

Principles of security:

- * Confidentiality
- * Authenticity
- * Integrity

To overcome CIA, there should be no

- * Interception
- * Modification
- * Fabrication

* Availability

* Access control

* Attacks

(i) Criminal

(ii) Publicity

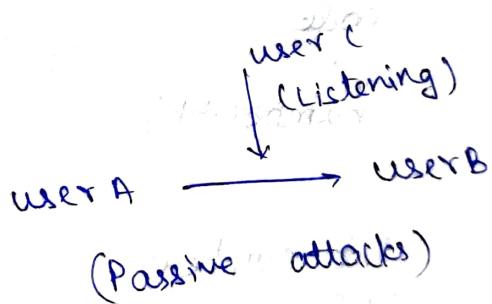
(iii) Legal

Attacks

→ passive

→ active

(eg) DOS



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
* BSS variable

* 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;

lge 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 occurrence of break point

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

next - moves to next line

bit - list and break pointer start with

Buffer:

* temporary storage, * fast processing

Cryptology:

short study of cryptography

* plain text - human readable form

* cipher text - unreadable form

Encryption: technique to convert plain to cipher text

Decryption: technique to convert cipher to plain text

Substitution:

Caesar cipher:

$$C = (P, k)$$

$$\text{cipher} = (P+k) \bmod 26$$

$$\begin{array}{|c|c|c|c|c|c|} \hline P & 0 & 1 & 2 & 3 & 4 & 5 \\ \hline C & 3 & 4 & 5 & 6 & 7 & 8 \\ \hline \end{array} \quad P = (C-k) \bmod 26$$

(eg): PF Meet Me
CT = PHHW PH } (k=3)

(Row 1) Caesar cipher, k=3		
G	H	I
H	I	J
I	J	K
J	K	L
K	L	M
L	M	N
M	N	O
N	O	P
O	P	Q
P	Q	R
Q	R	S
R	S	T
S	T	U
T	U	V
U	V	W
V	W	X
W	X	Y
X	Y	Z
Y	Z	A
Z	A	B

sentences are often obtained by Antony
Nishant is a friend of Antony
PFB RI DQWRAB
C.T = QLVKDQW LV D IULQJ RI DQWRAB

Hex

C.T = GEXXEQEXSFGR [DESUBNTBV]

P.T = QBUUVBNBUP (DR)
good morning friends *

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

Let $S = \{a, b, c\}$, $\xrightarrow{26 \text{ ways}} 25 \text{ ways} \text{ (since 1 is taken)}$

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	K	M	N	O
Q	R	S	T	U
V	W	X	Y	Z

P.T	A	T	T	A	C	K
C.T	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 \rightarrow

* same column \downarrow

* Rectangle square swap

P.T

C.T

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

Hill cipher: (1929)

$$(1929) \xrightarrow{1/26} \text{G T D E W E A N I O}$$

*using mathematical operation.

$$\begin{bmatrix} G & T & D & E \\ W & E & A & N \\ I & O & N & I \end{bmatrix} = \begin{bmatrix} 7 & 10 & 4 & 5 \\ 23 & 20 & 18 & 14 \\ 19 & 12 & 1 & 10 \\ 1 & 14 & 10 & 19 \end{bmatrix} \times \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} + \begin{bmatrix} 7 & 10 & 4 & 5 \\ 23 & 20 & 18 & 14 \\ 19 & 12 & 1 & 10 \\ 1 & 14 & 10 & 19 \end{bmatrix}$$

$$\text{C.T} = \text{P.T} \times K \pmod{26}$$

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

$$K = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \begin{bmatrix} 8 & 37 \\ 21 & 15 \end{bmatrix} \xrightarrow{1/26} \text{G T D E W E A N I O}$$

P.T = H E L P

$$\text{C.T} = \begin{bmatrix} 7 & 10 \\ 23 & 20 \end{bmatrix} \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \xrightarrow{1/26} \begin{bmatrix} 21+8 & 21+20 \\ 21+20 & 21+8 \end{bmatrix} \pmod{26}$$

$$\text{as } 1. \begin{bmatrix} 21 & 8 \\ 21 & 20 \end{bmatrix} \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \xrightarrow{1/26} \begin{bmatrix} 29 & 41 \\ 41 & 29 \end{bmatrix} \pmod{26}$$

$$\text{C.T.} = [D \ P] \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \xrightarrow{\text{first two characters}}$$

$$\text{C.T.} = \begin{bmatrix} 8 & 11 \\ 15 & 11 \end{bmatrix} \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \xrightarrow{1/26} \begin{bmatrix} 33+30 & 33+15 \\ 33+15 & 33+30 \end{bmatrix} \pmod{26}$$

$$= [63 \ 108] \pmod{26}$$

$$\text{as } 1. \begin{bmatrix} 8 & 11 \\ 15 & 11 \end{bmatrix} \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \xrightarrow{1/26} \begin{bmatrix} 11 & 4 \\ 4 & 11 \end{bmatrix}$$

$$\text{C.T.} = \text{bold } [E \ P]$$

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

as bold

Description:

$$P.T = E.T \times K^{-1} \pmod{26}$$

$$K^{-1} = \frac{1}{|K|} (\text{adj } K) \quad \text{Calculation: adj } K \text{ mod } 26$$

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

$$\therefore K = \begin{bmatrix} 3 & 8 \\ 2 & 5 \end{bmatrix} \pmod{26} \quad = P.7$$

$$\text{adj}(K) = \begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix} \begin{bmatrix} 5 & 8 \\ 2 & 5 \end{bmatrix} \quad = P.9$$

$$|K| = 15 - 8 = 7 \quad \text{Calculation: } 8 + 15 = 23 \quad = P.0$$

$$K^{-1} = \frac{1}{7} \begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix} \begin{bmatrix} 3 & 15 \end{bmatrix} \cdot \frac{1}{26} \quad \text{Calculation: } 23 \cdot 26 = 1 \quad = P.0$$

$$\Rightarrow 3 \begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix} \begin{bmatrix} 3 & 15 \end{bmatrix} \cdot \frac{1}{26} \quad \begin{array}{l} 9 \times (x) \\ \text{no remainder} \\ = 1 \end{array}$$

$$(\text{cancel out } 3) \begin{bmatrix} 15 & -9 \\ -6 & 9 \end{bmatrix} \begin{bmatrix} 3 & 15 \end{bmatrix} \cdot \frac{1}{26} \quad = P.2$$

$$\begin{bmatrix} 22+28 & 03+08 \end{bmatrix} = \begin{bmatrix} 2 & 8 \\ 2 & 5 \end{bmatrix} \begin{bmatrix} 21 & 17 \end{bmatrix} \cdot \frac{1}{26} \quad = P.0$$

Calculation: $22+28=40 \rightarrow 14$
 $03+08=11$

$$\begin{aligned} & 14 \cdot 14 \begin{bmatrix} 20 & 8 \end{bmatrix} \cdot \frac{1}{26} \\ & = 3 \begin{bmatrix} 3 & 15 \end{bmatrix} \begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix} \cdot \frac{1}{26} \\ & = \begin{bmatrix} -75 & 198 \end{bmatrix} \cdot \frac{1}{26} \\ & = \begin{bmatrix} 49 & 198 \end{bmatrix} \pmod{26} \end{aligned}$$

$$3. \quad \begin{pmatrix} 5 & 23 \\ 24 & 3 \end{pmatrix} \cdot \begin{pmatrix} 15 & 7 \\ -6 & 9 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{26}$$

