$x_6 = 0$, $x_5 = 1$ $\quad S = 27 - 20 = 7$

$x_4 = 0$

$x_3 = 1$ $\quad S = 7 - 4 = 3$

$x_2 = 1$, $x_1 = 1$ $\quad \therefore x = [1, 1, 1, 0, 1, 0]$

∴ Markle - Hellman knapsack cryptosystem :

$P = \{0,1\}^n$, $C = Z_{\geq 0}$ → integers

$[a_1, a_2, \ldots, a_n]$ → superincreasing sequence of wts.

$m > \sum_{i=1}^{n} a_i$, $1 < w < m$ s.t $\gcd(w, m) = 1$

$SK = \{[a_1, a_2, \ldots, a_n], w, m\}$

$PK = [b_1, b_2, \ldots, b_n]$

where $b_i = a_i w \bmod m$

Alice — Bob

PK, SK

$x = [x_1, x_2, \ldots x_n] \in \{0,1\}^n$

$E_{PK}(x) = \langle b; x \rangle$

$= x_1 b_1 + x_2 b_2 + \ldots + x_n b_n \in Z$

$D_{SK}(s) = s w^{-1} \bmod m$

$= x_1 a_1 + x_2 a_2 + \ldots + x_n a_n$

superincreasing.

∴ $[x_1, x_2 \ldots x_n]$ can be found easily.

∴ Markle - Hellman knapsack cryptosystem:

$P = \{0,1\}^n$, $\mathcal{C} = Z_{\geq 0}$ → integers

$[a_1, a_2, \ldots, a_n]$ → superincreasing sequence of wts.

$m > \sum_{i=1}^{n} a_i$, $1 < w < m$ s.t $\gcd(w, m) = 1$

$SK = \{[a_1, a_2, \ldots, a_n], w, m\}$

$PK = [b_1, b_2, \ldots, b_n]$

where $b_i = a_i w \bmod m$

Alice — Bob

$x = [x_1, x_2, \ldots x_n] \in \{0,1\}^n$ — PK, SK

$E_{PK}(x) = \langle b; x \rangle$

$= x_1 b_1 + x_2 b_2 + \cdots + x_n b_n \in Z$

$D_{SK}(s) = s w^{-1} \bmod m$

$= x_1 a_1 + x_2 a_2 + \cdots + x_n a_n$

superincreasing.

∴ $[x_1, x_2 \ldots x_n]$ can be found easily.

* The Pohlig - Hellman Algorithm to solve DLP:

Objective: To determine (uniquely) the value of $a = \log_\alpha \beta \bmod n$ $(\alpha, \beta = \alpha^a)$ (α: order n; $1 \leq a \leq n-1$)

let $n = \prod_{i=1}^{k} p_i^{e_i}$

Compute $a \bmod p_i^{c_i}$ for each i, $1 \leq i \leq k$.

Apply CRT to get $a \bmod n$.

Goal:-
Compute $a \bmod q^c$, q is prime such that

$$q^c \mid n \;\&\; q^{c+1} \nmid n$$

Let $x \equiv a \bmod q^c$ when $0 \le x \le q^c - 1$

$\Rightarrow q^c \mid a - x$

(or) $a = x + sq^c$, $s \in Z$.

Represent 'x' in radix q.

$x = (a_0 + a_1 q + a_2 q^2 + \cdots + a_{c-1} q^{c-1}) \bmod q^c$

as $0 \le x \le q^c - 1$

& $a_i \in \{0, 1, \ldots, q-1\}$

$$\Rightarrow x = \sum_{i=0}^{c-1} a_i q^i$$

$$\text{So} \quad a = \left\{ \sum_{i=0}^{c-1} a_i q^i \right\} + sq^c$$

Compute a_0

Claim:- $\beta^{\frac{n}{q}} = \alpha^{\frac{a_0 n}{q}}$

Proof: $\beta^{\frac{n}{q}} = \alpha^{\frac{an}{q}} = (\alpha^a)^{\frac{n}{q}} = \alpha^{a\left(\frac{n}{q}\right)}$

$$= \alpha^{\frac{n}{q}(a_0 + a_1 q + a_2 q^2 + \cdots + a_{c-1} q^{c-1} + sq^c)}$$

$$= \alpha^{\frac{a_0 n}{q}} (\alpha^n)^k = 1 \quad [\because \alpha \text{ is of order } n]$$

$$\therefore \beta^{\frac{n}{q}} = \alpha^{\frac{a_0 n}{q}}.$$

$\therefore$ To find out a_0, search exhaustively

if $\beta^{n/q} = \gamma^i \quad i = 0, 1, \ldots q-1$

where $\gamma = \alpha^{\frac{n}{q}}$

If $c = 1 \rightarrow$ done

If $c > 1$, proceed to determine $a_1, a_2 \ldots a_{c-1}$ as follows.

- Define $\beta_0 = \beta$

$$\beta_j = \beta \alpha^{-(a_0 + a_1 q + \cdots + a_{j-1} q^{j-1})}$$

claim:- $\beta_j^{\frac{n}{q^{j+1}}} = \alpha^{\frac{a_j n}{q}}$ for $1 \le j \le c-1$

for $j=0$, it is already Proved

Proof: same like above

Take $\gamma = \alpha^{\frac{n}{q}}$

Calculate $\beta_j^{\frac{n}{q^{j+1}}}$.

$$* \quad \frac{\beta_{j+1}}{\beta_j} = \alpha^{-a_j q^j} \Rightarrow \beta_{j+1} = \beta_j \alpha^{-a_j q^j}$$

Ex:- ElGamal

$p = 29, \alpha = 2$

$n = ord(\alpha) = p-1 = 28 = 2^2 \cdot 7^1$

let $\beta = 18 = \alpha^a$. Find a.

Sol: Find $a \bmod 2^2$

& $a \bmod 7^1$

Then, apply CRT

To find $a \bmod 2^2$

$x \equiv a \bmod 2^2$ ← c, $2^2 \rightarrow q$

write in radix '2'.

$a = a_0 + 2a_1 + 2^2 s, \quad s \in Z$.

Find a_0, a_1. Ans: $a_0 = 1, a_1 = 1$

To find $a \bmod 7^1$

$x \equiv a \bmod 7^1$ ← c, q

write in radix 'j'.

$a = a_0 + s \cdot 7^1 \quad s \in Z$ Ans: $a_0 = 4$

for a mod 7,

$x \equiv a \bmod 7$ ⇒ $q = 7, c = 1$

$\beta_0 = \beta = 18$

$a_0 = ?$

$x = a_0$

$\beta^{\frac{n}{q}} = \beta^{\frac{28}{7}^4} = (18)^4 = 2^4 \times 3^8$

$\gamma = \alpha^{\frac{n}{q}} = 2^{\frac{28}{7}^4} = 2^4$

$\gamma^2 = 2^8$

$\gamma^3 = 2^{12}$

$\gamma^4 = 2^{16} = 2^4 \times 2^{12}$

$2^4 \times 3^8 \bmod p = 2^4 \times 2^{12} \bmod p$

$2^4 \times 3^8 \bmod 29 = 2^4 \times 2^{12} \bmod 29 \Rightarrow \boxed{a_0 = 4}$

Elliptic curves :-

Let $p > 3$ be prime.

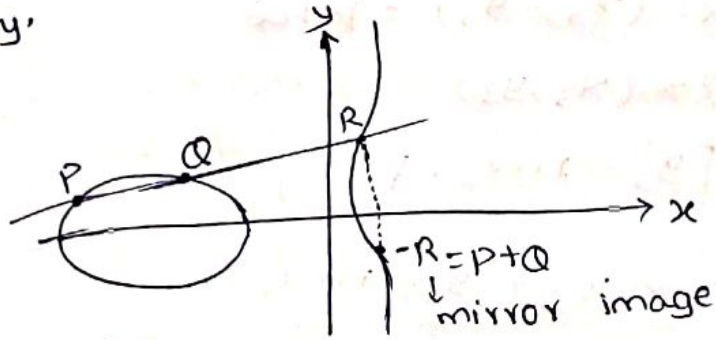
The elliptic curve over Z_p.

