Principles of security:

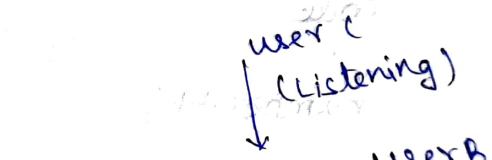
* Confidentiality
* Authenticity
* Integrity

To overcome CIA, there should be no

* Interception
* Modification
* Fabrication

* Availability
* Access control
* Attacks
  (i) Criminal
  (ii) Publicity
  (iii) Legal

Attacks
→ passive
→ active
(eg) DOS



(Passive attacks)

Registers:

* General purpose registers
  (i) EAX accumulator
  (ii) EBX base / offset
  (iii) ECX counter
  (iv) EDX data

* segment
  - → CS counter segment
  - → DS data segment
  - → SS stack segment

* control register:
  - → EIP - next instruction
  - → EEP - extended

Every program will have,
* text → read only
* Data } - Global / static variables
* BSS }

* Heap - FIFO
* Stack - LIFO

Dynamic register allocation - we use heap or stack

To define word in assembly: dw

(eg)
```
int number;
...
code
...
number++;
```

```
number dw 0;
...
...
mov eax, number;
inc eax;
mov number, eax;
```

```
int number;
if(number < 0) {
    ...
}
```

```
number dw 0;
mov eax, number;
or eax, eax;
jge label;
<No code>

label
<Yes code>
```

Debugging:

b main - stops after main
b - stops in current line
b N - stops after N line
r - run till the first occurence of break point

s - same as next if it is a block, it moves to next block

next - moves to next line

bt into b - list all break points

Buffer:

* Temporary storage, * fast processing

cryptology:

* study of cryptography
* plain text - human readable
* cipher text - unreadable form

Encryption: technique to convert plain to cipher text

Decryption: technique to convert cipher to plain text

Substitution:

Ceasor cipher:

$C = (P, k)$

$cipher = (P+K) \bmod 26$

$P = (C, K)$

$P = (C-K) \bmod 26$

(For ceasor cipher, K = 3)

(eg): PF Meet Me

CT = PHHW PH } (k=3)

P : Nishant is a friend of Antony

C.T = QLVKDQW LV D IUL#QG RI DQWRQB

Hint

P.T

C.T = GEXX EQQEX SF GI [DBUUBNLBU]

P.T = DBUUBNNBUP CDR

2/09/22

Monoalphabetic cipher:

* We take random key for substitution

Plain text = C I P H E R

Cipher text = L V Z S I T

26 ways, 25 ways (since I is taken)

Let S = {a, b, c},

there are 3! arrangements we can make

* Better than Caesar cipher

Playfair cipher:

key: A P P L E

A	P	L	E	B
C	D	F	G	H
I/J	K	M	N	O
Q	R	S	T	U
V	W	X	Y	Z

P.T

C.T

A	T	T	A	C	K
E	Q	Q	E	D	I

* Break P.T into text with 2 characters.
* Suppose if P.T is of odd length

Rules:

* Same row →
* same column ↓
* Rectangle square swap

P.T	E	N	C	R	Y	P	T	I	O	N
C.T	G	T	D	Q	W	E	Q	N	I	O

Hill cipher : (1929)

*using mathematical operation.

$C.T = P.T \times K \bmod 26$

$P.T = C.T \times K^{-1} \bmod 26$

$K = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$

P.T = H E L P

$C.T = [7 \quad 4] \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} = [21+8 \quad 21+20] \bmod 26$

$= [29 \quad 41] \bmod 26$

$= [3 \quad 15]$

C.T = D P (for first two characters)

$C.T = [11 \quad 15] \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} = [33+30 \quad 33+75] \bmod 26$

$= [63 \quad 108] \bmod 26$

$= [11 \quad 4]$

C.T = L E

$\Rightarrow$ C.T = D P L E

Decryption:

$$P.T = C.T \times K^{-1} \bmod 26$$

$$K^{-1} = \frac{1}{|K|}(adj\ K)$$

$$K = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \Rightarrow K^{-1} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

$$\therefore K = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$$

$$adj(K) = \begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix}$$

$$|K| = 15 - 6 = 9$$

$$K^{-1} = \frac{1}{9}\begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix}\begin{bmatrix} 3 & 15 \end{bmatrix} \bmod 26$$

$$= 3\begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix}\begin{bmatrix} 3 & 15 \end{bmatrix} \bmod 26$$

$$9 \times (x) \bmod 26 = 1$$

$$= \begin{bmatrix} 15 & -9 \\ -6 & 9 \end{bmatrix}\begin{bmatrix} 3 & 15 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 75 & -135 \\ -18 & 135 \end{bmatrix} \bmod 26$$

$$= 3\begin{bmatrix} 3 & 15 \end{bmatrix}\begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} -75 & 198 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 49 & 198 \end{bmatrix} \bmod 26$$

3. $\begin{pmatrix} 5 & 23 \\ 24 & 3 \end{pmatrix}$ $\begin{pmatrix} 15 & -9 \\ -6 & 9 \end{pmatrix} \bmod 26$

5) Polyalphabetic cipher

$$C_i = (P_i + K_i) \bmod 26$$

key = D e c e p t i v e D e c

P.T = P a y o n c e m o r e

∴ If P.T is larger than key, repeat key until it becomes equal to P.T.

(D, P) ⇒ (3 + 15) % 26 = 18 ⇒ S

(e, a) ⇒ (4 + 0) % 26 ⇒ 4 ⇒ E

Instead of repeating key when it's size is smaller than P.T, we can repeat P.T in key so that it will be easy to decipher.

6) Vernam cipher:

$$C_i = P_i \oplus K_i$$

One time pad:

Same as polyalphabetic cipher but here we use a key only once.

Transposition

Rail fence:

Depth = 2

Plain text = Attack at once

A		t		c		a		o		c	
	t		a		k		t		n		e

C.T = Atcaoctaktne

depth = 3

A			a			a			n	
	t			c			t			e
		t			k			o		

C.T = A a a n t c t c t k o e

depth = 3

A				c				o		
	t		a		k		t		n	e
		t				a				

C.T = A c o t a k t n e t a c

Row column transposition:

* we have to ~~read~~ till in rows & while reading use columns. Also, the columns are read based on priority.

* If any empty cells are there, fill it with any characters.

