Information Security

Page No.
Date 17/1/23

(observing) passive Attack → Attack

Sender → (Internet) → Receiver

⇒ CIA has 3 components :-

Confidentiality → maintained by encipherment (security techniques)

Possible threats [Additional components of CIA]

⇒ Authenticity → sender & receiver are trusted parties

⇒ Accountability

Integrity

Availability (timely & reliable access to system)

* Vulnerable - defined by certain threats : If threats occurs then attack happens

Passive (*)

Active (Immediately convert to attack)

⇒ ARP

⇒ Threats in confidentiality :- → can be achieved using encryption

i) Spoofing

ii) Traffic analysis (passive attack)

Attacker C

packet(T_1) Sender IP(A) MAC(A) — Active attack → Internet → Receiver IP(B) MAC(B)

$T_1 + \Delta y = T_2$

T_2

packet(T_1)

* Attacks in integrity :- (Message)

i) Modification

ii) Masquarding

iii) Replay

iv) Non-Repudiation

v) DOS

ARP Cache

IP	MAC
IP_B	MAC_C
IP_C	MAC_C

Integ. check	Payload

⇒ Message authentication Code (MAC) hash digital signature code

→ Security Technique are used to resist the threats / attacks

→ Two way authentication or OTP (biometric authentication) helps to avoid masquerading.

* Replay :- Preventive mechanism : to prevent
  - forward
  - Backward

  Replay :- Timestamp, ~~Nonce~~ Nonce

→ Network delay (Δy)

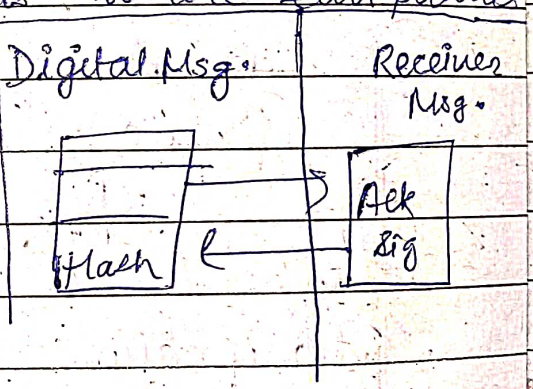
Sender = T_1 if $T_1 + \Delta y \neq T_2$

Receiver = T_2 (pkt is a replay pkt)

→ Non Repudiation :- Integrity threats where ~~can~~ parties can deny which can be prevented using this security technique :-

→ Digital Signature

Hash Code



* Availability :-

Control mechanism → Access Control (Read / write Access)

→ Denial of Service (DOS) is a threat that make the resource unavailable.

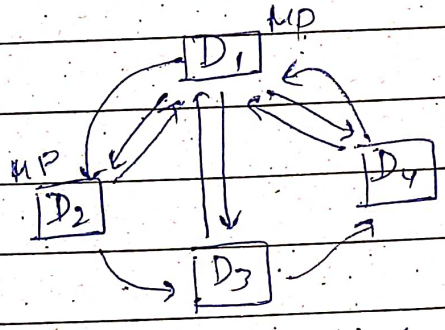
Traffic Padding
Notarization
Routing Control
(ITV)
} Security technique