$E/Z_p : y^2 = x^3 + ax + b \pmod p \rightarrow (1)$ (x over Z_p)

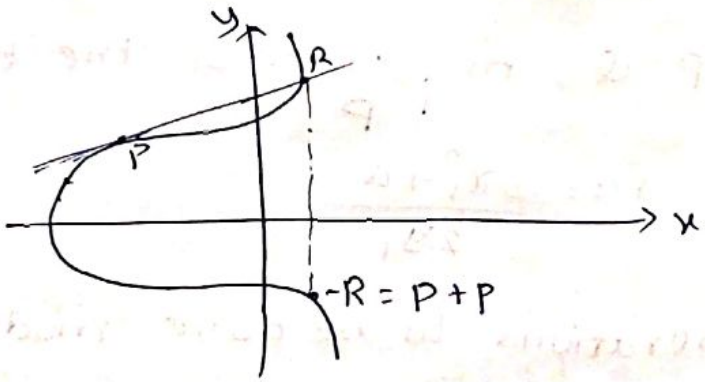
where $a, b \in Z_p$ are constants satisfying

$$4a^3 + 27b^2 \neq 0$$

Elliptic curve is the set of sol^{n}s $(x, y) \in Z_p \times Z_p$ satisfying (1) together with a special point (H) called the point at infinity.



(or)



*Point addition :-

The chord joining P & Q as in above fig. intersects the curve in 3rd point 'R'.

$-R$: the mirror image of R w.r.t x-axis

$$-R = P + Q.$$

If P & Q are same, then take the tangent.

* Chord & tangent law :

$P = (x_1, y_1)$

$Q = (x_2, y_2)$

$\overleftrightarrow{PQ}$ $\quad y = mx + \lambda$.

If $P \neq Q \Rightarrow \lambda = y_1 - mx_1$, $m = \frac{y_2 - y_1}{x_2 - x_1}$

$① \Rightarrow (mx + \lambda)^2 = (x^3 + ax + b) \pmod p$

$x^3 - m^2x^2 + (a - 2m\lambda)x + (b - \lambda^2) = 0$

$\Rightarrow x_1 + x_2 + x_3 = m^2$

$$\boxed{x_3 = m^2 - x_1 - x_2}$$

$-R = (x_3, -y_3) = P + Q$.

$R = (x_3, y_3)$

$$\therefore \boxed{y_3 = mx_3 + \lambda}$$

$y_3 = mx_3 + y_1 - mx_1$

$$\boxed{y_3 = \frac{y_2 - y_1}{x_2 - x_1}(x_3 - x_1) + y_1}$$

If $P = Q$, m = slope of the tangent at P

$$m = \frac{3x_1^2 + a}{2y_1}$$

All operations to be done modulo 'p'

so $m = \frac{y_2 - y_1}{x_2 - x_1} \Rightarrow m = (y_2 - y_1)(x_2 - x_1)^{-1} m$

* E/K : $y^2 = x^3 + ax^2 + b$, $4a^3 + 27b^2 \neq 0$

K any field

$a, b \in K$,

$Ch(K) \neq 2, 3$.

→ If $P = (x_1, y_1) \neq (H)$, than $-P = (x_1, -y_1)$.

→ If $P = (x_1, y_1) \neq (H)$, $Q = (x_2, y_2) \neq (H)$ & $P \neq -Q$ i.e $\overleftrightarrow{PQ}$ is not vertical line, then

$P+Q = (x_3, y_3)$

$\Rightarrow x_3 = m^2 - x_1 - x_2$

$y_3 = m(x_1 - x_3) - y_1$

$$m = \begin{cases} (y_2 - y_1)/(x_2 - x_1) & \text{if } P \neq Q \\ (3x_1^2 + a)/2y_1 & \text{if } P = Q,\ y_1 \neq 0 \end{cases}$$

→ If $P \neq \textcircled{H}$, then $P + \textcircled{H} = \textcircled{H} + P = P$

$\textcircled{H}$ → additive identity

(or) point at infinity

it is called so since $P + \textcircled{H} = P$

$\Rightarrow P + (-P) = -\textcircled{H}$

→ $\textcircled{H}$ is the point of intersection of chord joining P & -P i.e vertical line.

→ If $P = -Q$, then $P + Q = \textcircled{H}$

$= -\textcircled{H}$.

$(E/K, +)$ is an abelian group & $\textcircled{H}$ is identity element.

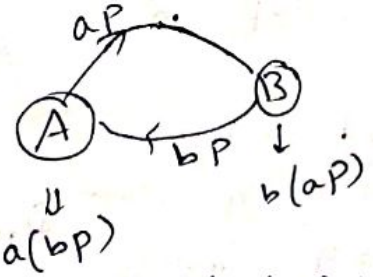
~~* DLP over $Z_p^*(=<g>)$~~

* DLP over $E/Z_p (=<P>)$ is

given P, aP → find a.

i.e. P, $\underbrace{P+P+P-\cdots+P}_{a \text{ times}}$ → find a.

DH keyexchange →



equally secure ~~to~~ over Z_p but with much lesser primes 'p' since DLP over Z_p has methods to solve it.

* Bilinear pairing / Bilinear map / weil pairing / Tate pairing → defined for an elliptic curve.

* $E/K : y^2 = x^3 + ax + b$, $a, b \in K$

By changing a, b we can get various elliptic curves over same K.

* E/K is also defined as E(K).

Find a generator for a cyclic subgroup of E(K).

Then only, we can use D-H key exchange.

Ex:- $E/Z_{11} : y^2 = x^3 + 7x + 5$.

Find all points on E.

& (set of Quadratic residues)

x	$(x^3+7x+5) \bmod 11$	is Q_{11}?	y
0	5	Yes	$\pm 4 \Rightarrow (0,4), (0,7)$
1	2	NO	-
2	5	Yes	$\pm 4 \Rightarrow (2,4), (2,7)$
3	9	Yes	$\pm 3 \Rightarrow (3,3), (3,8)$
4	9	Yes	$\pm 3 \Rightarrow (4,3), (4,8)$
5	0	NO	$- \Rightarrow (5,0)$
6	10	NO	-
7	1	Yes	$\pm 1 \Rightarrow (7,1), (7,10)$
8	1	Yes	$\pm 1 \Rightarrow (8,1), (8,10)$
9	5	Yes	$\pm 4 \Rightarrow (9,4), (9,-4)$
10	8	NO	-

$1^2 \equiv 1 \bmod 11$

$2^2 \equiv 4 \bmod 11$

$3^2 \equiv 9 \bmod 11$

$4^2 \equiv 5 \bmod 11$

$5^2 \equiv 3 \bmod 11$

$\therefore Q_{11} = \{1, 3, 4, 5, 9\}$

$\therefore E/Z_{11} = \{(0,4), (0,7), \ldots\} \cup \{H\}$

$\#E(Z_{11}) = 16$

Ex: $\text{ord}_E((2,4)) = ?$ (Point on E/Z_{11})

$P = (2,4)$

$\text{ord}_E(P)$ is the least +ve k such that

$kP = \mathcal{O}$ (H).

But $k \mid \#E(Z_{11}) \Rightarrow k \mid 16 \Rightarrow k = 2$ or 4 or 8 or 16.

Ex: $P = (2,4)$. Find $10P$. (scalar multiple)

Find by double & add.

$(10)_2 = (1010)_2$

$\Rightarrow 10P = 2P + 8P$

$2^0 \cdot P = P = (2,4)$

$2^1 \cdot P = 2P = (8,1)$

~~(x_3, y_3)~~ $P = (x_1, y_1)$

$x_3 = m^2 - x_1 - x_1$

$y_3 = m(x_3 - x_1) + y_1$

$m = \left(\frac{3x(2)^2 + 7}{8}\right) = 19 \times 8^{-1} \bmod 11$

$= 8 \times 8^{-1} \bmod 11 = 1 \bmod 11$

$\therefore x_3 = 1 - 4 = -3 = 8 \bmod 11$

$y_3 = 1(8-2) + 4 = 10 \bmod 11$

$\Rightarrow 2P = (x_3, -y_3) = (8,1)$

Similarly, $2^2 P = 4P = (9,4)$

$2^3 P = 8P = (5,0)$

$\therefore 10P = 2P + 8P = (8,1) + (5,0)$

$= (3,8)$.

Now, $8P = (5,0) \Rightarrow -8P = (5,-0) = (5,0)$.