P.T = Attack at once

	0	1	2	3
0	A	t	t	a
1	c	k	a	t
2	o	n	c	e

col 0 → 2
col 1 → 1
col 2 → 3
col 3 → 4

C.T = t k n a c o t a c a t e

Decryption:

key = MONARCHY

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

RS | SR | DE
⇒ ATTACK

ON | TS | ML
⇒ MOSQUE

key = CEASAR

C	A	E	S	R
B	D	F	G	H
I/J	K	L	M	N
O	P	Q	T	U
V	W	X	Y	Z

NT | MQ | KO | QP
⇒ MULTIPLE

RL | AC | NT | OM | UE
⇒ ENCRYPTION

Sample space (S):
set of all possible events

Deck of cards → 52
Toss a coin {H, T} → 2

Event (E):
the occurrence of action in the sample space.

*favourable event
*non-favourable event

↳ probability number of times a favourable event occurs.

$\frac{m}{n}$ — m — event, n — sample space

$\frac{u}{n}$ —

Addition:

$P(A \cup B) = P(A) + P(B) - P(A \cap B)$ → for dependent event

$P(A \cup B) = P(A) + P(B)$ → for independent event

Binomial:

P(occurence / success) = p

P(not occurence / failure) = 1 - p

Binomial distribution = $p^k (1-p)^{n-k}$

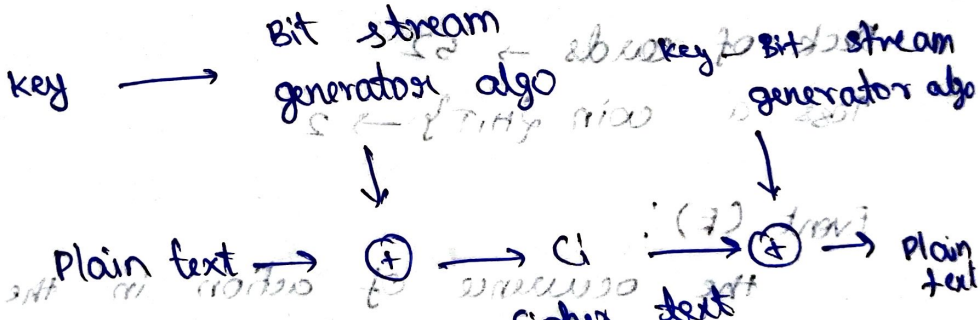
DES algorithm (Data Encryption Standard)

* based on symmetric algorithm

* stream cipher:
  - change P.T to C.T character by character

* block cipher:
  - change PT to CT block by block
  - minimum 64 bits / 8 bits

DES → Feistel block structure



* mapping
  - → reversible (eg) ceasar cipher)
  - → irreversible

Eg for irreversible:

P.T	C.T
00	10
01	11
10	00
11	01

here 01 & 11 is mapped to 11. so it requires 2^n combination to identify

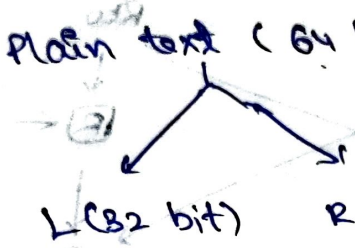
* Firstl block structure - idle block structure

* Concepts used in firstl block structure :

→ Diffusion ⇒ ~~substitution~~ Transposition

→ confusion ⇒ ~~Transposition~~ Substitution

* steps followed in DES encryption



→ every 8th bit is removed from key

→ initially key is 64 bit after removing parity it becomes 56 bits

eg. 1 2 3 4 5 6 7 8

16

24

(remove 8, 16, 24 ..)

64 bit plain text

↓ ↓ ↓ ↓

Initial permutation

↓ 64

Round 1

↓ 64

Round 2

:

Round 16

↓

32 bit swap

↓

Cipher text

* Initially DES is impossible to crack but later it becomes possible so we move to AES.

12/09/2022

AES (Advance Encryption Standard)

Plain text (128 bits)

↓ ↓ ↓

Add round key

↓

Sub bytes
S-box

↓

shift + Row

↓

Column multiplication

↓

Add round key

* Repeat the same process for 9 rounds.
* For the 10th round (last round) column multiplication is not used.

State array [Intermediate array]

↓

$$S = \begin{bmatrix} s_{0,0} & s_{0,1} & \cdot & \cdot \\ s_{1,0} & s_{1,1} & \cdot & \cdot \\ s_{2,0} & s_{2,1} & \cdot & \cdot \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{bmatrix}$$

↓

$$\Rightarrow O/P = \begin{bmatrix} 0_0 & \cdot & \cdot & \cdot \\ 0_1 & \cdot & \cdot & \cdot \\ 0_2 & & & \\ 0_3 & & & \end{bmatrix}$$

Add round key:
Intermediate text ⊕ key ⇒ [ ] → Round 2

For each row, we use different round key.

Root word:

	72	69	6e	67
x_1	69	6e	67	72
S-box y_1	f9	9f	85	40

Round const

$[R_1 \longrightarrow R_{10}]$

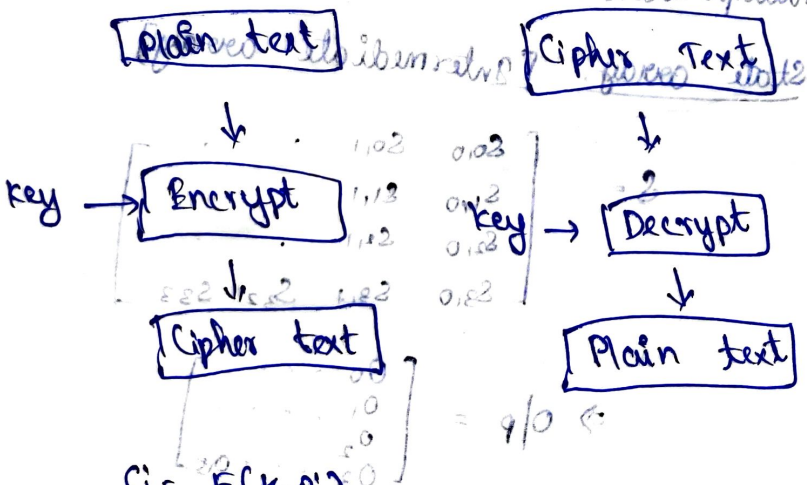
$$\begin{bmatrix}01\\00\\00\\00\end{bmatrix}\begin{bmatrix}02\\00\\00\\00\end{bmatrix}\cdots\cdots\begin{bmatrix}36\\00\\00\\00\end{bmatrix}$$

$$\Rightarrow g(w_3) = \begin{pmatrix}f9\\9f\\85\\40\end{pmatrix} \oplus \begin{pmatrix}01\\00\\00\\00\end{pmatrix}$$