5) Polyalphabetic cipher

$$c_i = (p_i + k_i) \bmod 26$$

key = Decepti~~v~~ive Dec
P.T = Pay once more

\therefore If P.T is longer than key, repeat key until it becomes equal to P.T.

$$(D, P) \Rightarrow (3 + 15) \bmod 26 = 18 \Rightarrow S$$

$$(E, A) \Rightarrow (4 + 0) \bmod 26 \Rightarrow 4 \Rightarrow E$$

Instead of repeating key when its size is smaller than P.T, we can repeat P.T in key so that ~~repetition will work~~ ^{will be easy to find} to decipher.

similar to square in box or work with ~~square~~

6) Vernam cipher: similar to previous one following no fixed box

$$c_i = p_i \oplus k_i$$

if we take all same for c_i

One time pad:

same as polyalphabetic cipher but here we use a key only once,

Attack

Attack

Attack

Attack

Transposition

Attack

Rail fence

Attack

Depth = 2

Plain Text = Attack at once

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

c.t = Atcaoctakthe

depth = 3

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

$$\text{so base } (x+3) = 12$$

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

or 9 other loops surround the letters

depth = 3

A	i	c								(7,1)
t	a	p	k	t	c	o	n	e	(8,2)	
t	t	a								(9,3)

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

see all words first phrasal for better

in the bigger row we have 19 words all

Row or column transposition: sort as per

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

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

so if the length is 13 then omit 2nd

P.T = Attack at once

	0	1	2	3	4
0	A	t	t	a	
1	c	k	a	t	
2					
3					
4					

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

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

and so do the - that make

entry PTD 2002 Tn = 7.0

1	2	3	4	5	6	7	8	9	10	11	12	13
3	4	5	6	7	8	9	10	11	12	13	14	15

Decryption:

key = MONARCHY → $\begin{matrix} M & O & N & A & R \\ C & H & Y & B & D \\ E & F & G & I & J \\ L & P & Q & S & T \\ V & U & W & X & Z \end{matrix}$ key = CÆSAR → $\begin{matrix} C & A & E & S & R \\ B & D & R & G & H \\ I & K & L & M & N \\ O & P & A & T & U \\ V & W & X & Y & Z \end{matrix}$

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

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

R S | S R | D E

→ ATTACK

WT | M@1KO1 QF

→ MULTIPLE

ON | TS | ML

→ MOSQUE

stl 80 / lsl 80

R@PAC | NTIONM | VE

→ ENCRYPTION

Sample space (S):

set of all possible outcomes $\leftarrow 2^{\infty}$

one deck of cards → 52
after returning → 52
Toss a coin {H, T} → 2

→ 2ⁿ

Event (E):

the occurrence of action in the sample space.

* favourable event

* non-favourable event

n - probability number of times a favourable event occurs.

$\frac{m}{n}$ - event

n - sample space

p_1

p_2

$\frac{n}{m}$ -

p_1

p_2

p_1, p_2, \dots, p_n

Addition:

$$P(A \cup B) = P(A) + P(B) - P(A \cap B)$$

→ for dependent event

$$P(A \cup B) = P(A) + P(B) \rightarrow \text{for independent event}$$

Binomial:

$$P(\text{occurrence (success)}) = P$$

$$P(\text{not occurrence / failure}) = 1 - P$$

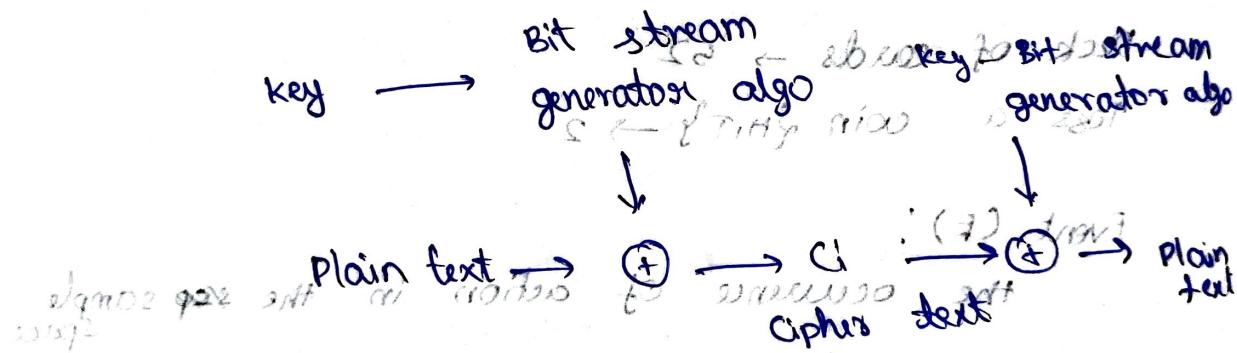
$$\text{Binomial distribution} = P^k (1-P)^{n-k}$$

DES algorithm (for data encryption standard)
* based on symmetric algorithm

101. **Stream cipher:**
→ bitstream, cipher:
change PT to CT character by character
initialization vector

101. **Block cipher:**
→ block cipher:
change PT to CT block by block
minimum 64 bits vs bits

101. **DES → Block structure**



* mapping
→ reversible (e.g. Caesar cipher)

Example of a ~~non-reversible~~ reversible function f(x) = x + n

Eg. for irreversible:

P.T C.T

00

10

01 → 11

10 00

(0101)2 → (0111)2 + (1010)2 = (0001)2

thus two inputs can be

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

* First block structure - idle block structure

* Concepts used in first block structure:

→ Diffusion → Substitution (Transposition)
→ confusion → Transposition / Substitution

* steps followed in DES encryption

Plain text (64 bit)

L (32 bit) R (32 bit)

- 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

↓ 64

Round 16

↓ 64

32 bit swap on *
swap 13 to 32 *

swap 28 to 15
Cipher text

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

brow tool

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

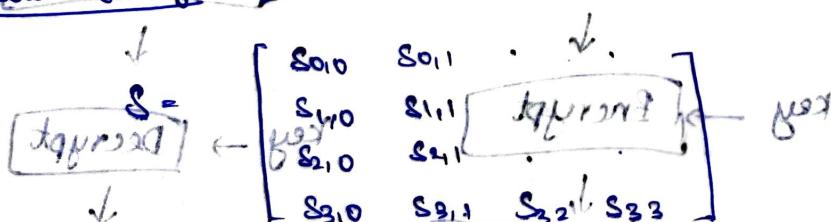
[00]	[10]	[01]	[11]
[10]	[00]	[00]	[00]
[00]	[00]	[00]	[00]
[00]	[00]	[00]	[00]

Round 1 Recip \leftarrow
f⁻¹
g⁻¹
h⁻¹

* Repeat the same process for 9 rounds.

* For the 10th round (last one), matrix multiplication is not used. Good idea to shorten it.

state carry [Intermediate value]



text now

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

Add round key:

Intermediate

text

$$\oplus \text{key} \Rightarrow \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = E$$

} Round 2

For each row, we use different round key.

