Date: Day: M T W T F S

IS-01 (16/01/23)

Cryptography:

msg → Cipher Text (so only intended person can read text)

⇒ Symmetric Encryption same key.

- Encrypts block or stream (of any size) of data.

⇒ Assymmetric Encryption.

- Encrypts small block of data.
- private + public key

⇒ Data Integrity

- protects block of data from alteration.

⇒ Authentication

- authenticate identity of user.

deter ⇒ delay / deterioriate (e.g security guard with gun)

prevent ⇒ security measures.

detect ⇒ detect if security measures are breached.

Authenticity:

- Information is authentic
- Source is authentic.

Date: Day: M T W T F S

Accountability:

- Source is accountable for info.

Task: 10 Domains of IS (details)

ISF-02 (17/01/23)

- No lec.

10 domains of IS.

Information security encompases various domains to address the different aspects of protecting information & systems. Here are 10 key domains of information security.

1- Access Control: This domain involves managing and controlling access to information system and data. It includes authentication, authorization and accountability mechanisms to ensure that only authorized individuals can access specific resources.

eg biometric, card. - level of access

1) Verification 2) Authentication 3) Access Control List:

Date: Day: M T W T F S

2) Network Security: Network security focuses on protecting the integrity, confidentiality and availability of data as it is transmitted over networks. This includes measures such as firewalls, intrusion detection and prevention systems and virtual private networks (VPNs).

3) Cryptography: Cryptography involves the use of mathematical techniques to secure communication and protect information from unauthorized access. It includes encryption, decryption and key management.

4) Incident Response: This domain is concerned with the development and implementation of processes and procedures to handle and respond to security incidents. It aims to minimize damage and reduce recovery time in the event of a security breach.

Date: _____ Day: M T W T F S

5) Security Governance and Compliance: Governance and compliance involve the development and enforcement of security policies, procedures and standards to ensure that an organization's information security practices align with regulatory requirements and industry best practices.

- **6) Security Architecture & Design (Model):** This domain focuses on designing and implementing a secure information infrastructure. It includes considerations for hardware, software, networks and other components to ensure a robust and secure architecture. - reference model with benchmarking.

- **7) Physical Security:** Physical security addresses the protection of physical assets, such as data centers, servers and other critical infrastructure from unauthorized access, theft or damage.

Date: Day: M T W T F S

8) Security Awareness & Training: Human factors play a crucial role in info security. This domain involves educating & training individuals within an organization to recognize and mitigate security threats, emphasizing the importance of security best practices.

9) Application Security: Application security involves measure to secure software applications from potential threats and vulnerabilities. This includes secure coding practices, code reviews and testing to identify and remediate security flaws.

10) Security Risk Management: This domain involves the identification, assessment and management of security ~~for~~ risks to an organization's info assets. It includes risk analysis, risk migration strategies and the development of a risk management framework.

Date: Day: M T W T F S

IS-03 (23/01/24)

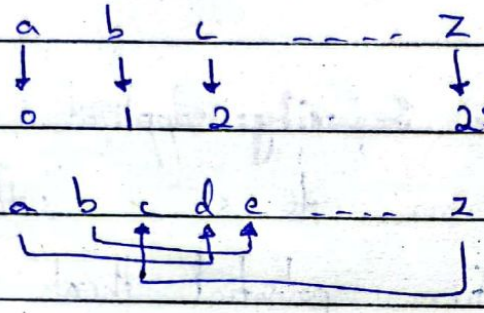
- 10 domains of IS.

IS-04 (24/01/24)

Ceaser Cypher:

Plain Text: meet me after the toga party.

Cipher Text: PHHW PH DIWHU WKH WRJD SDUWB.



Using Modulo Math:

$C = E(3, p)$

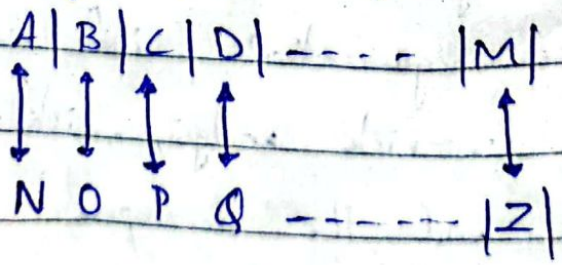
$= (p+3) \bmod 26$

$p = D(k, C)$

$= (C-k) \bmod 26$

Ceaser Cipher (ROT-13)

$26/2 = 13$



Date: Day: M T W T F S

P.T = hello.