14/09/2022

Block cipher mode:

* Electronic code book



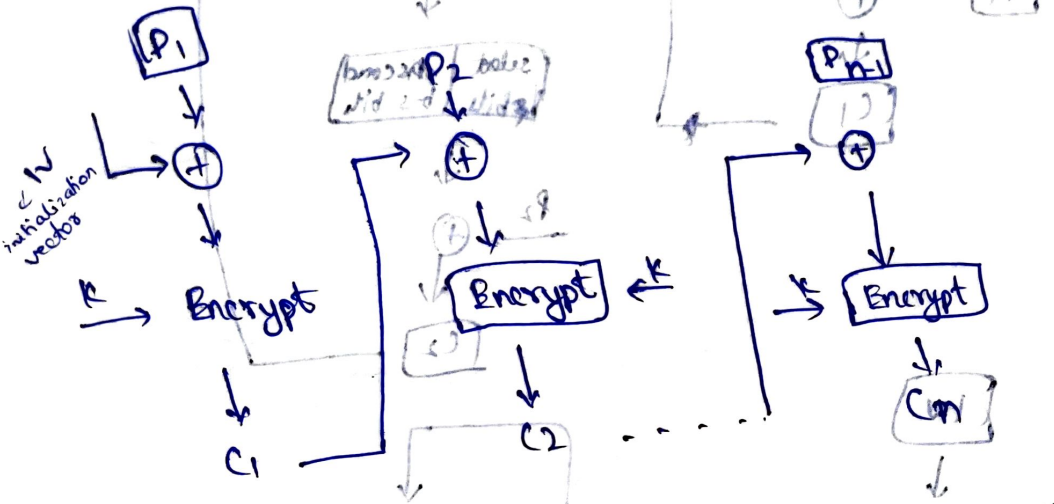
$C_i = E(K_i, P_i)$

$P_i = D(K_i, C_i)$

Other attributes that needed to be maintained while we move to other algorithms.

* Overhead.
* Error recovery propagation
* Error
* Diffusion
* Security

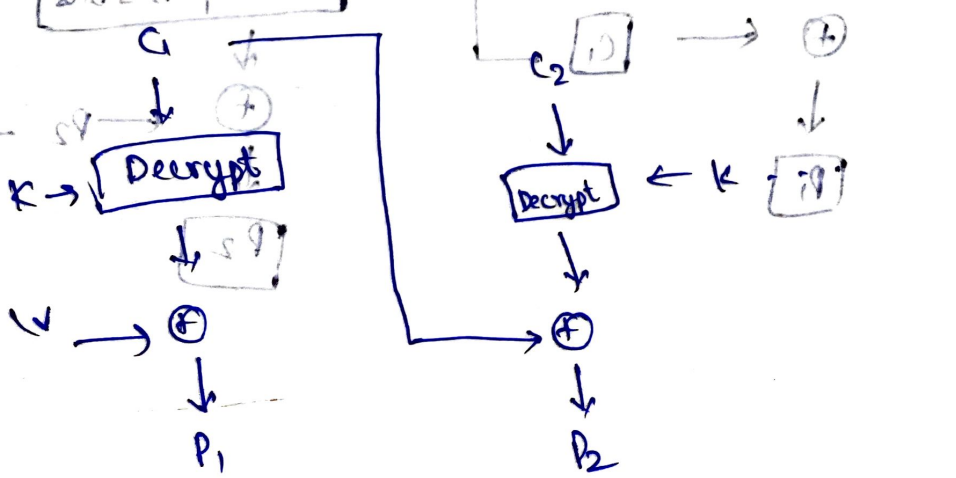
Cipher block chaining mode



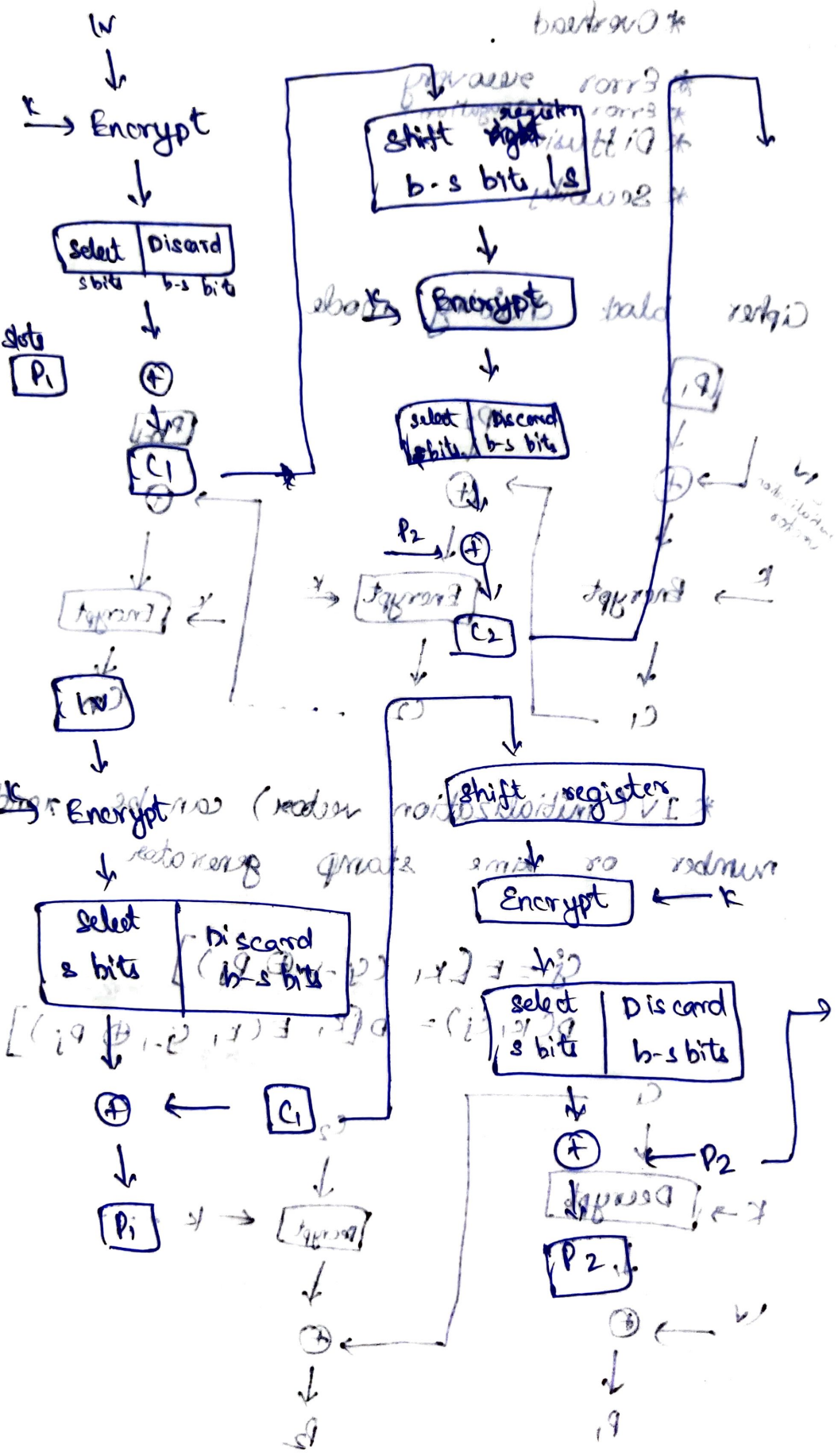
* IV (initialization vector) can be random number or time stamp generator