DDOS → Distributed Denial of Service

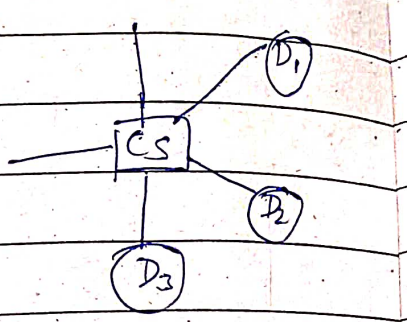
Page No.
Date 24/11/23

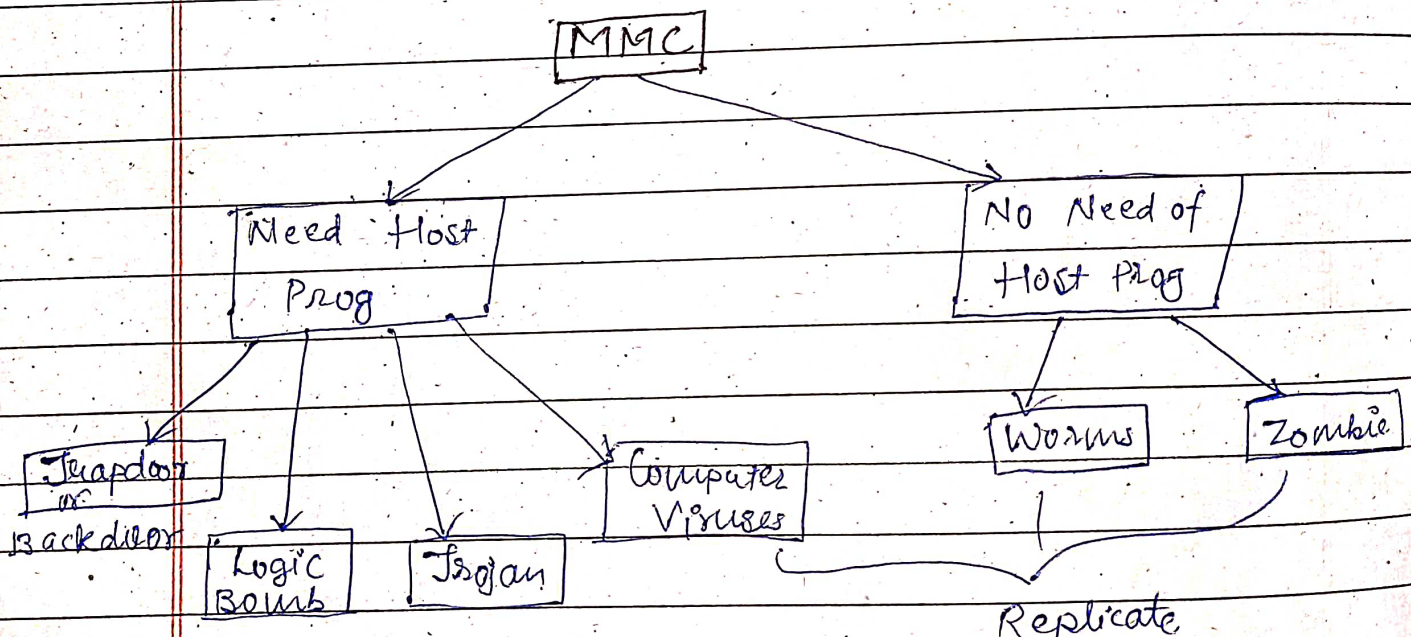
* Threats :-

→ Threat vector (Thread sources / targets, paths)
→ Types of attack (Active & Passive)
→ Malicious Mobile Codes
→ Advanced Persistent threads
→ Manual Attack
→ Has 2 categories :-



Decentralised





IDS :- Intitution detection system

* Trapdoor :- Doors ⟺ ports . Ports are open when connection is being setup . They scan all the ports . Some ports are weak , which are trapped . NP enters the system .

* 3 parts of Malicious Program :-
* infect()
→ if triggered()
→ then Payload()

→ Sneakers
→ Trojan :- Just steal small inf. works mainly with OS.

* Life cycle of Viruses :-
i) Dormant Phase
ii) Propagation "
iii) Triggering "
iv) Execution "

→ Viruses are programs that needs other host programs to replicates throughout the network.

Packet → [Header | Payload] (encryption)
Header: IP address, checksum, flags

1* Bootsector Virus :- It will infect the booting process by copying itself into the master booting block of hard disk

2* Executable File Infectors :- It infects files which the OS considers to be executable.

3. Overwriting Virus :- It overwrite the target

Creeper – 1st computer virus | Morris Worm – 1st worm

Ransome ware

files.

V.V.I Polymorphic & Metamorphic :- It is actually a complicated virus that affect data types and functions. It is in encrypted form.

Metamorphic can transform due to ability to edit and rewrite their own code. It is very dangerous virus.

→ Spam Bots

→ Mail ,,

→ Spoofing , Social Engineering ,

→ How to generate thread vector? How to generate path?

* Information Security

→ Goal :- CIA

→ Services :- Authentication (→ Entity Authentic. / Message ,,) , Authorization , Non Repudiation , Integrity , Access control

→ Technique :-

→ Threats / Attacks :- Traffic Monitoring } → affect confidentiality
Spoofing

Integrity threats → { Eavesdroping
Impersonation
Replay
Non-repudiation
Msg : Modification

1760 × 2 = 3520

2740 1760 980

Page No.
Date 31 | 1 | 23

Availability threats → { DOS, DDOS }

Security Techniques

Cryptography : Msg is concealed by using certain technique so that it will convert in a readable form

steganography → Msg is concealed by covering it some-thing else

⇒ Cryptanalysis :- Creating cipher and breaking cipher
→ Brute force attack

Integer Arithmetic

Set Integers → $Z = \{-2, -1, 0, 1, 2, 3, \dots\}$

Fact 1 :→ $\gcd(a, 0) = a$

Fact 2 :→ $\gcd(a, b) = \gcd(b, r)$, where r is the remainder of dividing a by b.

EA $r_1 = 2740$ $r_2 = 1760$

Eg :→

q	r_1	r_2	r
1	2740	1760	980
1	1760	980	780
1	980	780	200
3	780	200	180
1	200	180	20
9	180	20	0
	20	0	

(3)

∴ gcd(20, 0) = 20

→ continue until $r_2 = 0$ if so then gcd(2740, 1760) = 20

161 / 140 / 21   21 4 ×8 168   28 ×4   28 4 ×5 140   23 ×2 46   14)18(1 14

Eg. → gcd(36,10) = gcd(10,6) = gcd(6,4) = gcd(4,2) = gcd(2,0) = 2

→ when gcd(a,b) = 1, we say that 'a' & 'b' are relatively prime.

* Extended Euclidean Algorithm:-

$s = s_1 - q \times s_2$ $t = t_1 - q \times t_2$

$r = r_1 - q \times r_2$

given, A = 161   B = 28   find S & T and GCD.

$r_1 = A$ $r_2 = B$ (fixed & assigned)

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
5	161	28	21	1	0	1	0	1	-5
1	28	21	7	0	1	-1	1	-5	6
3	21	7	0	1	-1	4	-5	6	-23
	7	0		-1	4		6	-23	

$s = s_1$ $t = t_1$

$s = -1$ $t = 6$

GCD = 7

s = -1.

s = 1 - 5×0 = 1 - 0 = 1

s = 0 - 1×1 = -1

s = 1 - 3×(-1) = 1 + 3 = 4

t = 0 - 5×1 = -5

t = 1 - 1×(-5) = 1 + 5 = 6

t = 1 - 1×(-1) = 1 + 1 = 2

t = -1 - 3(2) = -1 - 6

t = -5 - 3(6) = -5 - 18

verify: $s \times a + t \times b = gcd(a,b)$

-1×161 + 6×28 = 168 - 161 = 7 = gcd(a,b)

* Modular arithmetic :- A modular operator can be converted into a binary operator with 2 input a & b and output 'r' remainder.