→ C.T = uryyb. } same method to decrypt

→ Issue: key can be detected by brute force attack.

Substitution (Mono Alphabetic)

random key for each alphabet,

unique combinations

A = B → k = +1

B = V → k = +20

C = G → k = +4.

D = Q → k = +13.

substitution with keyword:

keyword: KEYWORD.

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

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

1st step 2nd Step.

⇒ Don't repeat char in C.T.

⇒ Any keyword can be used which has no repeating char.

→ enhancement of substitution method.

Date: Day: M T W T F S

- P.T → alkindi

  C.T → kqfbiwb.

Issue: some char have more freq of occurence. so finding keyword is possible (not easy) by hit & try method.

Homophone Cipher:

⇒ Multiple chars against 1 char for encryption.

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

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

9 7 3 50 46

2

1

⇒ **Decrypt the cipher:**

C.T	F7E25F	UCZ	1DRE	MAPP	OE	SD4UP1
P.T	DEFEND	THE	EAST	WALL	OF	CASTLE

Date: Day: M T W T F S

Playfair Cipher:

→ Diagraph substitution cipher.
↳ (pair of 2)

keyword : MORARCHY.

→ Matrix 5x5 → 25 char but 26 total.

→ I/J replacement.

→ Repeating letter → (x)
↑
filler letter

→ to pair use "x" or "z"

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

- Hellow.
- Helxlowz

⇒ K.W ⇒ MONARCHY.

P.T ⇒ instrumentsx

GA | TL | MZ | CL | RQ | XA

Date: Day: M T W T F S

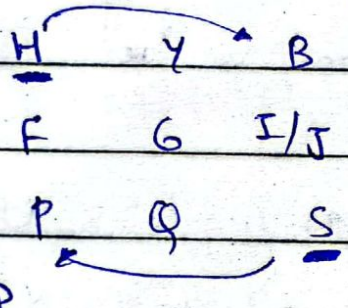
- If both char in pair are in same row, use next character to that letter

AR ⟹ RM.

FY ⟹ PO (same rule if both are in same col)

its FV not FY

- If both char are in diagonal use char at the other end of square formed by them.



HS → BP

- If not in diagonal same rule for rectangle formed by them.

EA → IM.

IDS-05 (30/01/24)

Hill Cipher:

msg: act

key: gybnqkrup

n: 3

Date: Day: M T W T F S

Encryption:

$$C = kP \bmod 26.$$

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} = \begin{bmatrix} 67 \\ 222 \\ 319 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 13 \\ 14 \\ 7 \end{bmatrix}$$

C.T = POH

Decryption:

$$P = k^{-1} C \bmod 26.$$

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} = \begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix}$$

$$= \begin{bmatrix} 260 \\ 574 \\ 539 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix}$$

PT = act

Date: _____ Day: M T W T F S

P.T = Short Example

key = Hill , n = 2.

$$\begin{bmatrix} H & I \\ L & L \end{bmatrix} = \begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix}$$

sh $C = KP \bmod 26 = \begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix} \begin{bmatrix} 18 \\ 7 \end{bmatrix}$

$$= \begin{bmatrix} 182 \\ 275 \end{bmatrix} \bmod 26 = \begin{bmatrix} 0 \\ 15 \end{bmatrix} = AP$$

or $= \begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix} \begin{bmatrix} 14 \\ 17 \end{bmatrix} = \begin{bmatrix} 234 \\ 341 \end{bmatrix} \bmod 26.$

$$= \begin{bmatrix} 0 \\ 3 \end{bmatrix} = ad.$$

te $\begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix} \begin{bmatrix} 19 \\ 14 \end{bmatrix} = \begin{bmatrix} 165 \\ 253 \end{bmatrix} \bmod 26.$

$$= \begin{bmatrix} 9 \\ 19 \end{bmatrix} = JT$$

xa $\begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix} \begin{bmatrix} 23 \\ 0 \end{bmatrix} = \begin{bmatrix} 161 \\ 253 \end{bmatrix} \bmod 26$

$$= \begin{bmatrix} 5 \\ 19 \end{bmatrix} = FT$$

mp $\begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix} \begin{bmatrix} 12 \\ 15 \end{bmatrix} = \begin{bmatrix} 204 \\ 297 \end{bmatrix} \bmod 26.$

If char are odd x or z can be added at end

Date: Day: M T W T F S

$$= \begin{bmatrix} 22 \\ 11 \end{bmatrix} = WL$$

ie $$\begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix} \begin{bmatrix} 11 \\ 4 \end{bmatrix} = \begin{bmatrix} 109 \\ 165 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 5 \\ 9 \end{bmatrix} = FJ.$$

$\Rightarrow$ APADJTFTWLFJ.