$\therefore 16P = 8P + 8P = 8P + (-8P) = \textcircled{H}$

$\therefore ord_E((2,4)) = 16 = \#E(Z_{11})$

$\Rightarrow E(Z_{11})$ is a cyclic group.

* $E/F_q : y^2 = x^3 + ax + b$, $Ch(F_q) \neq 2, 3$.

$E[2] \rightarrow$ set of all 2-torsion pts.

$E[m] = \{ P \in E/F_q \mid mP = \textcircled{H} \}$

↓ set of all m-torsion pts.

If $gcd(m,q) = 1$, then: $\#E[m] = m^2$

& $E[m] \tilde{\simeq} Z_m \times Z_m$.

↓ isomorphic

$\therefore P \in E[2] \Rightarrow 2P = \textcircled{H} \Rightarrow P + P = \textcircled{H}$

$\therefore P = -P \Rightarrow P = (x_1, 0)$.

↙ 3 soln's for $x^3 + ax + b = 0$

$\therefore E[2] = \{(x_1,0), (x_2,0), (x_3,0)\} \cup \{\textcircled{H}\}$

$\textcircled{H} \in E[m]$ $\forall m$ since $m\textcircled{H} = \textcircled{H}$

* q is an odd prime power,

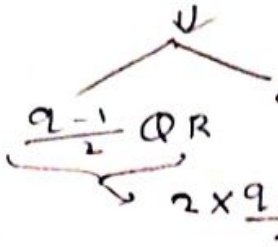
$q \equiv 2 \pmod 3$

$E/F_q : y^2 \equiv x^3 + b$, $b \in F_q$, $b \neq 0$.

$\#E(F_q) = ?$

$x \rightarrow x^3 + b$ → Forms a permutation of F_q if x is varied over entire F_q.

for $x \in F_q$, $x \neq 0$, $x^3+b \in F_q$ & it is a permutation of F_q



If $x^3+b=0$ i.e $y=0 \Rightarrow x = \sqrt[3]{-b} \Rightarrow (\sqrt[3]{-b}, 0)$.

3.

& $\infty \in E/F_q$

$\therefore \# E(F_q) = 2 \times \frac{q-1}{2} + 1 + 1 = q+1$

Q. E/F_{p^n}, $p \neq 2, 3$

. $E/F_{25} : y^2 = x^3 + x + 4$

$F_{25} = Z_5[x]/(x^2+4x+2)$

of the form $ax+b$, $a \in Z_5$, $b \in Z_5$

Total no. $= 5 \times 5 = 25$

Find $\# E(F_{25})$. Ans = 27

$F_{25} = \{0, 1, 2, 3, 4, \omega, \omega+1, \omega+2, \omega+3, \omega+4, \ldots \ldots \ldots 4\omega+4\}$

$(4\omega+4)^2 = 16\omega^2 + 32\omega + 16$

If $Z_5[x]$ it is $\omega^2 + 2\omega + 1$

$\therefore$ $\omega^2+2\omega+1 / (\omega^2+4\omega+2)$

$= \omega + 3 + 2\omega + 1$

$= 3\omega + 4$

$\left[\because \omega^2+4\omega+2 = 0 \Rightarrow \omega^2 = -4\omega - 2 = \omega + 3\right]$

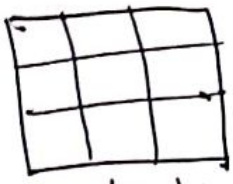
$\therefore QR_{25} = \{1, 4, \omega+3, 3\omega+4, 2, 2\omega+2, 4\omega+4, 4\omega+2, 3\omega+3, 2\omega+1, \omega+1, 3\}$

* Projective plane

$(X_1, Y_1, Z_1) \sim (X_2, Y_2, Z_2)$

if $X_1 = \lambda X_2$, $Y_1 = \lambda Y_2$, $Z_1 = \lambda Z_2$.

for some scalar $\lambda \in K$



equivalence class of (X, Y, Z)

Projective point

The equivalence class containing the triple (X, Y, Z) is a projective point.

Case: $Z \neq 0$ → only projective point is $(x, y, 1)$

→ The class containing the triple $(x, y, 1)$

$$x = \frac{X}{Z}, \quad y = \frac{Y}{Z}.$$

$$(x, y, 1) \sim (X, Y, Z)$$

Projective plane:

It is ~~defined as~~ identified with all points (x, y) in ordinary plane (affine plane)

+

The projection points for which $Z = 0$.

↙

line at infinity in the ~~proje~~ affine plane

$F(x,y)=0$ → a curve in affine plane

$\bar{F}(x,y,z)=0$ → projective equation satisfied by projective points.

↳ Substitute $x=\frac{X}{Z}$, $y=\frac{Y}{Z}$ & multiply by powers of Z to clear the denominators

* $E/K: y^2=x^3+ax+b \rightarrow ①$, $a,b \in K$.
$4a^3+27b^2 \neq 0$
$ch(K) \neq 2,3$

$z \neq 0$. put $x=\frac{X}{Z}$, $y=\frac{Y}{Z} \rightarrow ②$

$\Rightarrow \frac{Y^2}{Z^2}=\frac{X^3}{Z^3}+\frac{aX}{Z}+b$

$$\boxed{ZY^2=X^3+aXZ^2+bZ^3}$$

↓ projective equation → satisfied by all projective points (X,Y,Z) where $Z \neq 0$

$z=0$ in ③ $\Rightarrow X=0$

$\therefore (0,1,0)$ → only projective point with both $X, Z=0$

[$\because (0,1,0) \sim (0,\lambda,0)$ for any λ ⇒ they're the same point]

$(0,1,0) \rightarrow$ Ⓗ → In projective plane, Ⓗ $=(0,1,0)$.

↙ point of intersection of Y-axis with the line at infinity.

* Menezes-Vanstine Elliptic curve Cryptosystem:-

E/Z_p $(p>3$, prime) → Elliptic curve s.t E contains a cyclic subgroup H in which DLP is intractable

$P = Z_p^* \times Z_p^*$

$G_0 = E \times Z_p^* \times Z_p^*$

$K = \{ (\underbrace{E, \alpha, \beta}_{\text{public}}, \overset{\text{secret}}{a}) \mid \beta = a\alpha \}$ $\alpha \in E$

$P.k = (E, \alpha, \beta)$, $S.k = \{a\}$

Encryption :-

$\mathcal{E}_{pk}(x) =$ choose $k \in Z_{|H|}$ → cyclic subgroup 'H' in prev. page

$x = (x_1, x_2) \in Z_p^* \times Z_p^*$ (α, β)

compute $y_0 = k\alpha$

$(c_1, c_2) = k\beta$

$y_1 = c_1 x_1$, $y_2 = c_2 x_2$

$\mathcal{E}_{pk}(x) = (y_0, y_1, y_2)$ $[x = (x_1, x_2)]$

(α, β)

Decryption :-

$\mathcal{D}_{sk}(y) =$ From above,

$(c_1, c_2) = k\beta = ka\alpha$

$= ak\alpha$

$(c_1, c_2) = ay_0$

$y = (y_0, y_1, y_2)$

=> compute $ay_0 = (c_1, c_2)$

$y_1 = c_1 x_1 \Rightarrow x_1 = c_1^{-1} y_1$

$y_2 = c_2 x_2 \Rightarrow x_2 = c_2^{-1} y_2$

$\therefore \boxed{x = (x_1, x_2)}$

* Generalized ElGamal Public-key

Encryption :-

$(G, 0)$ → a finite group

$\alpha \in G$ s.t DLP in H is intractable where

$H = \{ \alpha^i \mid i \geq 0 \}$

$\alpha^i = \alpha \cdot \alpha \cdot \alpha \cdot \ldots \cdot \alpha$

$P = G$, $C = G \times G$ $K = \{(G, \alpha, \beta, a) \mid \beta = \alpha^a\}$

$PK = (G, \alpha, \beta)$

$SK = a$

Encryption :

$e_{PK}(x) = (y_1, y_2)$

choose $k \in Z_{|H|}$ $y_1 = \alpha^k$

$y_2 = x\beta^k = x\alpha^{ak} = x(\alpha^k)^a$

$= x\, y_1^a$

Decryption :

$D_{SK}((y_1, y_2)) = \frac{y_2}{y_1^a} = x$

* p prime

$(Z_p^*, \cdot)$ isomorphic $(Z_{p-1}, +)$

DLP $g, g^a \to a$ $g, ag \to a$

cyclic isomorphic to $(Z_{p-1}, +)$

$\phi : Z_p^* \to Z_{p-1}$

$\alpha, \beta = \alpha^a \to$ find $a \to$ DLP in $(Z_p^*, \cdot)$.