27 mod 5 = r = 2 (can be (-)ve)

36 mod 12 = 0

* Cryptography :-

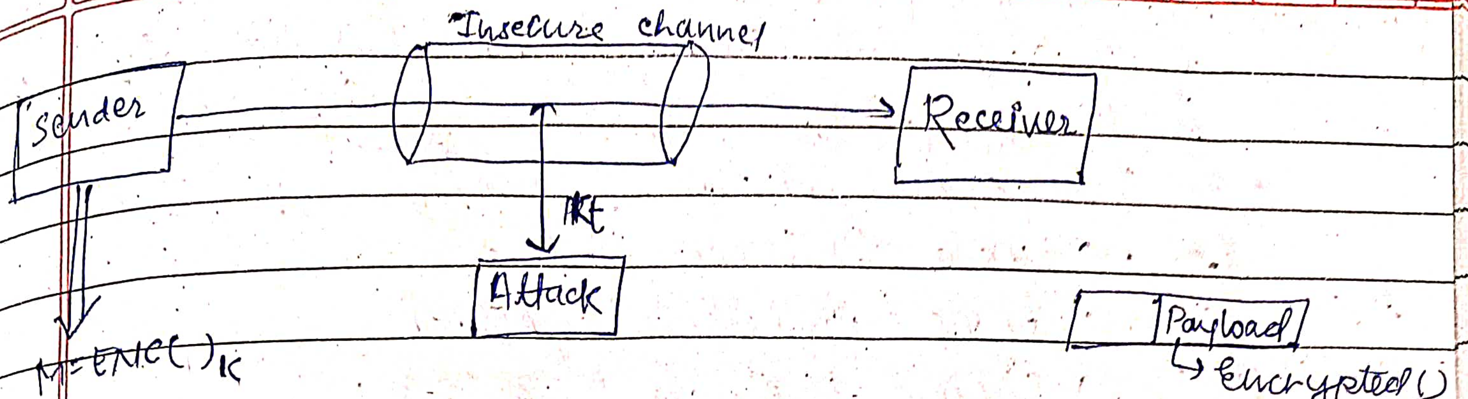
It is used for data security.

eg.2 → -18 mod 14 = -4, -4 + 14 = 10 = r

-7 mod 10 = -7, -7 + 10 = 3 = r

28 4 × 6 = 168

6) 25 (0 / 25



Eg. 2. If $r_1 = 25$, $r_2 = 60$. Find gcd(25, 60).

q	r_1	r_2	r
0	25	60	25
2	60	25	10
2	25	10	5
2	10	5	0
	5	0	

∴ gcd(25, 60) = 5.

(Msg)
plainText = EN((Msg)$_K$ = Cipher text

key will help the message to transfer into an unreadable form [ciphertext].

(Msg)
Plaintext = EN((Msg)$_K$ = Cipertext

Msg → (ATTACK TONIGHT) $K \to 3$ = (DWWDFN _ _)

→ Crypt Analysis is done by attacker.

Two types of attack :-

i) Bruteforce Attack :- Attacker tries all possible values/key in keyspace.

* To break cipher

ii) CryptoAnalysis is the decryption and analysis of codes, ciphers or encrypted text.

*Brute-force attack :- Trying every possible key, until an intelligible translation of the ciphertext into plaintext is obtained.
→ guessing
→ Exhaustive key search
→ CAPTCHA is one way to avoid brute force
[Completely Automated Public Turing test to tell Computers and Human Apart]

- Ciphertext Only Attack (it is a type of cryptanalysis)
  - Bruteforce (key implementation)
  - Statistical (frequency-related)

Types of cryptanalytic attack:
- → Known Plaintext Attack
- → Chosen Ciphertext Attack
- → Chosen Plaintext Attack

*Residue Set
Relationship comes under congruent
Additive Property = $a+b \equiv 0 \pmod n$
Multiplicative " = $a \times b \equiv 1 \pmod n$
$a+b \equiv 0 \pmod n$
If $n=5$ & $a=2$, $b=?$
$2+3 = 5 \bmod 5 = 0$
So, $b=3$ is called additive inverse of 2 in (mod 5)

Extended Euclidean → $s \times a + t \times b = \gcd(a,b)$
Algorithm

q, r $s \times a + t \times b = \gcd(a,b)$
(s_1 s_2) (t_1 t_2)

q	a	b	r	s_1	s_2	s	t_1	t_2	t
2	160	79	2	1	0	1	0	1	-2
39	79	2	1	0	1	-39	1	-2	79
2	2	1	0	1	-39	79	-2	79	-160

MI of 79 = 160
i.e., $\frac{a \times b}{160} = 1 \pmod{79}$
$1 \times 160 + 1 \times 79$

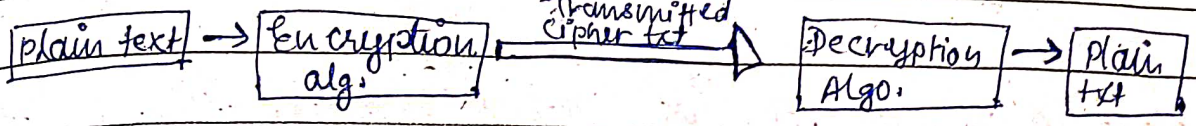
1. Find gcd of 740×1760

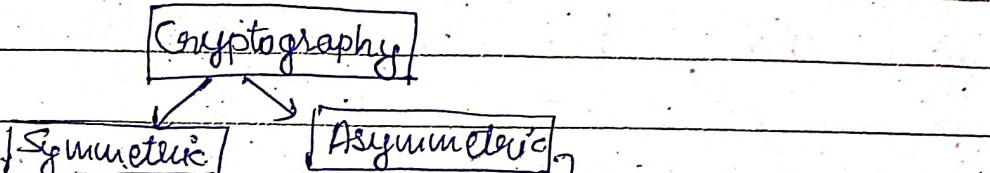
Page No.
Date

2. Find gcd of 25 x 60.

// Find MI of 11 in 226.

* Cryptography :- Method which converts plain text to cipher text and vice-versa.





That key is private

same key is used by encryption & decryption alg.