Decryption:

C.T = APADJTFTWLFJ.

$$\begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix}^{-1} = \begin{bmatrix}$$

$$Adj\ k = \begin{bmatrix} 11 & -8 \\ -11 & 7 \end{bmatrix} \bmod 26. = \begin{bmatrix} 11 & 18 \\ 15 & 7 \end{bmatrix}$$

$$\begin{vmatrix} 7 & 8 \\ 11 & 11 \end{vmatrix} = -11 \bmod 26$$

$$= 15$$

$15^{-1} \bmod 26$

$(15 \times x) \bmod 26.$

$(15 \times 7) \bmod 26 = 1$

$15^{-1} \Rightarrow 7$

$$k^{-1} = 7 \begin{bmatrix} 11 & 18 \\ 15 & 7 \end{bmatrix} \bmod 26$$

$$k^{-1} = 7 \begin{bmatrix} 11 & 18 \\ 15 & 7 \end{bmatrix} \bmod 26.$$

$$= \begin{bmatrix} 77 & 126 \\ 105 & 49 \end{bmatrix} \bmod 26 = \begin{bmatrix} 25 & 22 \\ 1 & 23 \end{bmatrix}$$

Date: Day: M T W T F S

Perception:

$$AP = \begin{bmatrix} 25 & 22 \\ 1 & 23 \end{bmatrix}\begin{bmatrix} 0 \\ 15 \end{bmatrix} = \begin{bmatrix} 330 \\ 345 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 18 \\ 7 \end{bmatrix} = sh$$

$$AD = \begin{bmatrix} 25 & 22 \\ 1 & 23 \end{bmatrix}\begin{bmatrix} 0 \\ 3 \end{bmatrix} = \begin{bmatrix} 66 \\ 69 \end{bmatrix} \bmod 26 = \begin{bmatrix} 14 \\ 17 \end{bmatrix} = or$$

$$JT = \begin{bmatrix} 25 & 22 \\ 1 & 23 \end{bmatrix}\begin{bmatrix} 9 \\ 19 \end{bmatrix} = \begin{bmatrix} 643 \\ 446 \end{bmatrix} \bmod 26 = \begin{bmatrix} 19 \\ 4 \end{bmatrix} = te$$

$$FT = \begin{bmatrix} 25 & 22 \\ 1 & 23 \end{bmatrix}\begin{bmatrix} 5 \\ 19 \end{bmatrix} = \begin{bmatrix} 543 \\ 442 \end{bmatrix} \bmod 26 = \begin{bmatrix} 23 \\ 0 \end{bmatrix} = xa$$

$$WL = \begin{bmatrix} 25 & 22 \\ 1 & 23 \end{bmatrix}\begin{bmatrix} 22 \\ 11 \end{bmatrix} = \begin{bmatrix} 792 \\ 275 \end{bmatrix} \bmod 26 = \begin{bmatrix} 12 \\ 15 \end{bmatrix} = mp$$

$$FJ = \begin{bmatrix} 25 & 22 \\ 1 & 23 \end{bmatrix}\begin{bmatrix} 5 \\ 9 \end{bmatrix} = \begin{bmatrix} 323 \\ 212 \end{bmatrix} \bmod 26 = \begin{bmatrix} 11 \\ 4 \end{bmatrix} = le$$

Euclidean.

Extended Euclidean:

Multiplicative Inverse.

Date: Day: M T W T F S

Vigenere Cipher:

→ Vigenere Table/Square.

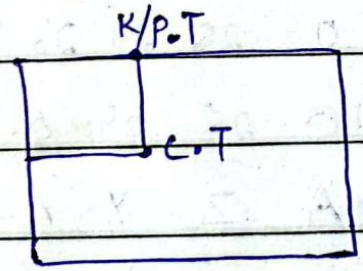
	A	B	C	D	.....	Z
A	A	B	C	D	.....	Z
B	B	C	D	E	.....	A
C	C	D	E	F	.....	B
!	!	!	!	!		!
Z	Z	A	B	C	.....	Y

→ intersection of x & z.