$\Rightarrow \phi(\alpha), \phi(\beta) = a\,\phi(\alpha) \to$ find $a \to$ DLP in $(Z_{p-1}, +)$.

If we know ϕ, using extended Euclidean algorithm, 'a' can be found.

[∵ all we need to do is find $(\phi(a))^{-1}$]

But finding ϕ is usually difficult.

*Careful about the choice of your group such that finding ϕ is difficult.

$G \to H = \langle \alpha \rangle$

If $\exists \phi : H \to Z_{|H|}$, then DLP in H will be easy

DLP may be easy or difficult depending on the representation of the cyclic group used

$GF(p^n)$ elliptic curve E.C. group

$K \to$ finite field, $\bar{K} \to$ algebraic closure

Ex: If $K = F_q$, then $\bar{K} = \bigcup_{m \geq 1} F_{q^m}$

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_5$$

$a_1, a_2, a_3, a_4, a_5 \in K$

with no singular point ($F(x,y) = 0$, $F' \neq 0$)

Weierstress eqn.

→ The set of K-rational points

$$E(K) = \{(x, y) \in K \times K\} \cup (H)$$

(satisfy the above eqn.)

where (H) is called the identity (also called the point at infinity).

* Simplified weierstress eqn:

1. $ch(K) \neq 2, 3$

$$y^2 = x^3 + ax + b, \quad a, b \in K, \quad 4a^3 + 27b^2 \neq 0$$

2. $ch(K) = 2$

$$y^2 + xy = x^3 + ax + b, \quad a, b \in K, \quad b \neq 0$$

(non-super singular)

(or)

$$y^2 + cy = x^3 + ax + b, \quad a, b \in K, \quad c \neq 0.$$

(super singular)

3. $ch(K) = 3$.

$$y^2 = x^3 + ax^2 + bx + c, \quad a, b, c \in K.$$

(cubic on the right has no multiple roots.)

* Supersingular Elliptic curve:-

E/F_q is supersingular if $p \mid t$

where $t = q+1 - \#E(F_q)$,

$q = p^m$, $p = ch(F_q)$.

* Hasse's Theorem:-

$$|t| \leq 2\sqrt{q}$$

$$\Rightarrow -2\sqrt{q} \leq q+1-\#E(F_q) \leq 2\sqrt{q}$$

$$q+1-2\sqrt{q} \leq \#E(F_q) \leq q+1+2\sqrt{q}$$

* Theorem (Waterhouse):-

E/F_q is supersingular iff

$t^2 = 0, q, 3q$, or $4q$.

Ex: ~~E/F_q~~ $q \rightarrow$ odd prime, $q \equiv 2 \pmod 3$.

$F/F_q : y^2 = x^3 + b$, $b \in F_q$, $b \neq 0$.

$\#E(F_q) = q+1$

$t = q+1 - \#E(F_q) = 0$

$\rightarrow$ It is supersingular.

* Ex: q be an odd prime power.

$q \equiv 3 \pmod 4$.

$E/F_q : y^2 = x^3 + ax$, $a \in F_q$, $a \neq 0$.

Show that E is supersingular.

Sol: $q = 4k+3 \Rightarrow (-1)^{\frac{q-1}{2}} = (-1)^{2k+1} = -1$

$-1 \in QNR$

$(-x)^3 + a(-x) = -(x^3+ax)$

For each $x \in F_q$ with $x \neq 0$ → $x^3 + ax \neq 0$

→ $x^3 + ax = 0$

$x(x^2 + a) = 0$

$x = \pm\sqrt{-a}$

$x^3 + ax \in QR$

2 Points for $y = \sqrt{x^3 + ax}$

$x^3 + ax \in QNR$

$\Rightarrow -(x^3 + ax) \in QR$

2 points.

#points = $2 \times \frac{q-1}{2}$ → either x or -x is contributing 2 points

$\frac{q-1}{2} + \frac{q-1}{2}$

for QR for QNR

$= q - 1$

$= q + 1$

* $x = 0 \Rightarrow y = 0 \rightarrow (0,0)$

$\therefore$ # points = $q - 1 + 1 + 1$ (for Ⓗ)

$\Rightarrow t = q + 1 - (q + 1) = 0$

* $E = E/\bar{K}$ → weierstress eqn.

Theorem:-

(i) $(E, +)$ is an abelian group with identity Ⓗ.

(ii) E/K is a subgroup of E.

* Theorem (Weil):-

Let $t = q + 1 - \#E(F_q)$

then $\#E(F_{q^k}) = q^k + 1 - \alpha^k - \beta^k$

where α, β are complex numbers determined from the factorization of

$1 - tT + qT^2 = (1 - \alpha T)(1 - \beta T)$.

* Sherf's algorithm: to count # of pts of Elliptic curve → Polynomial time algo.

Theorem:- (≅ → isomorphic)

$E(F_q) \cong Z_{n_1} \oplus Z_{n_2}$

where $n_2 | n_1$ & $n_2 | q-1$.

Moreover $E(F_q)$ is cyclic if $n_2 = 1$

* **Theorem :-**

If $\gcd(n, q) = 1$, then $[E \cong E/\langle \infty \rangle]$

$E[n] \cong Z_n \oplus Z_n$ (→ isomorphic)

$\therefore |E[n]| = n^2$

$E[n] = \{P \in E \mid nP = \oplus\}$

set of all n-torsion points

→ If 'n' is a prime with ~~$n \nmid F_q$~~ $n | E(F_q)$ with $\gcd(n, q) = 1$, then $E[n]$ is a subgroup E/F_{q^k} where k is the smallest +ve integer s.t. $n | q^k - 1$.

$k \rightarrow$ embedding degree.

Ex:- $q = 5$. $E(F_5): y^2 = x^3 + x + 4$

$\#E(F_5) = 9$.

$\#E(F_{25}) = 27$

$F_{25} = Z_5[x]/(x^2 + 4x + 2)$

Take $n = 3$ prime, $n | q$, $\gcd(n, q) = 1$ (3, 5)

$E[3] \rightarrow$ set of all 3 torsion point

↓ subgroup of E/F_{q^k}, $k \rightarrow$ embedding degree

$3 | q^k - 1 \Rightarrow$ smallest $k = 2$

* **Theorem** (schoof) (Supersingular elliptic curve).

E/F_q supersingular, $t = q + 1 - \#E(F_q)$.

(i) if $t^2 = q, 2q$ or $3q \Rightarrow E(F_q)$ is cyclic.

(ii) if $t^2 = 4q$ & $t = 2\sqrt{q} \Rightarrow E(F_q) \cong Z_{\sqrt{q}-1} \oplus Z_{\sqrt{q}+1}$

(iii) if $t^2 = 4q$ & $t = -2\sqrt{q}$

$$E(F_q) \cong Z_{\sqrt{q}+1} \oplus Z_{\sqrt{q}+1}$$

(iv) if $t = 0$ & $q \neq 3 \bmod 4$

$E(F_q)$ is cyclic

(v) if $t = 0$ & $q = 3 \bmod 4$

$$E(F_q) \cong Z_{\frac{q+1}{2}} \oplus Z_2$$

(iii) if $t^2 = 4q$ & $t = -2\sqrt{q}$

$$E(F_q) \cong Z_{\sqrt{q}+1} \oplus Z_{\sqrt{q}+1}$$

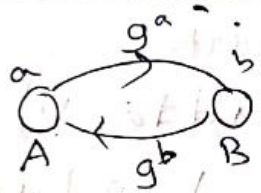
(iv) if $t = 0$ & $q \neq 3 \bmod 4$

$E(F_q)$ is cyclic

(v) if $t = 0$ & $q = 3 \bmod 4$

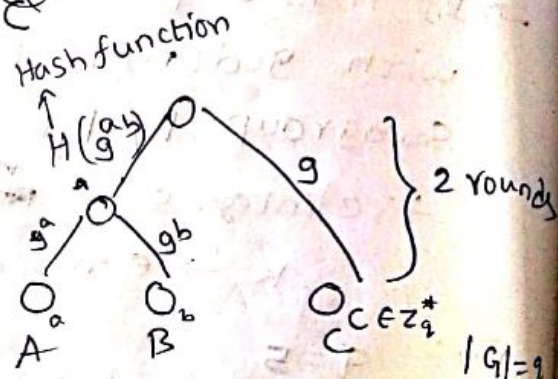
$$E(F_q) \cong Z_{\frac{q+1}{2}} \oplus Z_2$$

* Single Round 2-party key agreement (DH)



$K = g^{ab}$

* If there are '3' people,



$H: G \to Z_q^*$ (Hash func^n)

single round not possible for Diffie-Hellman

* Bilinear pairing:-

$e: G_1 \times G_1 \longrightarrow G_2$

$|G_1| = |G_2| = q$ → cyclic groups, DLP is hard in both G_1, G_2

$G_1 \rightarrow$ additive group

$G_2 \rightarrow$ multiplicative group.