Root word:

	72	69	6e	67		secret
x ₁	69	6e	67	72	modification	word37
s-box	y ₁	f ₉	9f	85	(A0 80)	first word

Round const

$$[R_1 \longrightarrow R_{10}]$$

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

$$\rightarrow \text{glw37} = \begin{pmatrix} \text{f901} & 01 \\ 9f & 00 \\ 85 & 00 \\ 40 & 00 \end{pmatrix}$$

(modification result)

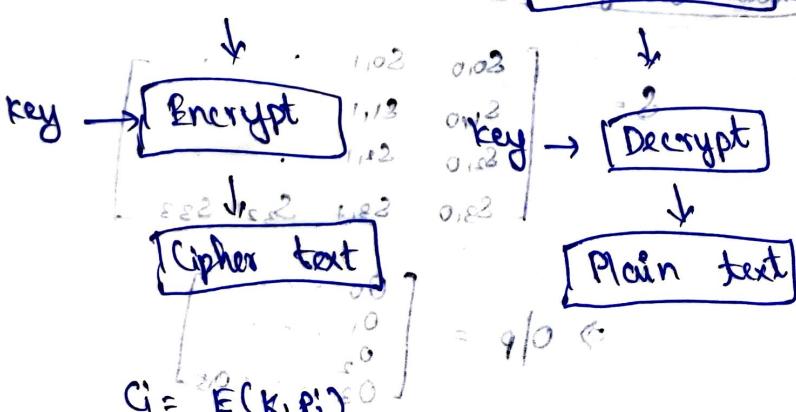
first b ware bba

14/09/2022 P root second more anti longest *

Block cipher mode: test b ware bba with root *

* Electronic code book . baa in mitsilgillum

Plaintext Cipher Text



$$C_i = E(K, P_i)$$

$$P_i = D(K, C_i)$$

↳ first b ware bba

↳ its it smearish

↓ slowest

(m1)

↓ first

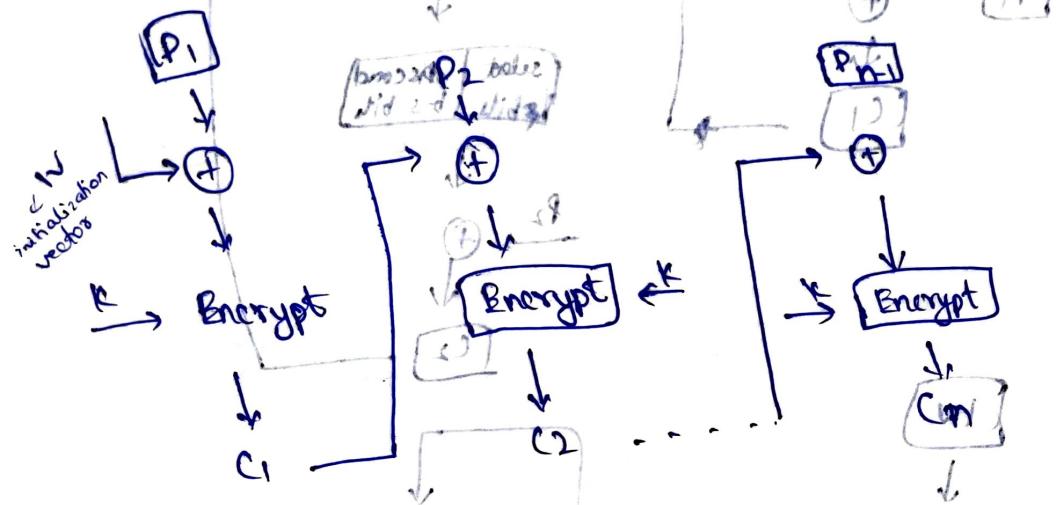
(m2)

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

* Overhead

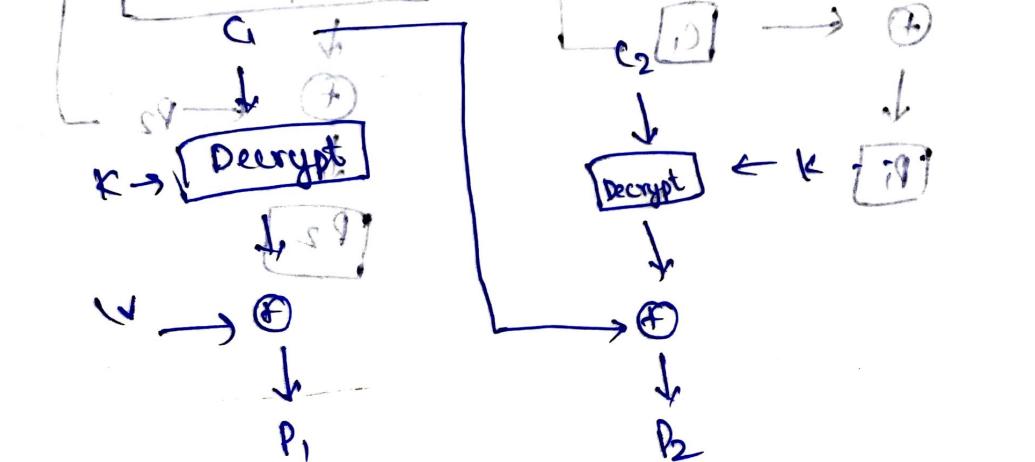
- * Error recovery
- * Error propagation
- * Diffusion
- * Security