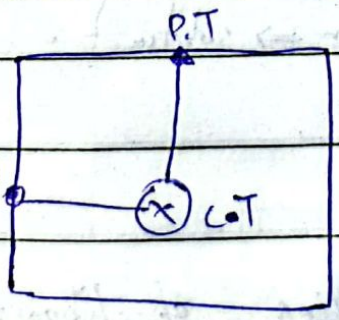
Plain Text : geeksforgeeks

Keyword : xyz

Enc:



Dec:



- keyword from row header is must in decryption.
- In encryption, keyword from row/col does not matter.

(31/01/24)

Example:

keyword = uet
uetuetuete
C.T = orbpikmimms.

P.T = ?

UNIVERSITY.

Vernam Cipher:

PT	r	a	m	s	w	a	m	i
P.No	17	0	12	18	22	0	12	8
key	r	a	n	g	e	l	a
key No	17	0	13	6	4	4	11	0
J=PN+kN	34	0	25	24	26	4	23	8
J Mod 26	8	0	25	24	0	4	23	8
C.T	I	A	Z	Y	A	E	X	I

for decryption ⇒ subtract.

VIC Cipher:

→ straddling checkboard/table.
→ Top Row [0-9]
→ Second Row → Popular letter in any order.

ESTONIA.R.

Date: Day: M T W T F S

0	1	2	3	4	5	6	7	8	9
E	T	x	A	O	N	x	R	I	S
2	B	C	D	F	G	H	J	K	L	M
6	P	Q	/	U	V	W	X	Y	Z	.

Encryption:

P.T → maryqueenof soots.

m a ry q ueen of scots

① S.T # 29 3 7 67 61 63005 423 92 1419

② Break 2-digit into single digit.

2 9 3 7 6 7 ------.

③ Add key 1542 & result % 10.

2 9 3 7 67 ---

1 5 4 2 1 5 4 2

res % 10 3 4 7 9 ---

④ Represent the result digit (Pair num with Row headers).

3	4	7	9	7	20
A	O				B.

Cipher Text.

Date: Day: M T W T F S

Example:

m a r y q u e e n o f s c o t s

2 9 3 7 6 7 6 1 6 3 0 0 5 4 2 3 9 2 1 4 1 9

2 9 3 7 6 7 6 1 6 3 0 0 5 4 2 3 9 2 1 4 1 9

+ 1 5 4 2 1 5 4 2 1 5 4 2 1 5 4 2 1 5 4 2 1 5 4 2 1 5

3 4 7 9 7 2 0 3 7 8 4 2 6 9 6 5 0 7 5 6 2 4

A O R S R B A R I O J / O

Decryption:

same steps but subtract key num in step 3.

3 4 7 9

− 1 5 4 2

2 −1 3 7) mod 10

2 9 3 7

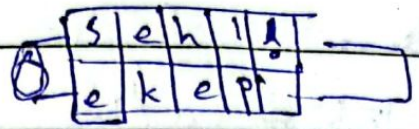
M A R

Transposition (Permutation)

↳ same char, arrangement shuffled.

i) Scytal Cipher

- Like ribbon wrapped on cylinder.
- diameter of rod should be on both sides.



P.T: Seek help!

1 3 5 7 9 2 4 6 8
C.T = Sehl ekep

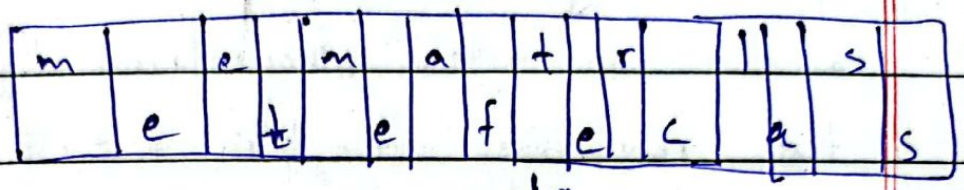
length/2 then one char from each part

if half = 4.5 5 char in first part

2) Rail Fence Cipher:

Depth = 2 (Diagonally).

P.T → meet me after class.



C.T → MEMATRSETEFECLAS

1 3 5 7 9 11 13 15 4 6 8 10 12 14 16

Description:

Divide C.T into 2 parts, then pick one char in seq from each part.