Satisfies

(i) Bilinearity → $e(aP, bQ) = (e(P,Q))^{ab}$,

$a, b \in Z_q^*$, $P, Q \in G_1$

& $e(P_1 + P_2, Q) = e(P_1, Q) \cdot e(P_2, Q)$

$e(P, Q_1 + Q_2) = e(P, Q_1) \cdot e(P, Q_2)$.

(ii) Non-degeneracy → if $G_1 = \langle P \rangle$, then

~~$G_2 = e(P,P)$~~

$G_2 = \langle e(P,P) \rangle$

i.e $e(P,P) \neq 1$

(iii) Computability → polynomial time algorithm to compute 'e'.

Miller's algo.

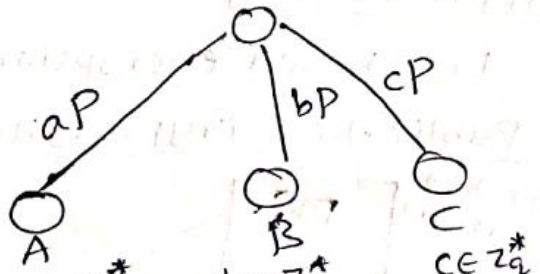
Examples:-

Weil pairing, Tate pairing.

* Single-round 3-party key agreement (Joux):-

$G_1 = \langle P \rangle$

$\Rightarrow G_2 = \langle e(P, P) \rangle$



A: receives bP, cP.

→ compute $(e(bP, cP))^a = (e(P,P))^{abc}$

B: → compute $(e(aP, cP))^b = (e(P,P))^{abc}$

C: → compute $(e(aP, bP))^c = (e(P,P))^{abc}$

$\therefore K = (e(P,P))^{abc}$

Given $\langle P, aP, bP, cP \rangle$ } → Bilinear Diffie-Hellman Problem (BDH)

finding $(e(P,P))^{abc}$ }

because P & aP given → cannot find a (DLP in G_1)

Adversary: Given $\langle P, aP, bP, cP \rangle$, should not be able to distinguish $e(P,P)^{abc}$ from a random key.

DBDH (Decisional BDH)

$\langle P, aP, bP, cP, K \rangle \equiv_c \langle P, aP, bP, cP, e(P,P)^{abc} \rangle$.

→ computationally

for any key K, he cannot tell if it is $e(P,P)$

DDH (Decisional Diffie-Hellman)

$\langle g, g^a, g^b, g^{ab} \rangle \equiv_c \langle g, g^a, g^b, k \rangle$

for any $k \in K$

* Generalisation to multilinear matching

$e : G_1^n \rightarrow G_2$.

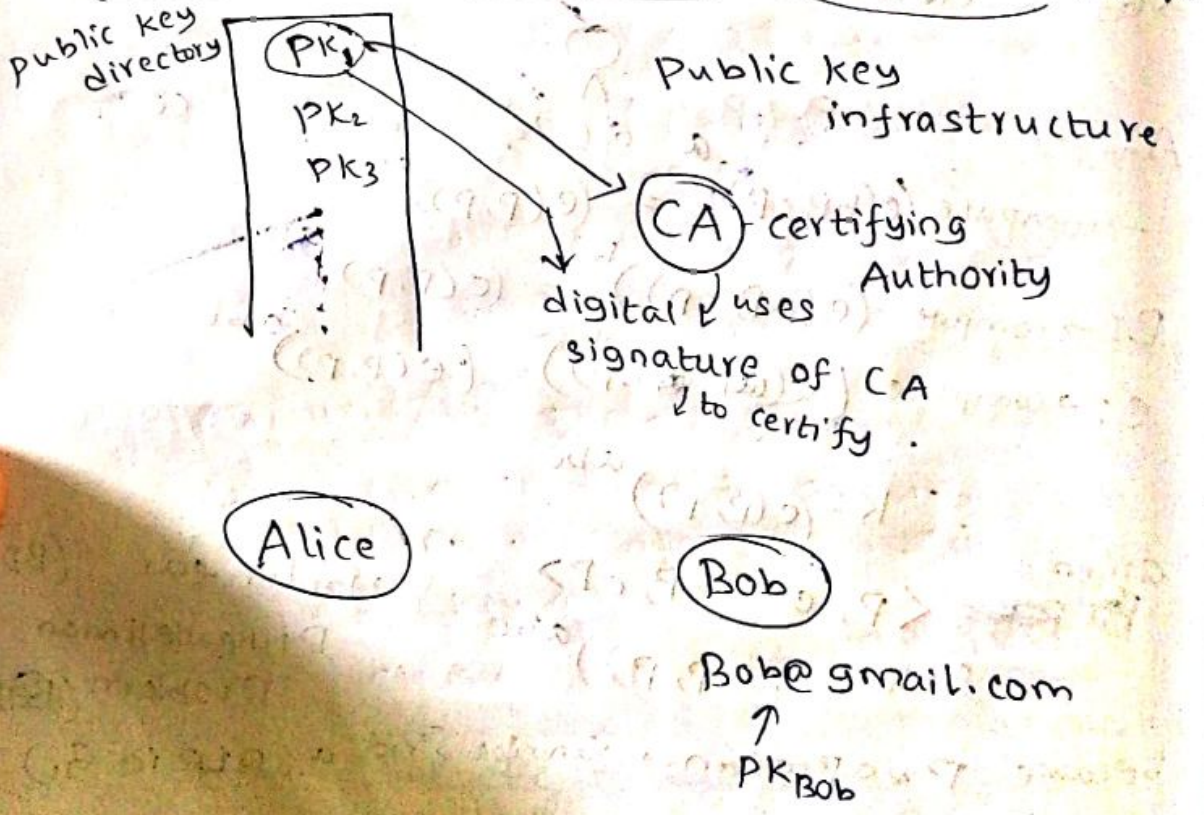
$e(P_1, P_2, \ldots, P_n)$. $n \geq 3$

Can achieve single round $(n+1)$-party key agreement.

* Application of Bilinear pairing :-

ID - based encryption → we can use our own id as public key unlike PK crypto

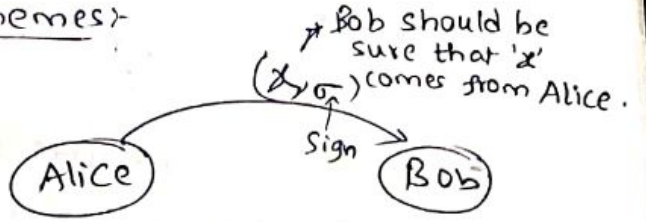
Public-key cryptosystem :-



→ Bonech - Franklin → IBE using pairing

* Digital Signature schemes:-

→ for Authentication.



→ Key Gen:→ PK, SK } Alice

→ Sign :- $(x, SK) \to \sigma$ } Alice

PK_{Alice}, SK_{Alice} PK_{Bob}, SK_{Bob}

→ Verification :-

$(x, \sigma, PK) \to 0/1$

(or) False/True } Alice

$\sigma = Sign(SK, x)$

$verif(x, \sigma, PK) = \begin{cases} true & \text{if } \sigma = Sign(SK, x) \\ false & \text{otherwise} \end{cases}$

→ RSA Signature Scheme

Key Gen:..

→ $n = pq$, p, q are large primes.

$\phi(n) = (p-1)(q-1)$

$SK = d, p, q$

$PK = n, e$

choose 'e' s.t.