Key used for encryption is diff. from key used for decryption

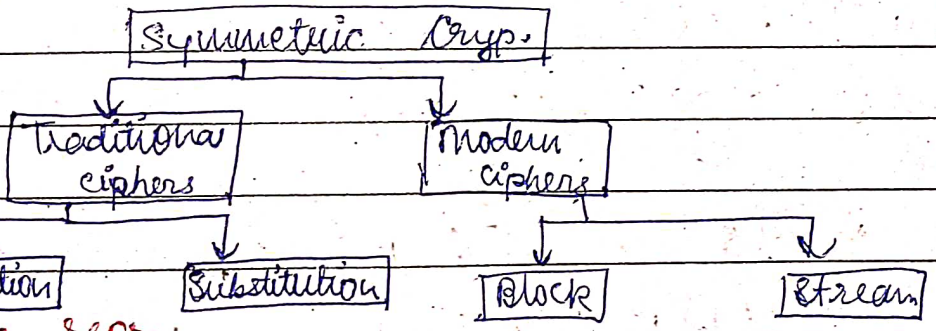
Encryption :- converting ↑ plain text to cipher text and decryption is reverse of it.

Pup. from

Both encryption & decryption are performed using algorithm. Also a key, which shouldn't be compromised.

→ Two keys used in asymmetric ~~alg~~ are :-

i) Public key ii) Private key



It involves the reordering of the elv. from one position to another position

* Cipher :- a secret code alg. that helps to perform encryption & decryption

In cryptography, $\equiv \Leftrightarrow$ congruence

$(a+b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$

Ajanta
Page No.
Date

(Z_n), Reduced set (Z_n^*) → set of values in Z_n which has MI.

* Set of Integers → In modular arithmetic, set of integers are visualised as set of least residues (Z_n)
  - Additive Inverse (relative to add^n operation) {for each element}
  - Multiplicative Inverse (relative to multi operation) {for each element}

* Lemma 1:- In a set of least residue (Z_n) all elements having their additive inverse.

* Lemma 2:- In a set (Z_n) the elements may or may not have their multiplicative inverse.

Proof (1):- $a+b = 0$

$Z_6 = \{0,1,2,3,4,5\}$

$1+x = 0 \pmod 6$ → all the no. are taken from this set only

∴ Additive pairs = $\{(1,5), (2,4), (3,3), (4,2), (5,1)\}$

Add Inverse in Z_{10} are $\{(0,0), (1,9), (2,8), (3,7), \ldots\}$

⇒ **Proof (2):-** $a \times b = 1 \pmod n$ holds if a & b are MI of one other

⇒ $\{2 \times x\} \bmod 6 = 1$ ⇒ NO MI in set

⇒ $\{3 \times x\} \bmod 6 = 1$ ⇒ No. MI "

MI exist if $\gcd(n, a) = 1$

∴ $(5 \times 5) \bmod 6 \equiv 1$ ∴ 5 and 5 are M.I.

Also $(1 \times 1) \bmod 6 \equiv 1$

So, Reduced set = $\{1,5\}$ ⇒ $Z_n^* \rightarrow Z_6^*$

* Lemma (3):- An element b in Z_n have a multiplicative Inverse if and only if

$\gcd(b \times n) = 1$; element 11 in Z_{100}

↓

So, ... any

→ Additive Inverse :- In Z_n AI is $b = n - a$ (7) 100 (
→ Two no. are a & b are A.I. if $a+b = 0 (\bmod n)$
A.I :- $[(a+b) \bmod n] = 0$
only if $a+b = n$ ∴ $b = n-a$

Page No.
Date

Euclid Concept :- $(s \times a) + (t \times b) = \gcd(a, b)$
Ex. also helps to find M.I

$(s \times n) + (t \times b) = 1$

$[(s \times n) + (t \times b)] \bmod n \equiv 1 \bmod n$

⇒ $[(s \times n) \bmod n + (t \times b) \bmod n] = 1 \bmod n$
(multiple of n)

⇒ $0 + (t \times b) \bmod n] = 1$

⇒ $(t \times b) \bmod n = 1$

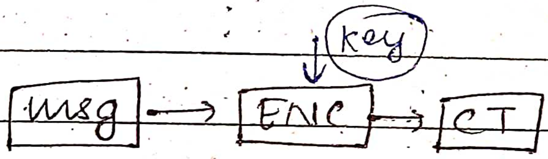
q	r_1 (n)	r_2 (a)	r	t_1	t_2	t
9	100	11	1	0	1	-9
11	11	1	0	1	-9	100
	1	0	0	-9	100	

once remainder is 0 transfer those values and mark

$(-9) \bmod 100 = 1$

$91 \bmod 100 = 1$

M.I. is equal to t_1



1) Substitution method :- It is a technique where we substitute some particular characters with some other characters/symbols.

- → Monoalphabetic Cipher (one to one)
  - → Caeser Cipher
- → Polyalphabetic Cipher (one to many)
  - → Playfair "
  - → Hill "
  - → One-Time Pad

The difference b/w plaintext & ciphertext is not uniform for all the characters.