Cipher block chaining mode

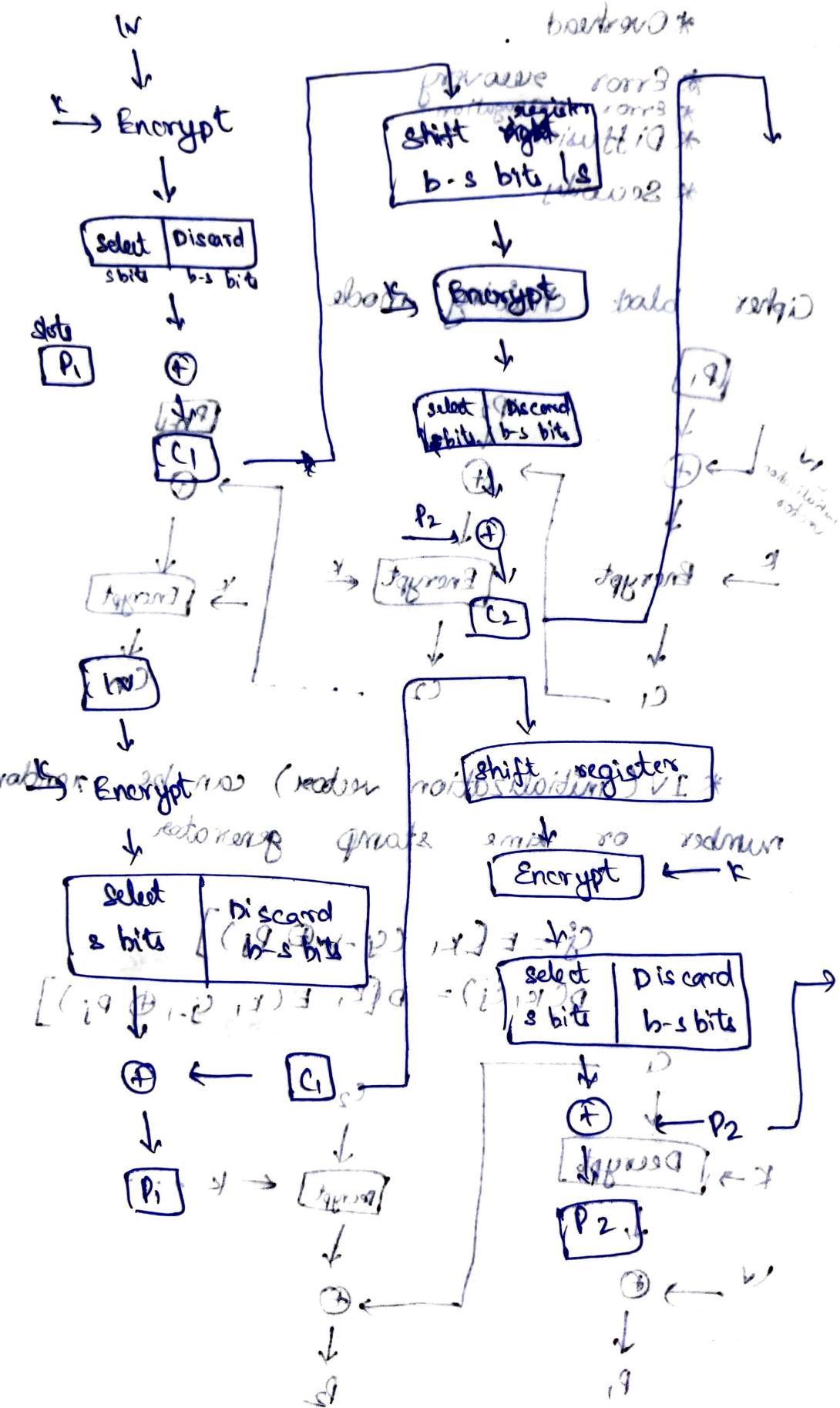


* Initialization vector (IV) can be random number or time stamp generator

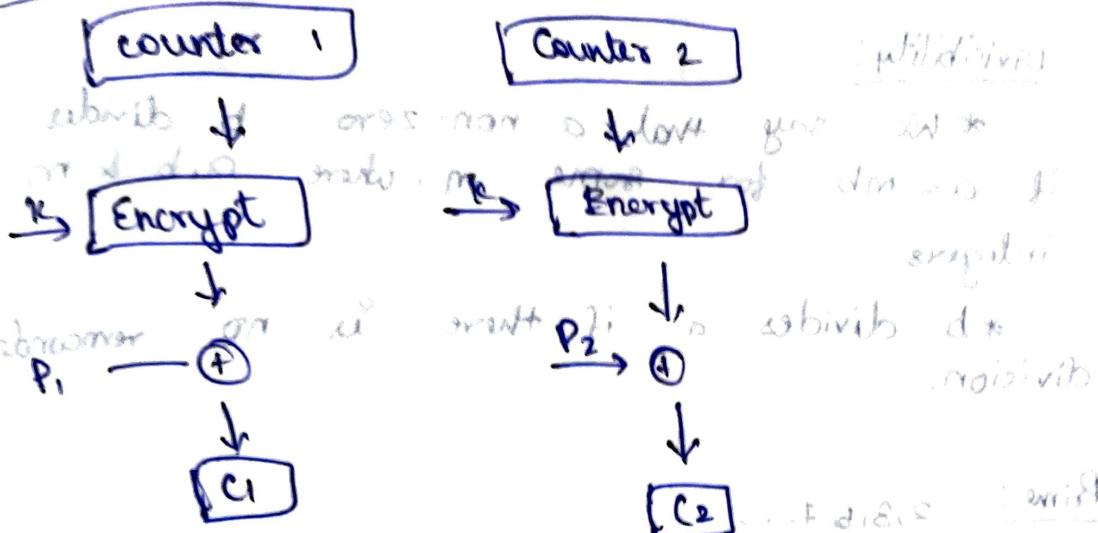
$$C_0 = E(K, IV) \quad C_i = D(K, E(K, IV \oplus P_{i-1}))$$



3) Cipher feedback mode

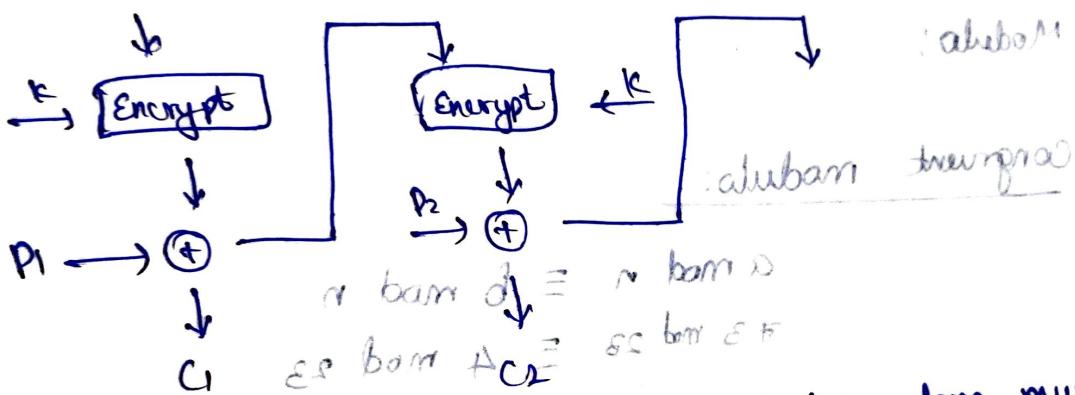


Counter Mode: ~~secret~~ ~~method~~ ~~parallel~~



Output feedback mode: switcheroo and 2011
i.e. (K, E, D) bop

Nonce



Counter mode (cont)
* Encryption & decryption can be done much

faster.

* can be performed well in parallel manner

$1 \leq n \leq m+1$

Padding: $d \leq n$ left old bno, d to *

sample - 10^* o subivib add just *

multirate - $10^* \dots$ so next old dlo *

perfids w/ $(n+m)/d$ next old * plo +
 $n \approx m$ regim

20/09/2022

Number Theory

Divisibility:

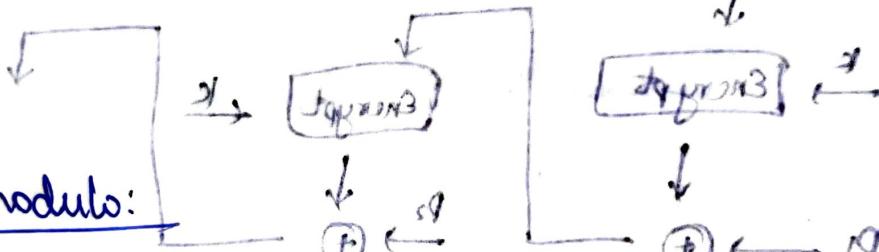
- * We say that a non-zero integer a divides a non-zero integer b , if $a = mb$ for some integer m , where a, b & m are integers.
- * b divides a if there is no remainder on division.

Prime: 2, 3, 5, ... [?]

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

$$\text{gcd}(2, 3, 4) \rightarrow 1$$

Modulo:



Congruent modulo:

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

$$73 \bmod 23 \equiv 4 \bmod 23$$

Two nos a & b \Rightarrow $a \equiv b \pmod{n}$ (mod n returns different values)

Divisibility properties: with examples retention

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

Division algorithm

(Proposed) bop (e)

* Given any positive integer a and any non-negative integer b , if we divide a by b , then the quotient is q and the remainder is r such that $0 \leq r < b$.

$$a = bq + r$$

$$d|a = (\text{Proposed}) \text{ bop}$$

GCD:

* largest integer that divides both a & b .