$C_j = E[K, (C_{j-1} \oplus P_j)]$

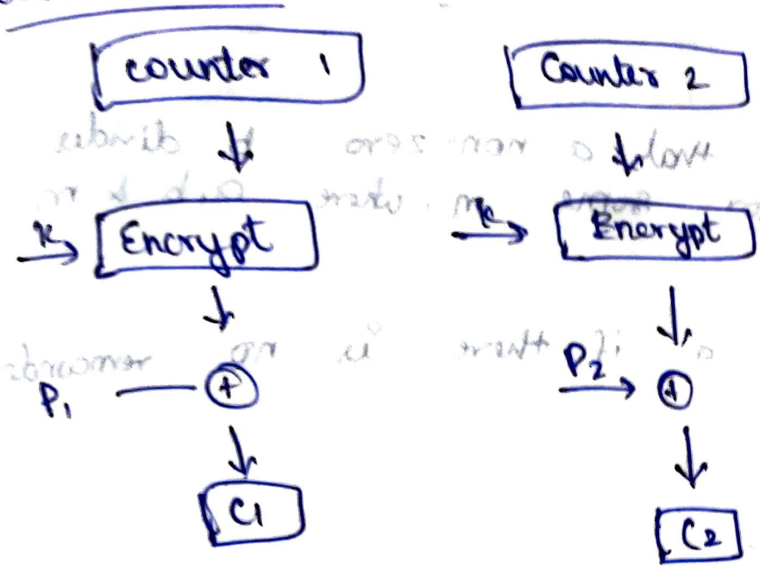
$D(K, C_j) = D[K, E(K, C_{j-1} \oplus P_j)]$



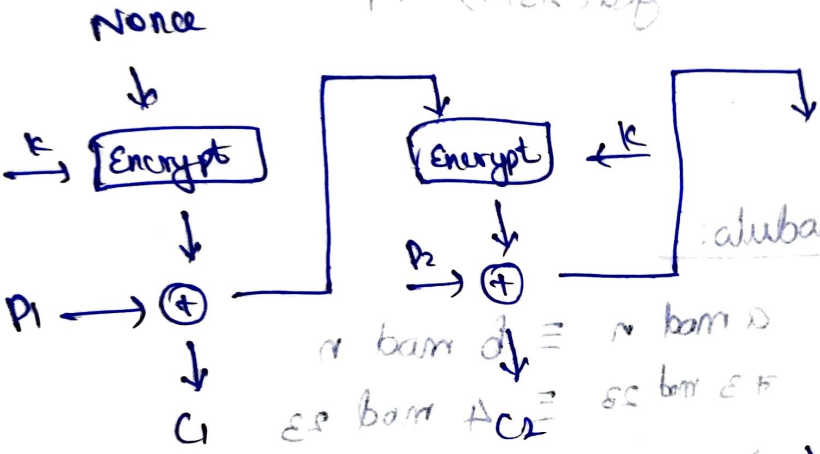
3) Cipher feedback mode



Counter Mode:



Output feedback mode:



Counter mode: (cont)

* Encryption & decryption can be done must faster.
* can be performed in parallel manner

Padding:

sample - 10^*

Multirate - $10^* \ldots 1$

20/09/2022 Number Theory

Divisibility:

* We say that a non-zero b divides a if $a = mb$ for some integers a, b & m where m is also an integer.

* b divides a if there is no remainder on division.

Prime: 2, 3, 5, 7 ...

Relative prime: gcd of two nos is 1 then those nos are relative prime. (2, 3, 4)

$\gcd(2,3,4) \rightarrow 1$

Modulo:

Congruent modulo:

$a \bmod n \equiv b \bmod n$

$3 \bmod 23 \equiv 4 \bmod 23$

Divisibility properties:

* $a \mid 1$, then $a = \pm 1$
* $a \mid b$, and $b \mid a$ then $a = \pm b$
* Any $b \neq 0$ divides 0
* $a \mid b$, $b \mid c$ then $a \mid c$
* $b \mid g$ & $b \mid h$ then $b \mid (mg + nh)$ for arbitrary integer m & n.

Division algorithm:

*Given any positive integer a and any non negative integer a, if we divide

GCD:

*largest integer that divides both a & b.

1) gcd(42345, 43215)
2) gcd(3486, 10298)
3) gcd(75, 32)
4) gcd(117, 218)

3) ~~75 = 75 · 32 ≠ xy~~

75 = 2×32 + 11

32 = 2×11 + 10

11 = 1×10 + 1

10 = 10×1 + 0

gcd(75, 32) = 1

4) 218 = 1×117 + 101

117 = 1×101 + 16

101 = 6×16 + 5

16 = 3×5 + 1

5 = 5×1 + 0

gcd(218, 117) = 1

1) 42345 = 1×43215 + 29130

43215 = 1×29130 + 14085

29130 = 2×14085 + 960

14085 = 14×960 + 645

960 = 1×645 + 315

645 = 2×315 + 15

315 = 21×15 + 0

gcd(42345, 43215)

2) gcd(3486, 10292)

$10292 = 2 \times 3486 + 3320$

$3486 = 1 \times 3320 + 166$

$3320 = 20 \times 166 + 0$

$\gcd(3486, 10292) = 166$

Modular Arithmetic:

congruent modulo n.

$a \equiv b \pmod{n}$ then $n \mid a$.