Monoalphabetic Cipher — 2 parts:

Additive Cipher	Multiplicative Cipher
If key is 'K'	$(P \times K) = C$
Enc eqn is $P+K = C$	$(C \times K)^{-1} = P$
Dec " " $C+K = P$	

$(5x) \bmod 26 = 1$

0	1	2	3	4	5	6
A	B	C	D	E	F	G
7	8	9	10	11	12	13	14	15
H	I	J	K	L	M	N	O	P
16	17	18	19	20	21	22	23	24
Q	R	S	T	U	V	W	X	Y
25								
Z								

H E L L O
↓ ↓ ↓ ↓ ↓
7 4 11 11 14

Additive If key = 3

Possibilities :-

H → (7+3) mod 26 = 10 = K → (10-3) mod 26 ⇒ 7 mod 26 = H

E → (4+3) " = 7 = H → (7-3) mod 26 ⇒ 4 mod 26 = E

L → (11+3) " = 14 = O → (14-3) mod 26 ⇒ 11 mod 26 = L

L → (11+3) " = 14 = O → (14-3) mod 26 ⇒ 11 mod 26 = L

O → (14+3) " = 17 = R → (17-3) mod 26 ⇒ 14 mod 26 = O

Multiplicative MI of 3

H → (7x3) mod 26 = 21 mod 26 = 21 = V ⇒ 21x9 mod 26 = 189 mod 26 = 7 → H

E → (4x3) " = 12 " = 12 = M ⇒ 12x9 " = 108 " = 4 → E

L → (11x3) " = 33 " = 7 = H ⇒ 7x9 " = 63 " = 11 → L

L → (11x3) " = 33 " = 7 = H ⇒ 7x9 " = 63 " = 11 → L

O → (14x3) " = 42 " = 16 = Q ⇒ 16x9 " = 144 " = 14 → O

$(11x) \bmod 26 = 1$

* Find MI of cipher where K = 11 & Z26 — 7 mod 26 = 19 ∴ MI = 19

and message is 'ATTACK TONIGHT'

MI is found using extended euclidean

→ A → (0x11) mod 26 = 0 = A ⇒ (0x19) mod 26 = 0 = A

T → (19x11) " = 1 = B ⇒ (1x19) mod 26 = 19

T → (19x11) " = 1 = B ⇒ (1x19) " = 19

A → (0x11) " = 0 = A ⇒ (0x19) " = 0

C → (2x11) " = 22 = W ⇒ (22x19) " = 2

K → (10x11) " = 6 = G ⇒ (6x19) " =

T → (19x11) " = 1 = B ⇒ (1x19) " = 19

O → (14x11) " = 24 = Y ⇒ (24x19) " = 14

N → (13x11) " = 13 = N ⇒ (13x19) " =

I → (8x11) " = 10 = K

G → (6x11) " = 14 = O

eg. $\rightarrow Z_6 = \{0,1,2,3,4,5\}$ $Z \rightarrow$ set of Integers

and $Z_n^* = \{1,5\}$ $Z_n \rightarrow$ set of least residual set.

means MI exist for when applied on modulo.

1 & 5 i.e. $\gcd(6,1)=1$ $\gcd(6,5)=1$ ✓

Ajanta

Page No.

Date

* Affine Cipher :-

→ Additive Key = K_2

→ Multiplicative Key = K_2

* Bruteforce attack are very vulnerable can happen by applying hit & trial value on key. So, additive cipher are bruteforce. also multiplicative

Ciphering Process $\begin{cases} (P \times K_1) \bmod 26 = T \\ (T + K_2) \bmod 26 = C \end{cases}$

H E L L O

↓ ↓ ↓ ↓ ↓

7 4 11 11 14

H → $(7 \times 3) + 2 \bmod 26 = 23 \bmod 26 = 23 = X$

E → $(4 \times 3) + 2$ " $= 14$ " $= 14 = O$

L → $(11 \times 3) + 2$ " $= 36$ " $= 9 = J$

L → $(11 \times 3) + 2$ " $= 36$ " $= 9 = J$

O → $(14 \times 3) + 2$ " $= 44$ " $= 18 = S$

$$\boxed{(C - K_2) \times K_1^{-1} \bmod 26 = P}$$

$a \longrightarrow e$

frequency analysis

(CipherText) CT → L T I K C P N P D L J T

L → 2. C → 1

T → 2

I → 1

K → 1

v.v.i

* Use a bruteforce attack to decipher the following message —

XPALASXYFGFUKP

The cipher technique is affine cipher where 'ab' is cipher to 'GL'.

Positional value of

→ Contain 2 key —

$(P \times K_1) + K_2 = C$

$(C - K_2) \times K_1' = P$

1) Bruteforce Attack :- To lessen the attack confusion is made on the key

Statistical attack :- Hide the frequency of symbol

→ Polyalphabetic Cipher uses a key matrix

(D)IAMON(D) → key

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

* Polyalphabetic :-

1) A bruteforce attack to decipher the following message —

XPALASXYFGFUKP

The cipher technique is affine cipher where 'ab'

is cipher to 'GL'.

$(P \times K_1) + K_2 = C$

$(C - K_2) \times K_1^{-1} = P$

these sets of values — eliminate then reach to 1.

a → G b → C

00 → 06 01 → 11

$00 \times K_1 + K_2 \equiv 6 \pmod{26}$ — (1)

$01 \times K_1 + K_2 \equiv 11 \pmod{26}$ — (11)

$\boxed{K_2 \equiv 6 \pmod{26}}$ $K_1 = 5$

$\boxed{K_1 + K_2 \equiv 11 \pmod{26}}$ $K_2 = 6$

$\Rightarrow 2K_1 + K_2 \equiv 6$

$K_1 + K_2 \equiv 11$

$$\begin{pmatrix} K_1 \\ K_2 \end{pmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}^{-1} \begin{bmatrix} 6 \\ 11 \end{bmatrix} \pmod{26}$$

This is modular arithmetic

*Brute force & Statistical Attack :-

↓ confusion mode. ↓ hide the freq. of symbol

on the key

eg. → DIAMOND → key (3)

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

I/J

et → WC

et → WF

* Mono → Poly

PT → H E L L O

mono → one to one.