Mathematical definition

1) $\gcd(42345, 43215)$ by addition subtraction

2) $\gcd(3486, 1029)$ rank (n term) d = 0

3) $\gcd(45, 32)$ Euclidean to subtraction

4) $\gcd(117, 218)$

$$(d-0) \mid r_i \quad (n \text{ term}) d = 0 *$$

3) $218 = 3 \cdot 75 + 13 \quad (n \text{ term}) d = 0 *$

$$75 = 5 \cdot 15 + 0 \quad (n \text{ term}) d = 0 *$$

$$(13 \text{ term}) 2 \times 15 + 0$$

$$11 = 1 \cdot 10 + 1 \quad z = n, 8 = d, 8s = 0 \quad \text{def}$$

$$10 = 1 \cdot 8 + 2 \quad (z \text{ term}) 8 = 8s$$

$$\gcd(75, 32) = 1 \cdot 2 = 2 = 8 - 8s \in$$

$$\begin{array}{r} 218 \\ 117 \\ \hline 101 \end{array}$$

4) $218 = 1 \cdot 117 + 101 \quad (z \text{ term}) z = 117 \in$

$$8 \cdot 13 = d = 2 - 117 \in$$

$$117 = 1 \cdot 101 + 16$$

$$n \text{ term } (d+0) \in = 16 \text{ term } (5 \text{ term}) + (n \text{ term}) *$$

$$n \text{ term } (d+0) 16 = 3 \cdot 5 + (n \text{ term }) + (n \text{ term }) *$$

$$n \text{ term } (d+0) 5 = 5 \cdot 1 + 0 \quad n \text{ term } ((n \text{ term }) + (n \text{ term })) *$$

$$\gcd(218, 117) = 1$$

1) by subtraction with respect to division algorithm

$$42345 = 1 \cdot 43215 + 29130$$

$$645 = 2 \cdot 315 + 15$$

$$43215 = 1 \cdot 29130 + 14085$$

$$315 = 2 \cdot 157 + 0$$

$$29130 = 2 \cdot 14085 + 960$$

$$\gcd(42345, 43215)$$

$$14085 = 14 \cdot 960 + 645$$

$$\text{with respect to } 15$$

$$960 = 1 \cdot 645 + 315$$

$$\text{with respect to } 15$$

2) $\gcd(3486, 10292)$

$$10292 = 2 \times 3486 + 3320$$

23320 \rightarrow remainder
3486 = $1 \times 3320 + 166$
3320 = $20 \times 166 + 0$

$$\gcd(3486, 10292) = 166$$

d & e have same remainders

Modular Arithmetic:

congruent modulo n:

$a \equiv 0 \pmod{n}$ then

(21584, 24854) b/p (1)

(21580, 24858) b/p (2)

(28, 24) b/p (3)

Properties of congruence:

* $a \equiv b \pmod{n}$ if $n|(a-b)$

* $a \equiv b \pmod{n}$ implies $b \equiv a \pmod{n}$

* $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ imply
 $a \equiv c \pmod{n}$

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

$$23 \equiv 8 \pmod{5} \quad 0+1 \times 1 = 01$$

$$\Rightarrow 23 - 8 = 15 = 5 \times 3 \quad (28, 24) \text{ b/p}$$

$$\Rightarrow -11 \equiv 5 \pmod{8} \quad 701 + 811 \times 1 = 812 \quad \text{BN} \quad (A)$$

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

$$d1 + 101 \times 1 = 611 \quad \text{BN}$$

* $((a \pmod{n}) + (b \pmod{n})) \pmod{n} \equiv (a+b) \pmod{n}$

* $((a \pmod{n}) - (b \pmod{n})) \pmod{n} \equiv (a-b) \pmod{n}$

* $((a \pmod{n}) * (b \pmod{n})) \pmod{n} \equiv (a * b) \pmod{n}$

Properties of modular arithmetic for integers in \mathbb{Z}_n^* :

* Commutative law $28041 + 02102xj = 21284$

* Associative law $0dp + 28041 \times 3 = 02102$

* Distributive law $2pd + 0dp \times j = 28041$

* Identity $212 \times 2pd^{-1} = 0dp$

* Additive inverse

Fermat's theorem:

If p is prime, then for any integer a not divisible by p , we have $a^p \equiv a \pmod{p}$.

Alternate form:

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

$$q^{73+4} \equiv q^{73} \pmod{73}$$

$$q^{(73 \times 10 + 64)} \equiv q^{64} \pmod{73}$$

$$[(q^{73})^{10} \cdot q^{64}] \equiv q^{64} \pmod{73}$$

$$\Rightarrow [q^{10} \cdot q^{64}] \equiv q^{64} \pmod{73}$$

$$\Rightarrow q^{64} \equiv q^{64} \pmod{73}$$

$$\Rightarrow q^{64} \equiv q^{73} \pmod{73} \quad \text{since } 73 \mid 64 - 73$$

$$\Rightarrow q \equiv q \pmod{73} \quad \text{since } 73 \nmid 1$$

$$\Rightarrow q \equiv q \pmod{73} \times q \equiv q \pmod{73}$$

$$\Rightarrow (q \times q) \equiv q \pmod{73}$$

$$\Rightarrow 81 \equiv 8 \pmod{73}$$

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

$$x^{29+28} \equiv 6 \pmod{29}$$

$x \pmod{29}$

$$(x^{29})^2 \equiv 6 \pmod{29}$$

$$(x^2)^{29} \equiv 6 \pmod{29}$$

$$x^2 \equiv 6 \pmod{29}$$

$$x^2 \equiv 6 \pmod{29}$$

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

$$\Rightarrow x = \pm 8$$

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

$$\begin{aligned} & \text{Divide } 100 \text{ by } 13 \\ & (4^{17})^{13} \mod 13 \times 4^4 \mod 13 \text{ rem } 4 \mod 13 \\ & \Rightarrow (4^{17} \mod 13)^{\text{mod } 13} \times 4^4 \mod 13 \text{ rem } 4 \mod 13 \\ & \Rightarrow 4^{13+4} \mod 13 \times (4^4 \mod 13)^{\text{mod } 13} \\ & \Rightarrow 4 \mod 13 \times 4^4 \mod 13 \times 4^4 \mod 13 \text{ rem } 4 \mod 13 \\ & \Rightarrow (4 \times 3 \times 3) \mod 9 \mod 13 = 0 \\ & \Rightarrow 12 \end{aligned}$$

$$ef.bam \xrightarrow{P.F} p$$

$$ef.bam [{}^{N.P.} {}^{O.P.}(ef.p)]$$

$$ef.bam [{}^{N.P.} {}^{O.P.}] \in$$

24/09/2022

Overflow buffer: ef.bam $\xrightarrow{P.F} \in$

ef.bam $\xrightarrow{P.F} \in$ ef.bam / | $\xrightarrow{P.F}$
 $\begin{array}{l} \text{func() \{ } \\ \text{ ef.bam } p \times \text{ef.bam } p \in \\ \text{ gets() } \\ \text{ printf("bam (%px) \n", p) } \\ \text{ \} } \end{array}$

main()

func()

} $\quad ps.bam \delta = ps.bam$

$$ps.bam \delta = \frac{ps + esp}{esp + esp} \cdot ps.bam$$

$$ps.bam \delta = ps.bam \cdot ps.bam \cdot ps.bam \cdot (ps.p)$$

$$ps.bam \delta = ps.bam \cdot ps.bam \cdot ps.bam \cdot (ps.p)$$

$$ps.bam \delta = ps.bam \cdot ps.bam$$

Format strings: (modifying output) : meant value

(i) used in output statements:
(eg) printf in C $i = (1, 0) \rightarrow$

Different form $\theta = 1$
%d - integer value
%u - unsigned int value

address / memory hexadecimal or $i = 1 - n = (1) \rightarrow$

%n - no. of bytes

metre p %s - string θ
metre p %b - string to algorithm o si n fi
code (after break) string esp p bno q

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

Format string vulnerability:
 $\#s = (A)(\theta) = (25)\phi$
 $x80 \rightarrow 8$ bytes in pack

Reading from arbitrary memory address /
writing to d bytes at memory address /

Pass initial 4 bytes

$$\dots (\frac{1}{\theta} \dots) (\frac{1}{\theta} \dots) \theta = (n)\phi$$

Direct parameter access: \$

(%printf("%f;%f\$4d", 10, 20, 30, 40, 50,
60, 70, 80, 90))

Output: 10.000000 20.000000
30.000000 40.000000 50.000000
60.000000 70.000000 80.000000
90.000000