Properties of congruences:

* $a \equiv b \pmod{n}$ if $n \mid (a-b)$
* $a \equiv b \pmod{n}$ implies $b \equiv a \pmod{n}$
* $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ imply $a \equiv c \pmod{n}$

Let $a = 23,\ b = 8,\ n = 5$

$23 \equiv 8 \pmod{5}$

$\Rightarrow 23 - 8 = 15 = 5 \times 3$

$\Rightarrow -11 \equiv 5 \pmod{8}$

$\Rightarrow -11 - 5 = -16 = -2 \times 8$

* $((a \bmod n) + (b \bmod n)) \bmod n = (a+b) \bmod n$
* $((a \bmod n) - (b \bmod n)) \bmod n = (a-b) \bmod n$
* $((a \bmod n) * (b \bmod n)) \bmod n = (a*b) \bmod n$

Properties of modular arithmetic for integers in Z_n:

* Commutative law
* Associative law
* Distributive
* Identities
* Additive inverse

Fermat's theorem:

If p is prime, a is +ve integer not divible by p then,

$$a^{p-1} \equiv 1 \pmod{p}$$

Alternate form:

$$a^p = a \pmod{p}$$

$$9^{794} \bmod 73$$

$$9^{(73\times 10+64)} \bmod 73$$

$$\left[(9^{73})^{10} \cdot 9^{64}\right] \bmod 73$$

$$\Rightarrow \left[9^{10} \cdot 9^{64}\right] \bmod 73$$

$$\Rightarrow 9^{74} \bmod 73$$

$$\Rightarrow 1 \bmod 73 \qquad \Rightarrow 9^{73} \bmod 73 \times 9 \bmod 73$$

$$\Rightarrow 1$$

$$\Rightarrow 9 \bmod 73 \times 9 \bmod 73$$

$$\Rightarrow (9 \times 9) \bmod 73$$

$$\Rightarrow 81 \bmod 73 \Rightarrow 8$$

$$x^{86} \equiv 6 \bmod 29$$

$$29\times 2 + 28$$

$$x^{58} \bmod 29 = 6 \bmod 29$$

$$(x^{29})^2 \bmod 29 \times x^{28} \bmod 29 = 6 \bmod 29$$

$$(x^2)^{29} \bmod 29 \times x^{29-1} \bmod 29 = 6 \bmod 29$$

$$x^2 \bmod 29 \equiv 6 \bmod 29$$

$$x^2 \bmod 29 \equiv 6$$

$$\Rightarrow x^2 = 6, 35, 64, \ldots$$

$$\Rightarrow x = \pm 8$$

3) $4^{225} \bmod 13$

$\Rightarrow (4^{17})^{13} \bmod 13 \times 4^4 \bmod 13$

$\Rightarrow (4^{17} \bmod 13)^{\bmod 13} \times 4^4 \bmod 13$

$\Rightarrow 4^{13+4} \bmod 13$

$\Rightarrow 4 \bmod 13 \times 4^4 \bmod 13 \times 4^4 \bmod 13$

$\Rightarrow (4 \times 3 \times 3) \bmod 13$

$\Rightarrow 12$

24/09/2022

Overflow buffer:

```
func() {
    getS()
    printf()
}
main() {
    func()
}
```

Format strings : (modifying output)

(i) used in output statements:

(eg) printf in c

Different form

%d - integer value

%u - unsigned int or value

%x - hexadecimal

%n - no. of bytes

%s - string

Code (refer book)

Format string vulnerability:

%8o → 8 bytes in pack

Reading from arbitrary memory address:

Pass initial 4 bytes

Direct parameter access: $

printf("%7$d", 4, %4$05d", 10,20,30,40,50,60,70,80,90)

output: 7:70, 4:00040

EL:

Detours using dbars

short writes

overwriting offset table

node search

Euler theorem:

$$GCD(a, n) \equiv 1$$

$n = 5$

$$a(1,5) = GCD(2,5) = GCD(3,5) = GCD(4,5) = 1$$

$$\therefore \phi(n) = 4$$

$\phi(n) = n-1$ if n is a prime number

if

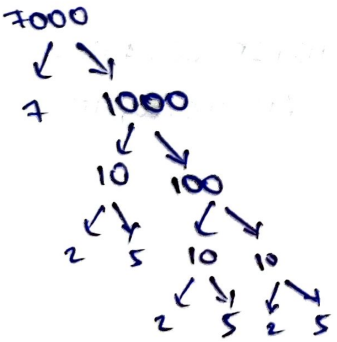
if n is a multiple of p and q where p and q are prime nos,

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

$$\phi(35) = (6)(4) = 24$$

if $n = ab$ where a and b or either a or b is composite,

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



$$\phi(7000) = 7000\left(1 - \frac{1}{7}\right)\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right)$$

$$= 7000\left(\frac{6}{7}\right)\left(\frac{1}{2}\right)\left(\frac{4}{5}\right)$$

$$= 2400$$

Using Euler theorem, solve $4^{99} \bmod 35$

$$a^{\phi(n)} \bmod n \equiv 1$$

1)

$$\phi(35) = 35 \times \left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{7}\right)$$

$$= 35\left(\frac{4}{5}\right)\left(\frac{6}{7}\right) = 24$$

$= (4^{24})^4 \cdot 4^3 \bmod 35$

$\Rightarrow 4^{24} = 1 \bmod 35$ $\quad [\because a^{\phi(n)} = 1 \bmod n]$

$= 1^4 \cdot 4^3 \bmod 35$

$= 64 \bmod 35$

$\Rightarrow 29.$

2) $3^{202} \bmod 13$

$\phi(13) = 12$

$= (3^{12})^{16} \, 3^{10} \bmod 13$

$= (1 \bmod 13)^{16} \, 3^{10} \bmod 13$

$= 3^{10} \bmod 13$

$= 3^3 \cdot 3^3 \cdot 3^3 \cdot 3^1 \bmod 13$

$= 3$

Chinese Remainder theorem:

Step 1: Identify or calculate m_1, m_2, m_3.

Step 2: $M = m_1 \times m_2 \times m_3 \times \cdots \times m_i$

Step 3: $M_i = \frac{M}{m_i}$

Step 4: Calc $a_1, a_2, a_3 \ldots a_i$

Step 5: Calculate M_i^{-1}

Step 6: $X = \sum_i a_i M_i M_i^{-1} \bmod M$

a_i m_i

$X \equiv 2 \bmod 3$

$X \equiv 3 \bmod 5$

$X \equiv 2 \bmod 7$

using CRT

if $a^m \bmod n$, $m < n$ go for Chinese remainder theorem.