* Playfair → Take key phrase

DIAMOND (matrix size is fixed)

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

Assumption:- I & J are found very much same in frequency in literature, so don't take it differently

eg. → THIS IS MY FIRST CLASS

If in same column circular upto down next element

TH IS IS MY FI RS TC LA SX → 11

RL AR AR EM BD ST SE KM XA

HE LL O → HE LX LO

* Vigenere :- 1 2 9 11 → key

1 2 9 11

1	2	9	11

1	2	9	11

1	2	9	11

TH	IS	IS	MY	FIRST	CLASS
19 7 8 18		9 18	12 25	5 8 17 18	
⊕ ⊕ ⊕ ⊕		⊕ ⊕	⊕ ⊕	⊕ ⊕ ⊕ ⊕	
1 2 9 11		1 2	9 11	1 2 9 11	
20 9 17 29		9 20	21 35	6 10 26 29	
(mod 26) 20 9 17 3		9 20	21 9	6 10 0 3	
CT → V J R D		J V	V		

Page No.
Date

et → WC

Q. e → W t → C
4 22 19 2

$(P \times K_1) + K_2 = C \pmod{26}$

$(4 \times K_1) + K_2 = 22 \pmod{26}$ — ①

$(19 \times K_1) + K_2 = 2 \pmod{26}$ — ②

② − ①

$15K_1 = -20 \pmod{26}$

or $\begin{bmatrix} 4 & 1 \\ 19 & 1 \end{bmatrix}^{-1} \begin{bmatrix} 22 \\ 2 \end{bmatrix} = \begin{bmatrix} K_1 \\ K_2 \end{bmatrix}$

$\frac{adj\,A}{|A|} \Rightarrow \frac{1}{15}\begin{pmatrix} 4 & -1 \\ -19 & 1 \end{pmatrix}\begin{pmatrix} 22 \\ 2 \end{pmatrix}$

$\Rightarrow \frac{1}{15}\begin{pmatrix} 88-2 \\ -418+2 \end{pmatrix} \Rightarrow \begin{pmatrix} 86 \\ -416 \end{pmatrix} \times \frac{1}{15} = \begin{matrix} K_1 \\ K_2 \end{matrix}$

Q. et → WC (cipher text) — ①

et → WF " — ①

Algo is affine

For ①

e → W t → C
04 22 19 02

$(04 \times K_1 + K_2) = 22 \pmod{26}$

$19 \times K_1 + K_2 = 02 \pmod{26}$

$\begin{bmatrix} K_1 \\ K_2 \end{bmatrix} = \begin{bmatrix} 4 & 1 \\ 19 & 1 \end{bmatrix}^{-1} \begin{bmatrix} 22 \\ 2 \end{bmatrix} = \begin{bmatrix} 19 & 7 \\ 3 & 24 \end{bmatrix} \begin{bmatrix} 22 \\ 2 \end{bmatrix}$

$= \frac{adj\,A}{|A|}$

$= \begin{bmatrix} 16 \\ 10 \end{bmatrix}$

Page No.
Date 11/2/23

So, $K_1 = 16 \quad K_2 = 10$

Now, $\gcd(16, 26) = 2$

For ②

e → W t → F

04 → 22 19 05

$(4K_1 + K_2) \equiv 22 \pmod{26}$

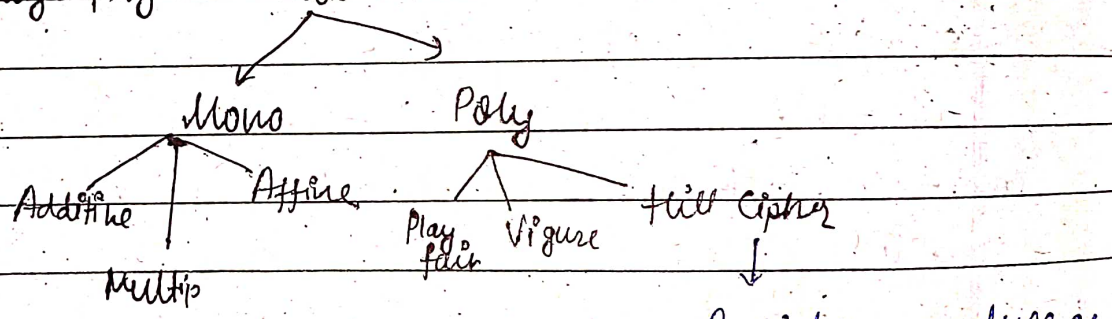
$19K_1 + K_2 \equiv 5 \pmod{26}$

$$\begin{bmatrix} K_1 \\ K_2 \end{bmatrix} = \begin{bmatrix} 4 & 1 \\ 19 & 1 \end{bmatrix}^{-1} \begin{bmatrix} 22 \\ 85 \end{bmatrix} = \begin{bmatrix} 19 & 7 \\ 3 & 24 \end{bmatrix} \begin{bmatrix} 22 \\ 5 \end{bmatrix}$$

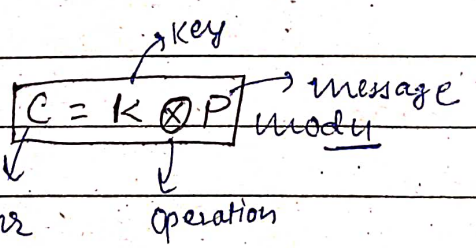
$$\begin{bmatrix} K_1 \\ K_2 \end{bmatrix} = \begin{bmatrix} 49 & 7 \\ 3 & 24 \end{bmatrix} \begin{bmatrix} 22 \\ 5 \end{bmatrix} = \begin{bmatrix} 11 \\ 4 \end{bmatrix}$$

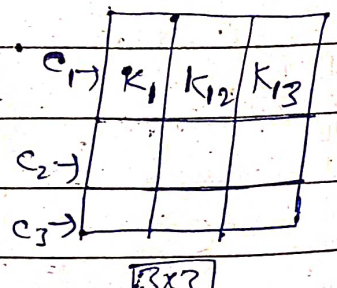
So, $K_1 = 11, \; K_2 = 4$

Cryptography → Substitution cipher



A cipher produce as a block





3x3

$$\begin{aligned} C_1 &= P_1K_{11} + P_2K_{12} + P_3K_{13} \\ C_2 &= P_1K_{21} + P_2K_{22} + P_3K_{23} \\ C_3 &= P_1K_{31} + P_2K_{32} + P_3K_{33} \end{aligned}$$