$gcd(e, \phi(n)) = 1$

$\exists d$ st $ed \equiv 1 \pmod{\phi(n)}$

→ $x \in Z_n^*$

$Sign(x, \overset{d}{SK}) = x^d \bmod n = \sigma$

$Verification(x, \sigma, \underset{n,e}{PK}) = \sigma^e \bmod n$

$= x^{ed} \bmod n$

$= x^{k\phi(n)+1} \bmod n$

$= x \bmod n$

→ ElGamal Signature Scheme

→ p be a prime s.t. DLP is in Z_p is intractable.

$\alpha \in Z_p^*$ is a primitive element

$P = Z_p^*$ — Set of Possible ~~Plaintexts~~ messages

$\mathcal{A} = Z_p^* \times Z_{p-1}$ — Set of possible signatures

$K = \{(p, \alpha, a, \beta) \mid \beta = \alpha^a \bmod p\}$

$Sk = a$

$Pk = p, \alpha, \beta$

→ $\underline{Sign(x, \underset{a}{sk}) = (\gamma, \delta)}$

$x \in P$

Choose $k \in_R Z_{p-1}^*$ ~~Set~~

↑ Randomly.

Set $\gamma = \alpha^k$, $\delta = (x - a\gamma) k^{-1} \pmod{(p-1)}$.

→ $\underline{Verification(x, \sigma = (\gamma, \delta), Pk)}$

$$Verif._{(x,\sigma,Pk)} = \begin{cases} true, & \text{if } \beta^\gamma \gamma^\delta = \alpha^x \bmod p. \\ false, & \text{otherwise} \end{cases}$$

* Security in this scheme

→ Oscar tries to forge a signature (γ, δ) for a given message x, without knowing the secret key 'a'.

→ Oscar chooses 'γ' and then tries to find the corresponding δ..

s.t. $\beta^\gamma \gamma^\delta = \alpha^x \bmod p$

$\Rightarrow \gamma^\delta = (\alpha^x)(\beta^\gamma)^{-1} \bmod p$

$\delta = \log_\gamma (\alpha^x \beta^{-\gamma}) \bmod p$

↓ Hard

(or)

→ Oscar first chooses 'δ' and then tries to find γ.

$\Rightarrow \beta^{\gamma} \cdot \gamma^{\delta} = \alpha^{x} \bmod p$ for unknown γ.

→ Random value 'k' used in computing signature, should not be revealed.

'k' known ⇒ 'a' known ⇒ System broken (from δ)

→ Same value of 'k' in signing two different messages makes it easy for oscar to compute 'a' & hence breaks the system.

~~Verification~~

→ suppose x_1, x_2 are two different messages

$\text{Sign}(x_1, sk) = (\gamma, \delta_1)$ $\quad [\gamma = \alpha^k]$

$\text{Sign}(x_2, sk) = (\gamma, \delta_2)$

~~$\delta_1 = x - a$~~

$\delta_1 = (x_1 - a\gamma) k^{-1} \bmod (p-1)$

$\delta_2 = (x_2 - a\gamma) k^{-1} \bmod (p-1)$

$\Rightarrow \beta^{\gamma} \gamma^{\delta_1} = \alpha^{x_1} \bmod p$

$\beta^{\gamma} \gamma^{\delta_2} = \alpha^{x_2} \bmod p$

$\Rightarrow \gamma^{\delta_1 - \delta_2} = \alpha^{(x_1 - x_2)} \bmod p$

$\alpha^{k(\delta_1 - \delta_2)} = \alpha^{(x_1 - x_2)} \bmod p$

$\Rightarrow \boxed{k(\delta_1 - \delta_2) = (x_1 - x_2) \bmod (p-1)}$

~~$k = (x_1 - x_2)(\delta_1 - \delta_2) \bmod (p-1)$~~

$ax \equiv b \pmod n$ — only k is unknown.

$d = \gcd(p-1, \delta_1 - \delta_2)$

If $d \mid (x_1 - x_2)$, then 'd' many k's exist

otherwise no solution

$\Rightarrow k\left(\frac{\delta_1 - \delta_2}{d}\right) \equiv \left(\frac{x_1 - x_2}{d}\right) \bmod \left(\frac{p-1}{d}\right)$

i.e $k\delta' \equiv x' \pmod{p'}$ → has unique soln. & $\gcd(\delta', p') = 1$

$\Rightarrow k = x'(s')^{-1} \bmod p'$

$k = x' \epsilon \bmod p'$ where $\epsilon = (\delta')^{-1} \bmod p'$

We get 'd' candidates for k;

$k = (\epsilon x' + ip') \bmod (p-1)$

$0 \le i \le d-1$

Find correct 'k' by checking if $\gamma = \alpha^k \bmod p$

$\Rightarrow$ from k, 'a' can be known.

* The Digital Signature Standard (DSS):-

Shorter signature to implement in smart cards. ↓ Sign. size = 170 bit

$P \rightarrow$ 512 bit prime s.t. DLP is hard in Z_p

$q \rightarrow$ 160 bit prime s.t. $q \mid (p-1)$.

$\alpha \in Z_p^*$ be a q-th root of unity mod p.

$\alpha = \sqrt[q]{1} \bmod p$

i.e $\alpha^q \equiv 1 \bmod p$.

Setup:-

$\mathcal{P} = Z_p^*$, $\mathcal{A} = Z_q \times Z_q$.

$K = \{(p, q, \alpha, a, \beta) \mid \beta = \alpha^a \bmod p\}$

$Pk = (p, q, \alpha, \beta)$, $Sk = a$, $0 < a < q$

Sign:-

choose $k \in Z_q^*$

compute $\gamma = (\alpha^k \bmod p) \bmod q$.

& $\delta = (x + a\gamma) k^{-1} \bmod q$

$\therefore Sign(x, sk) = (\gamma, \delta)$.

Verification:

Verify(pk, x, (γ, δ)) = { true, if ① holds; false, otherwise

compute $e_1 = x\delta^{-1} \bmod q$

$e_2 = \gamma\delta^{-1} \bmod q$

check if $(\alpha^{e_1}\beta^{e_2} \bmod p) \bmod q = \gamma \longrightarrow ①$

$\alpha^{e_1}\beta^{e_2} = \alpha^{x\delta^{-1}} \cdot \alpha^{a\gamma\delta^{-1}} = \alpha^{(x+a\gamma)\delta^{-1}} \bmod q$

$\alpha^{e_1}\beta^{e_2} \bmod p = \alpha^{k} \bmod p$

$(\alpha^{e_1}\beta^{e_2} \bmod p) \bmod q = (\alpha^{k} \bmod p) \bmod q = \gamma.$

* Boneh-Lynn-Shacham [2001] (BLS) signature:-

→ Same level of security as 320-bit DSS (or) DSA

→ uses Bilinear pairing.

Key Gen:-

G_1, G_2 → two groups of large prime order

$|G_1| = |G_2| = q$, DLP is hard in both G_1, G_2.

$e: G_1 \times G_1 \longrightarrow G_2$

G_1 → additive

G_2 → multiplicative

$G_1 = \langle P \rangle$ (P has two co-ordinates)

Hash func^n → $H: \{0,1\}^* \longrightarrow G_1$

$sk = s \in Z_q^*$

$pk = sP$,

Param = (P, G_1, G_2, H, e, q)

Sign:-

$\sigma = Sign(x, sk)$ (Param,) = x-coordinate of S.

message $x \in \{0,1\}^*$, $Q = H(x) \in G_1$, $S = sH(x)$

Verify:-

Verify(pk, x, σ) (Param,) → true

If valid: find a point $S \in G_1$ with x-coordinate σ, if no such point, reject the signature as invalid. Otherwise check whether $\langle P, pk, Q, \pm S \rangle$ is a valid DH-tuple (Diffie-Hellman tuple).