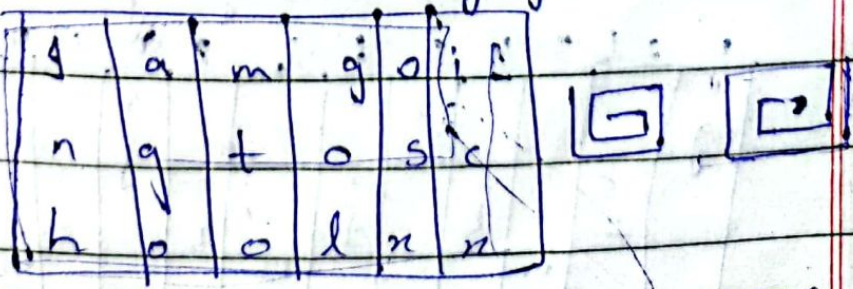
P.T = MEETMEAFTERCLASS

⇒ If half = 8.5 ⇒ then take first 9 char in 1 part.

3) Route Cipher:

key = 6 → 6 columns.

P.T → I am going to school.



C.T → ICXXLOOHNTAMGOSOTG

Date: Day: M T W T F S

Decryption:

~~length of text / key~~

~~18/6 = 3.~~

Make table with no of columns equal to key then fill the cipher text according to pattern, then read the text row wise for plain text.

g	a	m	g	o	i
n	g	t	o	s	c
h	o	o	l	x	x

P.T ⇒ Iamgoingtoschool.

Rail Fence Cipher-Decryption:

make a table with rows = depth and col = length & Place the char row wise by leaving empty spaces for char in rows below in a zig-zag manner.

1	2	3	4	5	6	7	8	9	10	11	12	13
1 g				2 s				3 g				4 s
	5 e		6 k		7 f		8 r		9 e		10 k	
		11 e				12 o				13 e		

Day: M T W T F S

Date:

C.T → gsgsekfrekeoe ✓

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

P.T → geeksforgeeks.

IS-07 (13/01/24)

Number Theory:

→ **Division Algo:**

If "a" & "b" → integers $b \geq 1$.

Then $a = qb + r$.

- **Modular Form:**

$a \equiv r \bmod b$.

$r = a \bmod b$.

- **Divisor & GCD**

integers a, b, c.

$c \mid a$, $c \mid b$ → c is common divisor.

GCD(a, b) ⇒ Greatest common divisor.

→ Co-Prime / Relatively Prime

Congruences:

If "a" & "b" are integers then "a" is said to be congruent to "b mod m" if $m \mid a - b$ m → modulus of congruence.

Date: Day: M T W T F S

Ex $24 \equiv 9 \bmod 5$ as $5 \mid 24-9$

$8 \equiv 5 \bmod 13$ $13 \mid -8-5$

$13 \mid 8$

→ 13 divides 8 ⇒ 8/13

Properties:

1) $a \equiv b \bmod n$ if $n \mid a-b$.

2) $a \equiv b \bmod n$ implies $b \equiv a \bmod n$.

3) If $a \equiv b \bmod n$ & $b \equiv c \bmod n$

then $a^b \equiv c \bmod n$. [$a \equiv c \bmod n$] *

4) $(a+b) \bmod n = ((a \bmod n) + (b \bmod n)) \bmod n$

5) $(a*b) \bmod n$ $((a \bmod n) * (b \bmod n)) \bmod n$

6) $(a-b) \bmod n$ (-) $\bmod n$

⇒ • $(6+8) \bmod 2 = (6 \bmod 2 + 8 \bmod 2) \bmod 2$.

$14 \bmod 2$ $= (0+0) \bmod 2$

$0 = 0$

⇒ $11^7 \bmod 13$.

$11^2 \bmod 13 = 121 \bmod 13 = 4$.

$11^4 \bmod 13 = (11^2)^2 \bmod 13$

$= 4^2 \bmod 13$

$= 16 \bmod 13 = 3$

$11^7 \bmod 13 = 11^{4+2+1} \bmod 13 = 11^4 \cdot 11^2 \cdot 11 \bmod 13$

$= (3 \times 4 \times 11) \bmod 13$

$= 132 \bmod 13 = 2$

Date: Day: M T W T F S

Multiplicative Inverse:

Let $a \in Z_n$ then $a^{-1} \bmod n$ is an integer $x \in n$ i.e $a \cdot x \bmod n = 1 \bmod n$.