EL:

Detours using share

short writes

overwriting offset addresses meant web prior

node search

$\theta = 1$ boom (web)

$$(\frac{1}{\theta} \dots) (\frac{1}{\theta} \dots) \times 28 = (28)\phi$$

Euler theorem:

$$\text{GCD}(a, n) = 1$$

$$n=5$$

$$\text{GCD}(1, 5) = \text{GCD}(2, 5) = \text{GCD}(3, 5) = \text{GCD}(4, 5) = 1$$

$$\therefore \phi(n) = \frac{n}{\cancel{5}}$$

$$\phi(n) = n-1 \quad \text{if } n \text{ is a prime number}$$

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,

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

$$7000$$

$$\begin{array}{r}
 \downarrow \quad \swarrow \\
 7 \quad 1000
 \end{array}
 \quad
 \begin{array}{r}
 \downarrow \quad \swarrow \\
 10 \quad 100
 \end{array}
 \quad
 \begin{array}{r}
 \downarrow \quad \swarrow \quad \swarrow \\
 2 \quad 5 \quad 10
 \end{array}
 \quad
 \begin{array}{r}
 \downarrow \quad \swarrow \quad \swarrow \quad \swarrow \\
 2 \quad 5 \quad 2 \quad 5
 \end{array}$$

$$\begin{aligned}
 \phi(7000) &= 7000 \left(1 - \frac{1}{7}\right) \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) \\
 &= 7000 \left(\frac{6}{7}\right) \left(\frac{1}{2}\right) \left(\frac{4}{5}\right) \\
 &= 2400
 \end{aligned}$$

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

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

$$\begin{aligned}
 1) \quad \phi(35) &= 35 \times \left(1 - \frac{1}{5}\right) \left(1 - \frac{1}{7}\right) \\
 &= 35 \left(\frac{4}{5}\right) \left(\frac{6}{7}\right) = 24
 \end{aligned}$$

$$= (4^{24})^4 \mod 35$$

F 80 prime
n bar 35 fi

$$\Rightarrow 4^{24} = 1 \mod 35$$

$$16^4 \mod 35$$

16 bar 16 mod 35

3 bar 35

$$\begin{cases} x \text{ bar } n \\ \phi(n) = x \\ x \cdot a \text{ bar } n = 1 \mod n \end{cases}$$

29. $\equiv 16^4 \mod 35$

→ 29.

F: 8M 2: 8M 8: 1M

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

201 = F * 8 + E = M 6 ③

$\Rightarrow 3^{201} = 8^M \cdot \phi(13) \cdot 3^{12} = CM$ $E = \frac{201}{8} = 1M$ 6 ④

$$= (3^{12})^{16} \cdot 3^{10} \mod 13$$

$\therefore 3^{12} \text{ bar } 1 \mod 13$ 6 ⑤

$= (1 \mod 13)^{16} \cdot 3^{10} \mod 13$ 6 ⑥

$\Rightarrow 3^{10} \mod 13$ 6 ⑦

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

$\therefore 3^3 \text{ bar } 1 \mod 13$ 6 ⑧

$\Rightarrow -3$

Chinese Remainder theorem:

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

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

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

Step 4: calc $a_1, a_2, a_3, \dots, a_i$

Step 5: calculate M^{-1}

Step 6: ~~$x = \sum_i a_i M_i M_i^{-1} \mod M$~~

$$x \equiv 2 \pmod{3}$$

$$x \equiv 3 \pmod{5}$$

$$x \equiv 2 \pmod{7}$$

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

$$\textcircled{2} \Rightarrow M = 3 \times 5 \times 7 = 105$$

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

$$\textcircled{4} \Rightarrow a_1 = 2 \quad a_2 = 3 \quad a_3 = 5 \quad (\text{since } a_i \text{ is } \text{mod } m_i)$$

$$\textcircled{5} \Rightarrow M_1^{-1} = 2 \quad (\text{since } 35 \times 2 \pmod{3} = 2) \quad M_2^{-1} = 1 \quad (\text{since } 35 \times 1 \pmod{5} = 1) \quad M_3^{-1} = 1 \quad (\text{since } 35 \times 1 \pmod{7} = 1)$$

$$\textcircled{6} \Rightarrow x = 2 \times 3 \times 2 + 3 \times 5 \times 1 + 2 \times 7 \times 1 \quad (\text{mergente rechnung})$$

~~$x = a_1 M_1 x_1 + a_2 M_2 x_2 + a_3 M_3 x_3$~~

~~$\therefore a_1, a_2, a_3 \text{ teilen } M_1, M_2, M_3$~~

~~$\therefore a_1 M_1 \pmod{m_1} = 0, a_2 M_2 \pmod{m_2} = 0, a_3 M_3 \pmod{m_3} = 0$~~

$$x = (2 \times 35 \times 2) + (3 \times 21 \times 1) + (2 \times 15 \times 1) \pmod{105}$$

$$= 283 \pmod{105} \quad (= iM) \quad \therefore \text{getl}$$

$$= 23 \pmod{105} \quad \text{(since } 283 \pmod{105} = 23\text{)} \quad \therefore \text{getl}$$

$$(\text{since } M \text{ teilen } m_1, m_2, m_3)$$

$$x \equiv 23 \pmod{105} \quad \therefore \text{getl}$$

$$2) \text{ H/W } 4x = 5 \pmod{9} \Rightarrow 8 \pmod{9} \quad (1) M_1 = 9 \quad m_2 = 20$$

LCM of 9 and 20

$$\begin{array}{l} \text{1. } x = 5 \pmod{3} \\ \text{2. } x = 2 \pmod{5} \\ \text{3. } x = 8 \pmod{11} \end{array}$$

$$(ii) M_2 = 180 \quad (iii) M_1 = 20 \quad M_2 = 9$$

$$(iv) a_1 = 8 \quad a_2 = 37$$

$$(v) N_1^{-1} = 5 \quad N_2^{-1} = 9$$

$$20 \times 2 \cdot 1 \cdot 9 = 180 \quad 9 \times 2 \cdot 1 \cdot 8 = 144$$

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

$$\textcircled{1} \quad M_1 = 3, M_2 = 5, M_3 = 11 = 8(20)(5) \pmod{180}$$

$$\textcircled{2} \quad M = 3 \times 5 \times 11 = 165 \quad \text{abam 5d} = 3(9)(9)$$

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

$$\textcircled{4} \Rightarrow a_1 = 5 \quad a_2 = 2 \quad a_3 = 1 \quad x = 143 \pmod{165}$$

$$\textcircled{5} \Rightarrow M_1^{-1} = . \quad \text{abam 5d} \quad A = ?$$

$$143 \times 5 = 715 \quad 715 \equiv 0 \pmod{165} \quad (\text{it})$$

$$143 \text{ abam } 5(8d) = 0d$$

$$1 =$$

$$0d \text{ abam } 5(8d) = 0d$$

$$5(8d) = 0d \pmod{165}$$

11/10/2022

Miller-Rabin Primality Test: as $bam \neq 1 \pmod{n}$

$$n-1 = 2^k \cdot m$$

$$a^{(2^k)m} \equiv 1 \pmod{n}$$

$$b_0 = a^m \pmod{n} \rightarrow \pm 1 \text{ prob prime}$$

$$b_1 = b_0^2 \pmod{n} \rightarrow \pm 1 \text{ comp}$$

$$b_2 = b_1^2 \pmod{n} \rightarrow \pm 1 \text{ prob prime} \rightarrow n$$

at lower $\approx 10^{10}$

1) Is 561 a prime number? $\frac{561}{2} = 280 \rightarrow n$

$$(i) 561-1 = 2^4 \times 35 \rightarrow k=4, m=35$$

$$k=4 \quad m=35 \quad 35 \pmod{56}$$

$$(ii) \quad a \neq 1, \quad \therefore 1 < a < n-1$$

$$\begin{aligned} b_0 &= 2^{35} \pmod{561} \\ &= (263) \neq \pm 1 \end{aligned}$$

$$\begin{aligned} b_1 &= (263)^2 \pmod{561} \\ &= 166 \neq \pm 1 \end{aligned}$$

$$b_2 = 166^2 \pmod{561}$$

$$b_3 = 67 \neq \pm 1$$

$$\begin{aligned} b_4 &= 67^2 \pmod{561} \\ &= 1 \end{aligned}$$

2) Is 53 a prime no?