Step 1:

$m_1 = 3 \quad m_2 = 5 \quad m_3 = 7$

② ⇒ $M = 3 \times 5 \times 7 = 105$

③ ⇒ $M_1 = \frac{105}{3} = 35 \quad M_2 = \frac{105}{5} = 21 \quad M_3 = \frac{105}{7} = 15$

④ ⇒ $a_1 = 2 \quad a_2 = 3 \quad a_3 = 2$

⑤ ⇒ $M_1^{-1} = 2$

$M_2^{-1} = 1$

$M_3^{-1} = 1$

$\therefore M_i M_i^{-1} = 1 \bmod m_i$

$35 \times 1 \bmod 3 = 2$

$35 \times 2 \bmod 3 = 1$

$21 \times 1 \bmod 5 = 1$

$15 \times 1 \bmod 7 = 1$

⑥ ⇒ $X = 2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1 \bmod 105$

$= 233 \bmod 105$

$= 23$

2) H/W

$4x = 5 \bmod 9$

$x = \frac{8}{3} \bmod 20$

$4 \times 2 \cdot 1 \cdot 9 = 1$

$x \Rightarrow 2$

3) $x = 5 \bmod 3$

$x = 2 \bmod 5$

$x = 1 \bmod 11$

(i) $m_1 = 9 \quad m_2 = 20$

(ii) $M = 180$

(iii) $M_1 = 20 \quad M_2 = 9$

(iv) $a_1 = 8 \quad a_2 = 3$

(v) $M_1^{-1} = 5 \quad M_2^{-1} = 9$

$20 \times 2 \cdot 1 \cdot 9 = 1 \quad 9 \times 2 \cdot 1 \times 20 = 1$

(vi) $x = \sum_{i=1}^{n} a_i M_i M_i^{-1} \bmod 180$

$= 8(20)(5) + 3(99)(9)$

$x = 1043 \bmod 180$

$x = 143$

① $m_1 = 3 \quad m_2 = 5 \quad m_3 = 11$

② $M = 3 \times 5 \times 11 = 165$

③ $\Rightarrow M_1 = \frac{165}{3} = 55 \quad M_2 = \frac{165}{5} = 33 \quad M_3 = \frac{165}{11} = 15$

④ $\Rightarrow a_1 = 5 \quad a_2 = 2 \quad a_3 = 1$

⑤ $\Rightarrow M_1^{-1} =$

14/10/2022

Miller - Robin Primality test:

$n-1 = 2^k * m$

$a \quad 1 \leq a \leq (n-1)$

$b_0 = a^m \bmod n \rightarrow \pm 1$ ⇒ prob prime

$b_1 = b_0^2 \bmod n \rightarrow +1$ comp
$\qquad\qquad \rightarrow -1$ prob prime

$b_2 = b_1^2 \bmod n$

1) is 561 a prime number?

(i) $561 - 1 = 2^4 \times 35$

$k = 4 \quad m = 35$

(ii) $a = 2$, $\therefore 1 < a < n-1$

$b_0 = 2^{35} \bmod 561$

$= 263 \neq \pm 1$

$b_1 = (263)^2 \bmod 561$

$= 166 \neq \pm 1$

$b_2 = 166^2 \bmod 561$

$= 67 \neq \pm 1$

$b_3 = 67^2 \bmod 561$

$= 1$

2) is 53 a prime no?

(i) $53 - 1 = 2^2 \times 13$ $\qquad n-1 = 2^k \times m$

$k = 2 \quad m = 13$

$a = 2$ $\qquad 1 < a < 52$

(ii) $a=2$,

$b_0 = 2^{13} \bmod 53$

$= 2^8 \cdot 2^4 \cdot 2 \bmod 53$

$= 11.11.2 \bmod 53$

$b_0 = 30$

$b_1 = (30)^2 \bmod 53$

$= 52$

$b_2 = (52)^2 \bmod 53$

$= 1$

GF (Galois Field) of Prime No:

Order of finite field is given as p^n

→ used in polynomial prime

→ used in AES

$GF(2) = \{Z, *, +\}$

$+_2$	0	1
0	0	1
1	1	0

$*_2$	0	1
0	0	0
1	0	1

a	0	1
$-a$	0	1
a^{-1}	-	1

$GF(5)$

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$*_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

a	-a	a^{-1}
0	0	—
1	4	1
2	3	3
3	2	2
4	1	4

$a+(-a)=0$

(1)

$(a * \frac{1}{a}) = 1$

GF(7), GF(8)

GF(7):

+7	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

*7	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

a	-a	a^{-1}
0	0	-
1	6	1
2	5	4
3	4	5
4	3	2
5	2	3
6	1	6

GF(8):

$+_8$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

$\times_8$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

a	-a	a^{-1}
0	0	-
1	7	1
2	6	-
3	5	3
4	4	-
5	3	5
6	2	-
7	1	7

26/10/2022

Not every element will have inverse. So, we move to polynomial ($a x_i^n$)

Maximum degree = n-1 (Eg: 2^3 degree = 3-1 = 2)

Polynomial addition: XOR

0 → 0 0 0 → 0

1 → 0 0 1 → 1

2 → 0 1 0 → x

⋮

7 → 1 1 1 → $x^2 + x + 1$

GF(28) Irreducible polynomial, ⇒ $x^8 + x^4 + x^3 + x + 1$

o/p

Addition

(eg) $f(x) = x^2 + x + 1$

$g(x) = x^2 + 1$

⇒ Result: x (2)

Multiplication: 2^3 ⇒ o/p ⇒ [0-3]

$x^2 + x + 1$

$x^2 + 1$

$x^4 + x^3 + x^2 + x^2 + x + 1$

⇒ $x^4 + x^3 + x + 1$

$m(x) = x^3 + x + 1$

$x^3 + x + 1 \;|\; x^4 + x^3 + x + 1 \;(x + 1$

$x^4 + x^2 + x$

$x^3 + x^2 + 1$

$x^2 + x + 0$

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	0	3	2	5	4	7	6
2	2	3	0	1	6	7	4	5
3								
4								
5								
6								
7								

$$x+1 \quad \overline{)\; x^3+x^2+x^2+x \;} \quad x^2+x$$

$$\Rightarrow x^3+x$$

$$x^3+x+1 \quad \overline{)\; x^3+x \;} \quad 1$$

$$x^3+x+1$$

$$1$$

$$f(x) = x^6+x^4+x^2+x+1$$

$$g(x) = x^7+x+1$$

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

Addition:

$$\Rightarrow x^7+x^6+x^4+x^2+x+x+1+x$$

$$\Rightarrow x^7+x^6+x^4+x^2$$

Multiplication:

$\Rightarrow x^{13} + x^7 + x^6 + x^{11} + x^5 + x^4 +$
$x^9 + x^3 + x^2 + x^8 + x^2 + x +$
$x^7 + x + 1$