$a \cdot x \bmod n = 1 \bmod n \quad (= a \cdot a^{-1})$

→ $a \in Z_n$ is invertable iff $\gcd(a, n) = 1$.

Calculating Multiplicative Inverse

Euclidean Algorithm:

If "a" & "b" are positive integers with $a > b$ then $\gcd(b, a \bmod b)$.

GCD (4864, 3458) =:

$4864 = (3458) \cdot 1 + 1406$

$3458 = (1406) \cdot 2 + 646$

$1406 = (646) \cdot 2 + 114$

$646 = (114) \cdot 5 + 76$ ← Extended method from this step.

$114 = (76) \cdot 1 + 38$ → GCD

$76 = (38) \cdot 2 + 0$

Euclidean ⇒ GCD / Extended Euclidean ⇒ Multiplicative Inverse.

Date: _____ Day: M T W T F S

Extended Euclidean

$a(x) + b(y) = d$.

$4864(x) + 3458(y) = 38$.

$\Rightarrow \quad 38 = (114).1 - (76).1$

$38 = (114).1 - (646.1 - 114.5).1$

$38 = (114).1 - (646).1 - (114).5$

$38 = (114).6 - (646).1$

$38 = (1406.1 - 646.2).6 - 646.1$

$38 = 1406.6 - 646.12 - 646.1$

$38 = 1406.6 - 646.13$.

$38 = 1406.6 - (3458 - 1406.2)13$

$38 = 1406.6 - 3458.13 + 1406.26$.

$38 = 1406.32 - 3458.13$.

$38 = (4864 - 3458.1).32 - 3458.13$.

$38 = 4864.32 - 3458.32 - 3458.13$.

$38 = 4864.32 - 3458.45$.

Date: _____ Day: M T W T F S

ISA - 08

2) GCD (1025, 35)

$1025 = (35)29 + 10$.

$35 = (10)3 + 5$ → GCD

$10 = (5)2 + 0$.

2) $45(x) + 130(y) = 5$

GCD (130, 45)

$130 = (45)2 + 40$.

$45 = (40)1 + 5$. → GCD

$40 = (5)8 + 0$.

$\Rightarrow 5 = 45 - 40.1$

$= 45 - (130 - (45)2).1$

$= 45 - 130.1 + 45.2$

$5 = (45)3 - 130(1)$

$\Rightarrow x = 3, y = -1$

3) $513(x) + 144(y) = 9$.

GCD (513, 144)

$513 = (144)3 + 81$.

$144 = (81)1 + 63$.

$81 = (63)1 + 18$.

$63 = (18)3 + 9$. → GCD.

$18 = (9)2 + 0$

Date: Day: M T W T F S

$9 = 63 - (18)3$

$9 = 63 - (81 - 63)3$

$9 = 63 - 81(3) + 63(3)$

$9 = 63(4) - 81(3)$

$= (144 - 81)4 - 81(3)$

$= (144)4 - 81(7)$

$= (144)4 - (513 - 144(3))7$

$= 144(4) - (513)7 + 144(21)$

$= 144(25) - (513)7$

$y = 25 \quad , x = -7$

4) $13^{-1} \bmod 15 = ?$

Date: Day: M T W T F S

Affine Cipher:

→ monoalphabetic substitution cipher.

→ Each letter encrypts to one letter & back again.

→ working in mod "m" → (length of alphabets used)

→ letters are mapped to integers in the range (a-m-1).

→ key consists of 2 numbers "a" & "b"

→ for 26 alphabets "a" must be relatively prime to "m"

Encryption:

$c = (ap + b) \bmod m$.

$b \rightarrow 1 \leq b \leq m$.

$a \rightarrow 1 \leq a \leq m$, $\gcd(a, m) = 1$

Decryption:

$P = a^{-1}(c - b) \bmod m$.

⇒ Plain Text ⇒ I am a secret.

$m = 26 \quad a = 15 \quad b = 7$.

GCD $(26, 15) \Leftrightarrow 26 = 15(1) + 11$

$15 = 11(1) + 4$.

$11 = 4(2) + 3$.

$4 = 3(1) + 1$.

Date: _____ Day: M T W T F S

GCD is 1 $3 = (1).3 + 0$

I → $c = (15(8) + 7) \bmod 26$.

$= 127 \bmod 26 = 23 = X$