S → R
CT
AT

$$\begin{bmatrix} C_1 \\ C_2 \\ C_3 \end{bmatrix} = \begin{bmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{bmatrix} \times \begin{bmatrix} P_1 \\ P_2 \\ P_3 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \times \begin{bmatrix} P_1 \\ P_2 \\ P_3 \end{bmatrix} \text{ mod } 26$$

ENC ⇒ $C = KP$

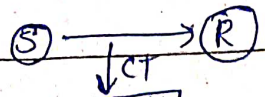
DEC ⇒ $P = K^{-1}C$

K

$$K^{-1} = \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix}$$

Plain Text → PAY MORE MONEY

$$\begin{bmatrix} C_1 \\ C_2 \\ C_3 \end{bmatrix} = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \begin{bmatrix} 15 \\ 0 \\ 24 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 17\times15+0+120 \\ 21\times15+0+21\times24 \\ 30+0+19\times24 \end{bmatrix} = \begin{bmatrix} 11 \\ 13 \\ 18 \end{bmatrix}$$



CT → HC(R 7)(S S)XNSP S → E
↓↓↓↓ ↓ ↓ ↓ 18 ↷ 4
1 1 1 1 3 1 1

H C
7 2

(H C) → C

(H I) → P

(7 8) K mod 26 = (7 2)

(11 1) K mod 26 = (17 25)

$$\begin{bmatrix} 7 & 8 \\ 11 & 1 \end{bmatrix} K \bmod 26 = \begin{bmatrix} 7 & 2 \\ 17 & 25 \end{bmatrix}$$

Applying some sort of permutation on the plaintext letters
↳ Eg. → NESO Ciphertext :- ESON, SONE, ONES, ENOS, etc.

(2) Transposition Cipher → reordering so change of position / more effective if plaintext length is big.

Types :-
⇒ Rail Fence
⇒ Row Column Transposition

Input string → 0 1 0 0 1 0 0 1 0 1

Output string → 0 0 0 1 1 0 0 0 1 1

1's = 4

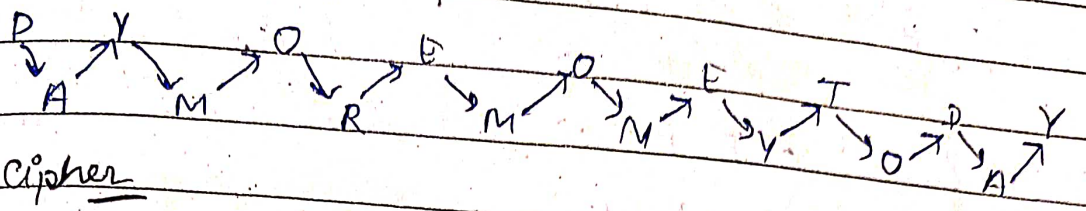
0's = 6

* Diffusion & Confusion :-

Diffusion ↓ hide the relationship between the cipher & the plain text.

Confusion ↳ hide the relationship b/w the cipher & the key

PT → PAY MORE MONEY TODAY



Keyless Cipher

CT: P Y O E O T D Y A M R M N Y O A

* With a key:-

(2 1 3 5 4) → 5 values so 5 columns

(2 1 3 5) → 4 values 4 column

ENC ↓ key → [2 1 3 5 4] ↑ DEC → Blocks of operations (S Box), (P Box/D Box)

Indx → [1 2 3 4 5]

3 bit S Box

Eqn

P	A	Y	M	O
R	E	M	O	N
E	Y	T	O	D
A	Y	X	Y	Z

Rowwise → 3 cell values will be predefined

↓↓

A	P	Y	O	M
E	R	M	N	O
Y	E	T	D	O
Y	A	X	Z	Y

Columnwise generated text will be cipher

→ AEYYPREAYMTXONDZMOOY

→ For double transposition repeat this steps once more treating last CT as PT for new steps.

(C, P) Input → X
(y, x) Output → y
Key → K

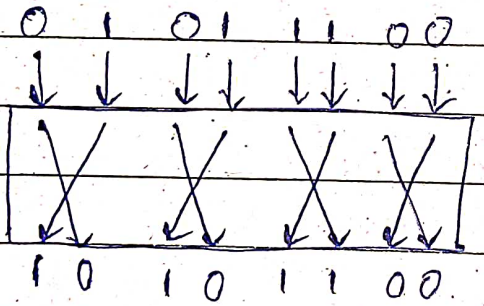
$\Rightarrow P + K = C$

$x_1 + K_1 = y_1$

$x_2 + K_2 = y_2$

$x_3 + K_3 = y_3$

* Building Blocks of Modern ciphers:-
→ Block size
→ key size
→ Round no.
→ SBOXS / DBOXS
→ OPERATIONS (SWAP, SHIFT, Inverse)

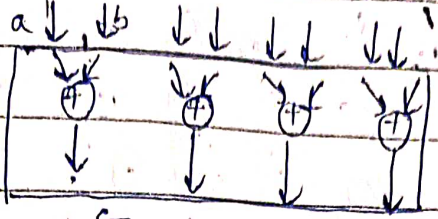


S + D BOX Straight DBOX
Compression & Extension

* Three types of DBox :-
i) Straight DBOX
ii) Compressed ,,
iii) Extended ,,

If $a \oplus b = c$
then $c \oplus b = a$

PT → 0 1 0 1 1 1 0 0 [Compressed DBox]