$$(i) \quad 53-1 = 2^2 \times 13$$

$$n-1 = 2^k \cdot m$$

$$k=2 \quad m=13$$

$$a=2$$

$$1 < a < 52$$

(ii) $a=2$,

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

$$(1+2^6)^2 \cdot 2 \pmod{53}$$

$$11 \cdot 1182 \pmod{53}$$

$$b_0 = 30$$

$$b_1 = (30)^2 \pmod{53}$$

$$= 52$$

$$b_2 = (52)^2 \pmod{53}$$

$$= 1$$

GF (Galois Field) of prime No: \mathbb{Z}_p

Order of finite field is given as p^n

→ used in polynomial prime

→ used in AES

$$GF(2) = \{Z_2[x] + y\}$$

x_2	0	1	x	x^2	x^3
0	0	1			
1	1	0	x	x^2	x^3

x_2	0	1	x	x^2	x^3
0	0	0			
1	0	0	x	x^2	x^3

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

$GF(5)$

x_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

x_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

		(0)	(1)
a	-a	a ⁺	a⁻
0	0	0	1
1	4	1	3.
2	3	2	2
<u>$a + (-a) = 0$</u>	<u>3</u>	<u>2</u>	<u>4</u>
	4		

(1)

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

GF(7), GF(8)

GF(7):

+1	0	1	2	3	4	5	6	7	8
0	0	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8	0
2	2	3	4	5	6	7	8	0	1
3	3	4	5	6	7	8	0	1	2
4	4	5	6	0	1	2	3	7	8
5	5	6	0	1	2	3	4	7	8
6	6	0	1	2	3	4	5	8	7
*2	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	0	0	1	2	3	4	5	6
2	0	1	2	3	4	5	6	7	8
3	0	1	2	3	4	5	6	7	8
4	1	0	2	3	5	6	7	8	0
5	0	1	3	6	2	4	7	8	1
6	0	1	5	4	3	2	0	7	8
7	0	1	6	5	4	3	2	0	1
8	0	1	7	6	5	4	3	2	0

a $-a$ a^{-1}

0 0 -

1 6 1

2 5 4

3 4 5

4 3 2

5 2 3

6 1 6

GIF(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

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

137/10

26/10/2022

Not every element will have inverse. So,
we move to polynomial (axi)
Maximum degree = n-1 (Eg: x^3 degree = 3-1
 $= 2$)

Polynomial addition: KOK

$$0 \rightarrow 0 \quad 0 \rightarrow 0$$

$$1 \rightarrow 0 \quad 0 \rightarrow 1$$

$$2 \rightarrow 0 \quad 0 \rightarrow x$$

Irreducible polynomial,
 $\Rightarrow x^8 + x^4 + x^3 + x + 1$

O/P

$$7 \rightarrow 1 \quad 1 \rightarrow x^2 + x + 1$$

Addition

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

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

\Rightarrow Result: $x^4 (2)$

Multiplication: $2^3 \rightarrow 1010$

$$x^2 + x + 1$$

$$x^2 + 1$$

$$\overline{x^4 + x^3 + x^2 + x^1 + x^0}$$

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

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

$$\frac{x^3 + x + 1}{x^4 + x^3 + x^2 + x^1 + x^0} \quad \overline{x^4 + x^3 + x^2 + x + 1}$$

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

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

$x+1$

$$x^2 + x + 3x^6 + 2x^5 + 3x^4 + 2x^3 + x^2$$

$$x^3 + x^2 + x^2 + x + 3x^6 + 2x^5 + 3x^4 + 2x^3 + x^2$$

$$\Rightarrow x^3 + x^2 + x^2 + x + 3x^6 + 2x^5 + 3x^4 + 2x^3 + x^2$$

2

$x^3 + x + 1$

$$\begin{array}{r} 1 \\ \times x + 0 \\ \hline x^3 + x \\ x^3 + x + 1 \end{array}$$

(is basis of the field)

and addition by the same procedure should be:

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

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

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

Addition:

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

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

Multiplication:

$$\Rightarrow x^{13} + x^7 + x^6 + x^{11} + x^5 + x^4 + x^{10} + x^9 + x^3 + x^2 + x^8 + x^2 + x^1 + x^5 + x^4 + x^3 + x^1$$

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

$$\begin{array}{r} x^5 + x^3 + 1 \\ \hline x^8 + x^4 + x^3 + x + 1 \left| \begin{array}{r} x^{13} + x^{11} + x^9 + x^6 + x^5 + x^4 + x^2 + 1 \\ x^{13} + x^9 + x^8 + x^6 + x^5 \\ \hline x^{11} + x^8 + x^4 + x^3 + 1 \\ x^{11} + x^2 + x^6 + x^4 + x^3 \\ \hline x^8 + x^7 + x^6 + x^4 + x^3 + 1 \\ x^8 + x^4 + x^3 + x + 1 \\ \hline x^7 + x^6 + x^4 + x^3 + x \end{array} \right. \end{array}$$

Assignment: (Mod 8)

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

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

GR(2⁸)

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

$$g(x) = 4 \Rightarrow x^2 + x + 0$$

$$g(x) = x^2 + x^0$$

$$m(x) = x^8 + x^5 + x^3 + x + 1$$

Addition:

$$\Rightarrow x + 1 (3)$$

Multiplication:

$$\begin{array}{r} \xrightarrow{x+1} x^4 + x^3 + x^2 \\ x^3 + x + 1 \\ \hline x^4 + x^3 + x^2 \\ x^4 + x^2 + x \\ \hline x^3 + x \\ x^3 + x + 1 \\ \hline 1 \end{array}$$

② $f(x) = x^6 + x^5 + x^3 + 1$

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

$$m(x) = x^{13} + x^{12} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

Addition:

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

Multiplication:

$$\Rightarrow x^{13} + x^{12} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

$$\begin{array}{r} \xrightarrow{x^5 + x^3 + x^2 + 1} x^{13} + x^{11} + x^{10} + x^9 + x^7 + x^6 \\ x^8 + x^4 + x^3 + x + 1 \\ \hline x^{13} + 3x^9 + x^8 + x^6 + x^5 \\ x^{11} + x^{10} + x^8 + x^7 + x^5 \\ x^4 + x^7 + x^6 + x^4 + x^3 \\ \hline x^{10} + x^8 + x^6 + x^4 + x^2 \\ x^{10} + x^8 + x^5 + x^3 + x^2 \\ x^4 + x^7 + x^6 + x^4 + x^3 \\ \hline x^3 + x^2 + x + 1 \end{array}$$

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

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

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

9/11/2022

Affine cipher

$$f(x) = \alpha x + \beta \pmod{26} \quad \text{key: } (\alpha, \beta)$$

↓ ↓
 C.T P.T

1. $\alpha \neq 0 \pmod{26}$
 2. $\alpha \neq 26$
 3. $\alpha \neq 0$

constraints:

(i) $\text{GCD}(\alpha, 26) = 1$

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

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

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

$G=6$

$f(x) = 7(6) + 2 \pmod{26}$

$= 44 \pmod{26} \Rightarrow 18$

$= 18$

$\therefore CT = S$

Eg 1: hello

$H=7$

$f(x) = 7x + 2 \pmod{26}$

$= 51 \pmod{26} \Rightarrow 25$

$CT = I$

$E = 4x + 2 \pmod{26}$

$f(x) = 4x + 2 \pmod{26}$

$= 30 \pmod{26}$

$= 4$

$CT = E$

$$L = 11$$

$$\begin{aligned} f(x) &= f(11) + 2 \pmod{26} \\ &= 79 \pmod{26} \\ &= 1 \end{aligned}$$

$$CT = B$$

$$D = 14$$

$$f(x) = 7(14) + 2 \pmod{26}$$

$$= 98 + 2 \pmod{26} = 100 \pmod{26}$$

$$= 22$$

$$CT = N$$

Hello \rightarrow IEBBW

$$\Rightarrow f(x) = ax + b \Rightarrow y \equiv ax + b \pmod{26}$$

$$\Rightarrow x = \frac{y - b}{a} \pmod{26}$$

For z ,

$$z = 25$$

$$\begin{array}{r} 26 \\ \times 25 \\ \hline 26 \\ 52 \\ \hline 15 \end{array}$$

$$\begin{array}{r} 26 \\ \times 2 \\ \hline 52 \\ \hline 1 \end{array}$$

$$15 \times 2 \pmod{26} = 1$$

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

$$\begin{array}{r} x = 4[23] \pmod{26} \quad 15[23] \pmod{26} \\ x = 92 \pmod{26} \quad \Rightarrow 345 \pmod{26} \\ x = 14 \quad \Rightarrow 7 \end{array}$$

I \rightarrow 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	1	26			
15	15	15	15	15	15	15

$$T = T_1 - T_2 \times \text{quotient}$$

$$11 \pmod{26}$$

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	

$$-7 \pmod{26}$$

19

$E \rightarrow 4$

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

$= 4$

$$\boxed{P \cdot T = E}$$

$B \rightarrow 1$

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

$$= -15 \bmod 26$$

$x = 11$

$$\boxed{P \cdot T = L}$$

$N \rightarrow 22$

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

$$= 15(20) \bmod 26$$

$$= 300 \bmod 26$$

14

$$\boxed{P \cdot T = O}$$

ZEBBW → HELLO

Public key cryptography

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

$$E = P_{\text{public}} (P_{\text{pub}} \times X)$$

$$D = (P_{\text{priv}} \times E)$$

Pub - public

P_{priv} - 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 $p \times q$. [such that it should be kept private]

- * Calculate n , $n = p \times q$

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

- * Choose the value e such that $1 \leq e < \phi(n)$

Also make sure, $\text{gcd}(e, \phi(n)) = 1$

- * Calculate d , $d = e^{-1} \pmod{\phi(n)}$

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

- * public key: (e, n)

- * private key: (d, n)

* Encryption formula:

$$C.T = M \pmod{n}$$

$$\therefore M < n$$

* Decryption formula:

$$P.T = C^d \pmod{n}$$

length of msg

Eg:

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

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

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

(iv) $e = 7$

(v) $d = 7^{-1} \pmod{20}$

$$d = 3$$

(vi) $P_{UD} = (7, 33)$

(vii) $P_{UR} = (3, 33)$

$$CT = M \pmod{n}$$

$[1 \leq e < 20]$

$[\nmid \gcd(e, \phi(n))]$

$[e^{-1} \equiv 1]$

$7 \times x \pmod{20}$

$= 1$

$x = 3$

$$= 31^7 \pmod{33} \quad (\text{it's obviously } 31)$$

$$= 31^2 \times 31^2 \times 31^2 \times 31^1 \pmod{33}$$

$$CT = 4$$

$$P \cdot T = C^d \pmod{n}$$

$$= 4^3 \pmod{33}$$

$$P \cdot T = 31$$

Different attacks which can bring down RSA!

* Brute force attack \rightarrow [trying all possible comb]

* Mathematical attack \rightarrow [using factors of pub, we can find private key]

* Timing attack \rightarrow [finding amount of time it take to find its complexity]

* Chosen cipher test attack

[adding blifff cipher into msg
[using the properties of RSA, it
is possible to bring down]]

[add constant
time,
random
delay]

	R	A	B	R ₁	T ₁	T ₂	T
	53	160	31	0	1	-53	

(i) $P = 17 \quad q = 187$

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

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

(iv) $e = 3$

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

$d = 107$

(vi) $P_{ub} = (3, 18^e)$

(vii) $P_{ub} = (3, 18^3) = (3, 512)$

$C_T = M^e \bmod n$

$= 31^3 \bmod 187$

$C_T = 58$

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

$P.T = 71$

28/11/2022 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 .

$a \bmod q, \alpha \bmod q, \alpha^3 \bmod q, \dots, \alpha^{p-1} \bmod q$

\downarrow

1, 2, 3, ..., $p-1$

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

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

$$\begin{aligned}
 k &= (Y_A)^{x_B} \bmod q \\
 &= (\alpha^{x_A} \bmod q)^{x_B} \bmod q \\
 &= (\alpha^{x_A \cdot x_B}) \bmod q \\
 &= (\alpha^{x_B} \bmod q)^{x_A} \bmod q \\
 &= (Y_B)^{x_A} \bmod q
 \end{aligned}$$

\therefore with one key, we can generate another.

Problem

Given $q = 11$, $\alpha = 2$, $x_A = 6$, $x_B = 8$

$$\begin{aligned}
 Y_A &= \alpha^{x_A} \bmod q \\
 &= 2^6 \bmod 11 \\
 &= 64 \bmod 11 \\
 &= 9
 \end{aligned}$$

\therefore $Y_B = \alpha^{x_B} \bmod q$

$$\begin{aligned}
 &\text{most significant bit} = 2^8 \bmod 11 \\
 &= 3
 \end{aligned}$$

$$k = (Y_B)^{x_A} \bmod q$$

$$= 3^6 \bmod 11$$

$$\boxed{x = 3}$$

$$k = (Y_A)^{x_B} \bmod q$$

$$= 9^8 \bmod 11$$

30/11/2022

Module - 3

* ELF

→ static binaries

→ SEL 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

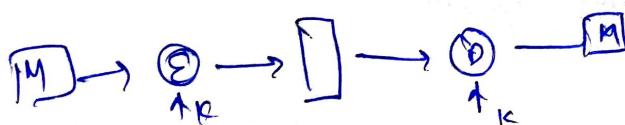
→ low level → authentication

→ hash fn / encryption (MAC)

Frame check reference

Cryptographic checksum

$$\text{MAC} = \text{Enc}_{\text{key}}((K, M))$$



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

Refinery sensors:

Credit card validation

multi level certification:

PKI runs a clock through which a particular digital signature will get expired. So thus, security improving.

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) Expiry (need to be stored in CL)

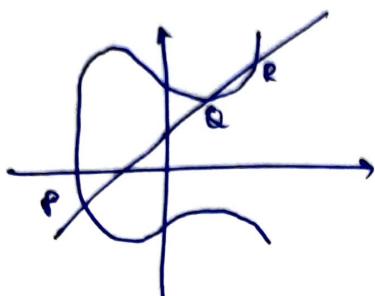
Certification format:

Revision

Root key (root satisfactory certifying key)

Elliptic curve cryptography digital signature

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



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
- * Signature verification
- * signing algo

Digital certificate:

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