It is a valid DH tuple, if

$$e(P, \pm S) = e(pk, Q).$$

P ; $\pm sH(x)$; sP ; $H(x)$

$$e(P, sH(x)) = e(P, H(x))^s \qquad e(sP, H(x)) = e(P, H(x))^s$$

$Q = H(x) \in G_1 = tP$ (say)

$\Rightarrow$ DH tuple is $\langle P, sP, tP, \pm stP \rangle$

The group G_1 here is a GaP DH group

$\Downarrow$

Decisional DH problem → easy

but Computational DH problem → hard

Given $\langle g, g^a, g^b, g^c \rangle$ check if $c = ab$

(or) $\langle P, sP, tP, rP \rangle$ check if $r = st$

$e(P, rP) \stackrel{?}{=} e(sP, tP)$

$\Leftrightarrow e(P,P)^r \stackrel{?}{=} e(P,P)^{st}$

$\Leftrightarrow r \stackrel{?}{=} st$

Given $\langle g, g^a, g^b \rangle$ compute g^{ab}

(or) $\langle P, aP, bP \rangle$ compute abP

→ Security :- CDH hard

Computational Diffie Hellman problem.

* Sakai-Ohgishi-Kasahara [2000] key Agreement:

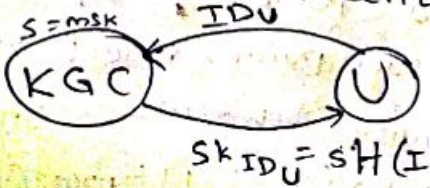
Public key of user $U \rightarrow ID_U \in \{0,1\}^*$

Setup:

$|G_1| = |G_2| = q$ $\quad \langle G_1, G_2, e, P, q, H \rangle$ = params, $pk = sP$

msk = master secret key $= s \in Z_q^*$

KGC = key Generation Centre.



Alice

$ID_{Alice}(ID_A) \to PK_A$

$SK_{Alice}(SK(ID_A))$.

$e(H(ID_B), SK_{ID_A})$

$= e(H(ID_B), H(ID_A))^s$

Bob

$ID_{Bob}(ID_B) \to PK_B$

$SK_{Bob}(SK(ID_B))$

$e(H(ID_A), SK_{ID_B})$.

$= e(H(ID_A), H(ID_B))^s$

* $e: G_1 \times G_1 \to G_2$

$\Rightarrow e(P, Q) \in G_2$ if $(P, Q) \in G_1$

$G_1 \to$ elliptic curve group, $G_2 \to$ multiplicative group.

$\langle P, R = rP \in G_1 \rangle$ find $r \to$ DLP in G_1

$\beta = e(R, P) = e(rP, P) = e(P, P)^r = \alpha^r \to$ find r

$\Downarrow$

DLP in G_2.

* Theorem:-

Let $E[m]$ be the m-torsion subgroup of an elliptic curve E/F_q where $q = p^m$ for some prime p and $m \mid \#E/F_q$;

$\gcd(m, q) = 1$ and $m \nmid (q-1)$, then $|E[m]| = m^2$

Let k be the smallest +ve integer s.t.

$m \mid q^k - 1$. ($k \to$ embedding degree of the curve)

and $e_m: G_1 \times G_2 \to F_{q^k}^*$ be a pairing with

$\to O(G_1) = m = O(G_2)$. ($\to$ size)

$\to G_1$ is a cyclic subgroup of $E[m]$

$\to G_2$ is a cyclic subgroup of E.

$E = E/\bar{K}$, $\bar{K} = \bigcup_{i \geq 0} F_{q^i}$

$\to$ No efficiently computable isomorphism between G_1, G_2 (Type-3 pairing).

Then, e_m satisfies all the properties of Bilinear pairing discussed earlier.

* ~~BLS~~ - short signature

* BLS signature

→ Pros:

→ short sized (160-bit)

→ Cons:

→ security depends on the hardness of CDH problem.

→ secure under ROM (Random Oracle Model)

↘ Having a Hash function like a blackbox.

$m \in P \rightarrow H(m) \in G_1$

* Boneh - Boyen signature (without ROM):

(BB signature).

→ Setup:-

→ Bilinear group setup.

$e: G_1^2 \longrightarrow G_2 \quad [G_1 \times G_1 \rightarrow G_2]$

G_1 → additive grp

G_2 → multi group

$G_1 = \langle P \rangle, \quad |G_1| = |G_2| = q$

Choose $(x, y) \in Z_q^{*2}$

$U = xP$

$V = yP$

$Sk = (x, y)$; $PK = (U, V)$, params → $\langle G_1, G_2, e, q, P \rangle$

→ Sign :-

$m \in Z_q^*$ = message space

Randomly choose $r \in Z_q^*$

compute σ

$\text{Sign}(m, sk=(x,y)) = \left\{ \frac{1}{x+ry+m} P \right.$

If inverse doesn't exist, choose another 'y'.

In BLS, this multiple comes from Hash function ⇒ all trust is bestowed with Hash func^n

$\therefore \text{sign}(m, sk=(x,y)) = (r, \sigma)$

→ Verify :

$$\text{verify}(m, (r,\sigma), pk) = \begin{cases} \text{true}, & \text{if } e(\sigma, U+rV+mP) = e(P,P) \\ \text{false}, & \text{otherwise} \end{cases}$$

calculate $e(\sigma, U+rV+mP)$

$= e\left(\frac{1}{x+ry+m} P, (x+ry+m)P\right)$

$= e(P,P)^{\frac{1}{x+ry+m} \cdot (x+ry+m)}$

$= e(P,P).$

~~* BB-signature~~

* BB signature is secure without ROM under the k-strong DH assumption in G_1.

Instance :- $\langle P, yP, y^2P, \ldots, y^kP \rangle$

for a random $y \in Z_q^*$

output :- $\left(c, \frac{1}{y+c} P\right)$ where $c \in Z_q^*$

* Water's signature (without ROM, CDH assumption)

CDH problem is hard in the underlying group.

→ Setup

params = $\langle G_1, G_2, e, P, g \rangle$

G_1, G_2 → both multiplicative

$G_1 = \langle g \rangle$, $|G_1| = |G_2| = P$

$e : G_1^2 \rightarrow G_2$

$\Rightarrow e(g^a, g^b) = (e(g,g))^{ab}$

$\rightarrow g_1 = g^\alpha$, $\alpha \in_R Z_p^*$ (Randomly)

$\rightarrow g_2, f', f_1, f_2, \ldots, f_n \in_R G_i$

$\rightarrow sk = g_2^\alpha$; $vk = \langle params, g_1, g_2, f', f_1, f_2 \ldots, f_n \rangle$ (verification key)

Sign :-

message $M = M_1 M_2 \ldots M_n$

$M_i \in \{0,1\}$

let $S = \{i \in [n] \mid M_i = 1\}$ $\quad [n] = \{1, 2, \ldots, n\}$

choose $r \in_R Z_p^*$

$\sigma = \langle sk \cdot (f' \prod_{i \in S} f_i)^r , g^r \rangle$ ($sk = g_2^\alpha$)

Verify :-

Verify $(M, \sigma_M = (\sigma_1, \sigma_2), vk)$

check if $e(\sigma_1, g) = e(g_1, g_2)\, e(f' \cdot \prod_{i \in S} f_i , \sigma_2)$

$e(\sigma_1, g) = e\left(g_2^\alpha (f' \prod_{i \in S} f_i)^r , g_2 \right)$

$= e(g_2^\alpha, g)\, e\left((f' \prod_{i \in S} f_i)^r , g \right)$

[$\because$ In additive grp, $e(P+Q, R) = e(P,R) e(Q,R)$
$\Rightarrow$ In mult-grp, $e(PQ, R) = e(P,R) e(Q,R)$]

$= e(g_2, g^\alpha)\, e\left(f' \prod_{i \in S} f_i , g^r \right)$

$= e(g_2, g_1)\, e\left(f' \prod_{i \in S} f_i , g^r \right)$ ✓

Public key Director

→ Cons for Water's signature:-

→ VK size is very large → linear in the size of message

* Identity-Based Encryption :-

→ identity of individual user is the public key.

→ Trusted third party

→ KGC (key Generation centre)

or

→ PKG (private key Generator).

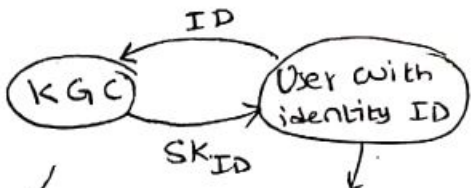
* Setup:

→ public parameters (params) are generated.