$\Rightarrow x^{13} + x^{11} + x^9 + x^6 + x^5 + x^4 + x^3 + 1$

$$
\begin{array}{r|l}
 & x^5 + x^3 + 1 \\
\hline
x^8+x^4+x^3+x+1 & x^{13} + x^{11} + x^9 + x^6 + x^5 + x^4 + x^3 + 1 \\
 & x^{13} + x^9 + x^8 + x^6 + x^5 \\
\hline
 & x^{11} + x^8 + x^4 + x^3 + 1 \\
 & x^{11} + x^7 + x^6 + x^4 + x^3 \\
\hline
 & x^8 + x^7 + x^6 + 1 \\
 & x^8 + x^4 + x^3 + x + 1 \\
\hline
 & x^7 + x^6 + x^4 + x^3 + x
\end{array}
$$

Assignment: (Mod 8)

Take one application, apply any hashing fn to get o/p. (eg: SHA -256)

GF(2^8)

$f(x) = 7 \Rightarrow x^2 + x + 1$

$g(x) = 4 \rightarrow x^2$

$m(x) = x^3 + x + 1$

$f(x) = x^8 + x^5 + x^3 + 1$
$g(x) = x^7 + x^6$

Addition:

$\Rightarrow x + 1$ (3)

Multiplication:

$\Rightarrow x^4 + x^3 + x^2$

$x^3 + x + 1 \;\big|\; x^4 + x^3 + x^2$

$x + 1$

$x^4 + x^2 + x$

$x^3 + x$

$x^3 + x + 1$

1

(2) $f(x) = x^6 + x^5 + x^3 + 1$

$g(x) = x^7 + x^6$

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

Addition:

$x^7 + x^5 + x^3 + 1$

Multiplication:

$\Rightarrow x^{13} + x^{12} + x^{10} + x^7 + x^{12} + x^{11} + x^9 + x$

$x^8 + x^4 + x^3 + x + 1 \;\big|\; x^{13} + x^{11} + x^{10} + x^9 + x^7 + x^6$

$x^5 + x^3 + x^2 + 1$

$x^{13} + x^9 + x^8 + x^6 + x^5$

$x^{11} + x^{10} + x^8 + x^7 + x^5$

$x^{11} + x^7 + x^6 + x^4 + x^3$

$x^{10} + x^8 + x^6 + x^5 + x^4 + x^3$

$x^{10} + x^6 + x^5 + x^3 + x^2$

$x^8 + x^4 + x^2$

$x^8 + x^4 + x^3 + x + 1$

$x^3 + x^2 + x + 1$

9/11/2022

Affine cipher

$f(x) = \alpha x + \beta \pmod{26}$ | key: (α, β)

$f(x)$ → C.T, x → P.T

constraints:

(i) $GCD(\alpha, 26) = 1$

(ii) $1 \leq \alpha \leq 25$

(iii) $0 \leq \beta \leq 25$

Encrypt letter 'G' for $\alpha = 7$ $\beta = 2$

$G = 6$

$f(x) = 7(6) + 2 \mod 26$

$= 44 \mod 26$

$= 18$

$\therefore CT = S$

Eg 1: hello

$h = 7$

$f(x) = 7(7) + 2 \mod 26$

$= 51 \mod 26$

$= 25$

$CT = Z$

$e = 4$

$f(x) = 7(4) + 2 \mod 26$

$= 30 \mod 26$

$= 4$

$CT = E$

$T = T_1 - T_2 \times Q$ (Q: quotient)

11 mod 26

Q	A	B	R	T_1	T_2	T
2	26	11	4	0	1	-2
2	11	4	3	1	-2	5
1	4	3	1	-2	5	-7
3	3	1	0	5	-7	26
	1	0		-7	26	

$-7 \bmod 26$

19

$L = 11$

$f(x) = 7(11) + 2 \bmod 26$

$= 79 \bmod 26$

$= 1$

CT = B

$O = 14$

$f(x) = 7(14) + 2 \bmod 26$

$= 98 + 2 \bmod 26 = 100 \bmod 26$

$= 22$

CT = W

Hello → ZEBBW

$\Rightarrow f(x) = \alpha x + \beta \Rightarrow y = \alpha x + \beta$

$\Rightarrow x = \frac{y - \beta}{\alpha} \bmod 26$

For z,

$z = 25$

$x = \frac{25 - 2}{7} \Rightarrow (7)^{-1} [23] \bmod 26$

7 × 15 mod 26 = 1

$x = 4[23] \bmod 26 \quad 15[23] \bmod 26$

$= 92 \bmod 26 \Rightarrow 345 \bmod 26$

$x = 14 \Rightarrow 7$

7 → 'H'

Q	A	B	R	T_1	T_2	T
3	26	7	5	0	1	-3
1	7	5	2	1	-3	4
2	5	2	1	-3	4	-11
2	2	1	0	4	-11	26
	1	0		-11	26	

$-11 \bmod 26$

$\Rightarrow 15$

E → 4

$x = \frac{4-2}{7} \Rightarrow 15(2) \bmod 26$ $[7^{-1} = 15]$

$= 4$

P.T = E

B → 1

$x = 15(1-2) \bmod 26$

$= -15 \bmod 26$

$x = 11$

P.T = L

W → 22

$x = 15(22-20) \bmod 26$

$= 15(20) \bmod 26$

$= 300 \bmod 26$

14

P.T = O

ZEBBW → HELLO

Public key cryptography

* consist of 2 keys (public & private)
* Encryption done using public key
* Decryption done using private key

$E = (Pu_b \times X)$ Pu_b - public

$D = (Pr_b \times E)$ Pr_b - private

Terminology used:

* Encryption algorithm (symmetric)
* Decryption algorithm

RSA

* It is not very secure
* It is very easily prone to attack

3 steps:

(i) key generation
(ii) Encryption
(iii) Decryption

Key generation steps:

* Select prime nos p & q. [such that it shld be kept private]
* Calculate n, $n = p \times q$
* Find $\phi(n) = (p-1)(q-1)$
* Choose the value e such that $1 < e < \phi(n)$
  Also make sure, $\gcd(e, \phi(n)) = 1$
* Calculate d, $d = e^{-1} \bmod \phi(n)$
  $ed \bmod \phi(n) = 1$
* public key; (e, n)
* private key; (d, n)
* Encryption formula:
  $C.T = M^e \bmod n$
* Decryption formula:
  $P.T = C^d \bmod n$

$\therefore M < n$

↓

length of msg

Eg:

(i) $p = 3 \quad q = 11$

(ii) $n = 3 \times 11 = 33$

(iii) $\phi(n) = (3-1)(11-1) = 20$

(iv) $e = 7$ $\quad [1 < e < 20]$ $\quad [\because \gcd(e, \phi(n)) = 1]$

(v) $d = (7)^{-1} \bmod 20$ $\quad 7 \times x \bmod 20 = 1$ $\quad \boxed{x = 3}$

$d = 3$

(vi) $PU_D = (7, 33)$

(vii) $PU_R = (3, 33)$

$$CT = M^e \bmod n \qquad \boxed{M = 31}$$

$$= 31^7 \bmod 33$$

$$= 31^2 \times 31^2 \times 31^2 \times 31 \bmod 33$$

$$= 4 \times 4 \times 4 \times 31 \bmod 33$$

$$\boxed{CT = 4}$$

$$P.T = C^d \bmod n$$

$$= 4^3 \bmod 33$$

$$\boxed{P.T = 31}$$

2	20	7	6	0	1	-2
1	7	6	1	1	-2	3
6	6	1	0	-2	3	-20

Different attacks which can bring down RSA!

* Brute force attack → [trying all possible comb]
* Mathematical attack → [using factors of pub. we can find private key]
* Timing attack → [finding amount of time it take to find its complexity]
* Chosen cipher text attack → [adding diff cipher into brug] [using the properties of RSA, it is possible to bring down] [add constant time, random delay]

(i) $p = 17 \quad q = 11$

Q	A	B	R	T_1	T_2	T
53	160	3	1	0	1	-53

(ii) $n = 17 \times 11 = 187$

(iii) $\phi(n) = (17-1)(11-1) = 160$

(iv) $e = 3$ $\quad [1 < e < 160]$

(v) $d = (3^{-1}) \bmod 160$

$d = 107$

(vi) $PU_b = (3, 187)$

(vii) $PU_r = (107, 187)$

$CT = M^e \bmod n \qquad M = 31$

$= 31^3 \bmod 187$

$\boxed{CT = 58}$

$P.T = 58^{107} \bmod 187$

$\boxed{P.T = 31}$

26/11/2022 **Diffie Hellman** (no encryption but key is shared)

* Private key $x_A \rightarrow$ value or number less than q (prime no.)

α - primitive root of q.

$a \bmod q, a^2 \bmod q, a^3 \bmod q \ldots a^{p-1} \bmod q$

$\downarrow$

$1, 2, 3, \ldots, p-1$

* public key, $Y_A = \alpha^{x_A} \bmod q$ [only public key is exchanged]

key generation, $K = (Y_B)^{x_A} \bmod q$

$$K = (Y_A)^{X_B} \bmod q$$

$$= (\alpha^{X_A} \bmod q)^{X_B} \bmod q$$

$$= (\alpha^{X_A \cdot X_B}) \bmod q$$

$$= (\alpha^{X_B})^{X_A} \bmod q$$

$$= (\alpha^{X_B} \bmod q)^{X_A} \bmod q$$

$$= (Y_B)^{X_A} \bmod q$$

∴ With one key, we can generate another.

Problem

Given $q = 11$, $\alpha = 2$, $X_A = 6$, $X_B = 8$

$$Y_A = \alpha^{X_A} \bmod q$$

$$= 2^6 \bmod 11$$

$$= 64 \bmod 11$$

$$= 9$$

$$Y_B = \alpha^{X_B} \bmod q$$

$$= 2^8 \bmod 11$$

$$= 3$$

$$K = (Y_B)^{X_A} \bmod q$$

$$= 3^6 \bmod 11$$

$$\boxed{K = 3}$$

$$K = (Y_A)^{X_B} \bmod q$$

$$= 9^8 \bmod 11$$

30/11/2022

Module - 3

* ELF
→ Static binaries

→ SQL injection

3/12/2022

→ Fuzzing
→ Port scanning
→ ARP poisoning

7/12/2022

Authentication

Traffic analysis

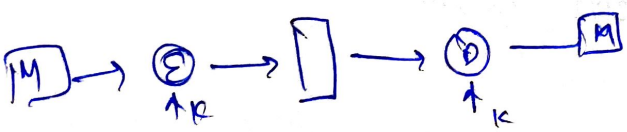
Masquerade

Content modification
Sequence modification
Timing (delay)
Source repudiation
Message authentication function
→ 2 levels of authentication
→ low level → authentication
→ hash fn / encryption / MAC

Frame check reference
Cryptographic checksum

$$MAC = C(K, M)$$

(M → Msg, K → Key, C → Enc)



Uses

* Network broadcasting
*

HMAC

12/12/2022 PKI (2nd ref book)

Public key Infrastructure

→ Certificate Authority
  * collect all public keys
  * should be trustable
  * communication must be secure

Example:

Universal PKI:

→ everyone will have one public key which is highly impossible

→ non a feasible option

VPN access:

→ allowing employee to access resource

→

→ electronic Banking:

  * Functional transaction
  * Person making transaction should be authorized
  * need PKI to provide secure & accept

Refinary sensors:

Credit card validation

Multi level certification:

PKI uses a clock through which a particular digital signature will get expired. Thus, improving security

PKI reality

- → name
- → Authority
- → Trust

Indirect Authorization

- Access control list

Direct Authorization

Credential System

Revocation

- → Speed of revocation
- → Reliability
- → Connectivity

To overcome revocation: we expiry date

Life of a key:

1) create
2) get certificate
3) broadcast certificate details using PKI
4)
5) Expiration (need to be stored in CL)

Certification format:

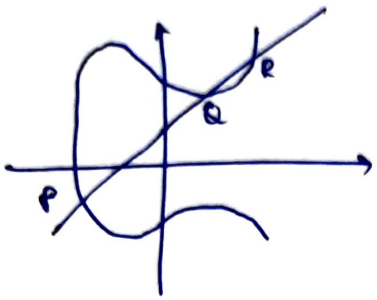
Permission

Root key (root certifying key)

14/12/2022 Mod-9

Elliptic curve cryptography digital signature

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1 \quad \Rightarrow \quad y^2 = x^3 + ax + b$$



Characteristic

→ Faster
→ Efficient

RSA Vs ECC

In ECC to generate key, it require 256-bit while in RSA, it requires 3072-bit.

Disadvantage:

* Difficult to implement
* Computation is slow but secure

ECDSA (Elliptical curve Digital Signature Algorithm ...)

Digital Signature & Certificate:

Digital Signature operations:

* Key generation
* Signing algo
* Signature verification

Digital certificate:

issued by certificate authority to verify the identity of certificate holder.