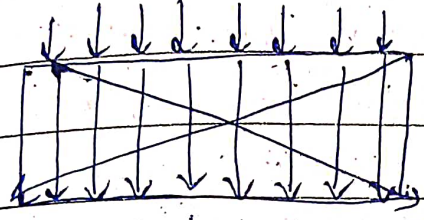


$a \oplus b = c$

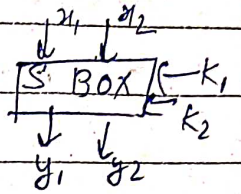
$c \oplus a = b$

PT → 8-bit [Extended DBox]

0 1 0 1 1 1 0 0



0 0 1 0 1 1 1 0 0 0 (10-bit)



0101 1010 1100 Extended D-Box some bits are appended (Bit-Stuffing)

* Assignment :-

i) Design an affine cipher where the key depend on the position of the character in plaintext. If the character to be encrypted is in position i. We find the key as

MI key is $(i^2 \bmod 12)$ th element in Z_{26}^*

Addition " " $(i^2 \bmod 26)$ th " " Z_{26}

Encrypt the message "PAY MORE MONEY".

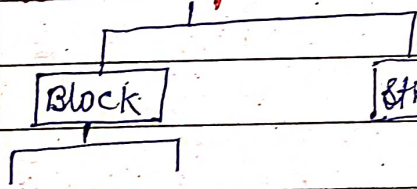
Ajanta
Page No.
Date 17/2/23

$Z_{26}^* = \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$

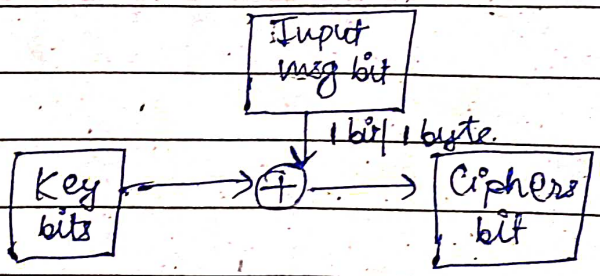
		M. key $K_1 (i \bmod 12)$	A. key $K_2 (i \bmod 26)^{th}$
15	P	3rd → 7	15
0	A	0 → 1	0
24	Y	0 → 1	24
12	M	0 → 1	12
14	O	2 → 5	14
17	R	5 → 11	17
4	E	4 → 9	4
12	M	0 → 1	12
14	O	2 → 5	14
13	N	1 → 3	13
4	E	4 → 9	4
24	Y	0 → 1	24

	CT
K_1^{-1}	$(P \times K_1) + K_2$
15	120 mod 26 = 16 → Q
1	0 mod 26 = 0 → A
1	48 mod 26 = 22 → W
1	24 mod 26 = 24 → Y
21	204 mod 26 = 22 → W
19	40 mod 26 = 14 → O
3	24 mod 26 = 24 → Y
1	84 mod 26 = 6 → G
21	52 mod 26 = 0 → A
9	40 mod 26 = 14 → O
3	48 mod 26 = 22 → W
1	

* Modern ciphers :-



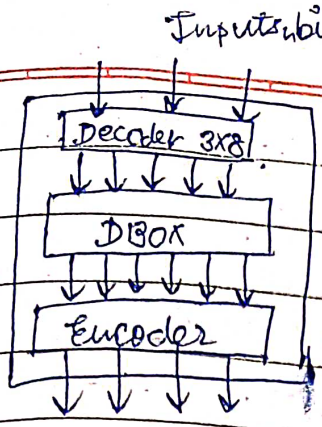
* Components :-
→ Block size
→ key → small size key → b
→ S Box
→ D Box
→ Operations
SWAP SHIFT Invert



→ Round structure (to train cipher)

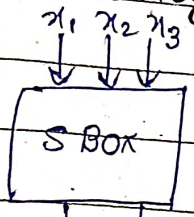
1024
X 64
4096
6144
65536

Page No.
Date



→ n bits (Input)
→ 2^n bits (Output)
single 1
$(2^n - 1)$ no. of 0's

* Product Cipher (Key Mixer, S Box, DBox)



Linear S Box ← $y_1 = x_1 \oplus x_2 \oplus x_3$, $y_2 = x_1 \oplus x_3$

Non-linear → $y_1 = x_1 \cdot x_2 \oplus x_2 \cdot x_3$, $y_2 = x_1 x_2 x_3$

(01010000) · (10010001)
$(x^5 + x^3)$ $(x^7 + x^4 + 1)$

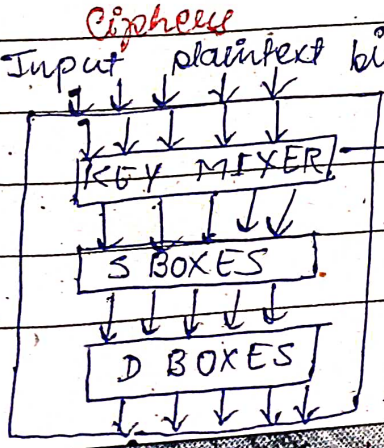
1) 6 5 3 1 2 4
INDEX → 1 2 3 4 5 6

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

brute force attack
(easily breakable)

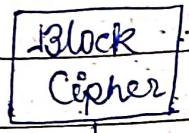
3) 4 5 3 6 2 1 Avelanche {input & output are diff}

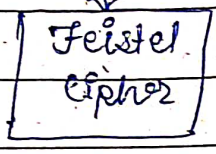
* Product Ciphers

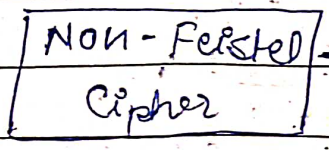


Round key
K bits

DES → finished in 21st is the syllabus midsem.







→ don't have feistel func

* Feistel Ciphers:-