* Key Extract:

PK = ID

SK = SK_{ID}



When ID is given, it is thoroughly verified to confirm it's the same person (like documents etc..)

first goes through a registration phase to avail membership in KGC

→ Public key Encryption Vs. ~~ID-based encryption~~

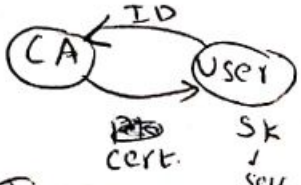
→ PK, SK generated during the setup phase

→ public key certificate is used (CA (certifying Authority))

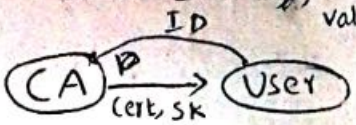
→ PK → ~~Center~~ certificate contains a signature of CA on the public key.

Certificate = (PK, Sign(PK), time of validity)

(or) another method is



Public key Directory



Vs. ID-Based encryption

→ No need to maintain a public key directory.

~~Shamir~~

* ID-based encryption (IBE):

→ Shamir → first IBE & IBS (ID-Based Signature) (crypto 1984)

→ Boneh & Franklin (crypto 2001)

→ using bilinear pairing

→ IBE (in ROM)

Random Oracle Model

→ Sakar, Ohgishi, Kasahara (2000)

→ ID-Based key Agreement & IBS.

→ Boneh, Boyen (Eurocrypt 2004)

→ IBE (without ROM).

* Boneh Franklin's IBE (in ROM)

params = $\langle G_1, G_2, q, e, P, P_{pub}, H, n, H_1 \rangle$

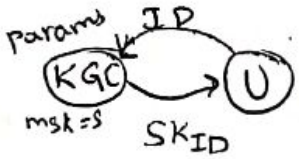
n message = n-bit string

$|G_1| = |G_2| = q$, DLP is hard in both G_1, G_2.

G_1 → additive group

G_2 → multiplicative group

$e: G_1^2 \longrightarrow G_2$



$G_1 = \langle P \rangle$

$P_{pub} = sP$, $msk = s$

master secret key

$H: \{0,1\}^* \longrightarrow G_1$ $\quad H_1: G_2 \longrightarrow \{0,1\}^n$

$M = \{0,1\}^n$

message.

Key Extract:

$(ID, msk) \rightarrow SK_{ID}$

$H(ID) \in G_1$

$SK_{ID} = sH(ID) \rightarrow$ BLS signature on ID.

Encryption:

$(m, ID) \rightarrow C$

$m \in \{0,1\}^n$

choose $r \in Z_q^*$

then $C = \left(rP, m \oplus H_1\left(e\left(H(ID), P_{pub}\right)^r\right)\right)$

Decryption:

Decrypt (C, SK_{ID})

(C_1, C_2)

$e\left(P_{pub}^{sP}, H(ID)\right)^r = e\left(sP, H(ID)\right)^r$

$= e(rP, sH(ID))$

$= e(C_1, SK_{ID})$

Final output,

$m = C_2 \oplus H_1\left(e(C_1, SK_{ID})\right)$.

Security:

Given $\langle P, rP, P_{pub}, H(ID)\rangle$

$P_{pub} = sP$, $H(ID) = tP$ (say)

calculate $e\left(P_{pub}, H(ID)\right)^r$

$= e(sP, tP)^r$

$= e(P, P)^{rst}$

Joux key agreement prob

BDH (Bilinear DH) problem, given

given $\langle P, aP, bP, cP\rangle$, to calculate $e(P, P)^{abc}$

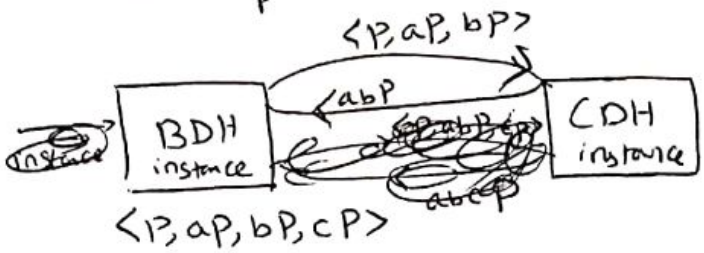
Theorem:

* BDH problem is no harder than CDH problem.

CDH problem (computational DH) in $G_1 = \langle P \rangle$:

given $\langle P, aP, bP \rangle$ → calculate abP.

i.e $BDH \leq_p CDH$



$\downarrow$

$e(abP, cP) = e(P, P)^{abc}$

* Boneh-Boyen's IBE (without ROM):-

Key Extract:-

$SK_{ID} = \left(r, \frac{1}{x + ry + ID} P\right)$ $(r \in_R \mathbb{Z}_q^*)$

↓

Boneh-Boyen's signature

Setup:-

$Params = \langle G_1, G_2, q, P, P_{pub} \rangle$

$P_{pub} = (U = xP, V = yP)$

$msk = (x, y)$.

Encrypt:-

$(ID, M) \rightarrow C$

$M \in G_2$, message

choose $s \in Z_q^*$

$C = (s \cdot ID \cdot P + sU, sV, e(P, P)^s M)$.

Decrypt $(C, SK_{ID}, Params) \rightarrow M$:

(C_1, C_2, C_3)

Calculate $e(C_1 + rC_2, \frac{1}{x+ry+ID} P)$

$= e(s.ID.P + sU + rsV, \frac{1}{x+ry+ID} P)$

$= e(sP(x+ry+ID), \frac{1}{x+ry+ID} P)$.

$= e(sP, P) = e(P, P)^s$

→ Problem in this setup:

→ Key Generation Centre is heavily trusted

↳ with msk, it can decrypt every cipher text.

↓

called key escraw.

KGC is a single point failure → if it is corrupted, everything's gone.

avoiding → by Threshold system

↓

makes a single point failure to a t-point failure

i.e n KGS's ⇒ t KGC's should come together to get msk.

→ Security:

→ Non-standard hardness assumption.

Instance:- $\langle P, yP, y^2P, \ldots, y^kP, r \rangle$ $G_1 = \langle P \rangle$

for some $y \in Z_q^*$ & $r \in_R G_2$.

output yes if $r = e(P,P)^{1/y} \in G_2$,

NO otherwise.

K-Decisional Bilinear DH Inversion (K-DBDHI) in (G_1, G_2, e)

→ security is little lower.

* SPN
  - DES → different S-boxes
  - AES → same S-box

* Ceaser Cipher
$y = (x+3) \bmod 26$

* Shift Cipher
$y = (x+k) \bmod 26$
$P = Z_{26} = C = K$

* Affine Cipher
$y = (ax+b) \bmod 26$
$P = C = Z_6$
$(a,b) \in Z_{26}^* \times Z_{26}$
$x = a^{-1}(y-b) \bmod 26$

* Substitution Cipher
$C = \{A, B, C, \ldots, Z\}$
$P = \{a, b, \ldots z\}$
K = Set of permutations of the 26 letters

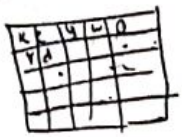
If Φ is a permutation of a-z
$e_\Phi(x) = \Phi(x)$
$d_\Phi(y) = \Phi^{-1}(y)$

* Vigenere Cipher
$P = C = Z_{26}^m = K$
let $\underset{\sim}{K} = (k_1, k_2, \ldots k_m) \in K$
$e_{\underset{\sim}{K}}(\underset{\sim}{x}) = (\underset{\sim}{x} + \underset{\sim}{K}) \bmod 26$

* Hill Cipher
$P = C = Z_{26}^m$
$K = m \times m$ invertible matrix $\bmod 26$
$X \rightarrow r \times m$ matrix of plaintext
$Y \rightarrow r \times m$ matrix of ciphertext
$Y = XK$
$X = YK^{-1}$

* Transposition / permutation Cipher
$P = C = (Z_{26})^m$
K = Set of permutations of $\{1, 2, 3, \ldots, m\}$
for each $\pi \in K$
$e_\pi(\underset{\sim}{x}) = \{x_{\pi(1)}, x_{\pi(2)} \ldots x_{\pi(m)}\}$
$d_\pi(\underset{\sim}{y}) = \{y_{\pi^{-1}(1)}, y_{\pi^{-1}(2)} \ldots y_{\pi^{-1}(m)}\}$

* Playfair cipher



* Autokey Cipher
$P = C = K = Z_{26}$
$K_1 = k$, $K_i = x_{i-1}$ $\forall i > 1$
$e_K(x_i) = (x_i + K_i) \bmod 26$
$d_K(y_i) = (y_i - K_i) \bmod 26$