UNIT-1

* classical substitution
  - caesar cipher
    - using key (3)

encryption (+3)

TEST => WHVW

Decryption (-3)

WHVW => TEST

* PLAYFAIR
  - i) Fill the key without repetition (MONARCHY)
  - ii) Bakupon => For same letter can use 'X'

BA/LX/LO/ON

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

iii) Next fill remaining alphabets

=> if the letter are in same row (or) same column select the next letter in row (or) column

=>

IB/US/PM/NA

=> letter are in another row (or) column select nearby

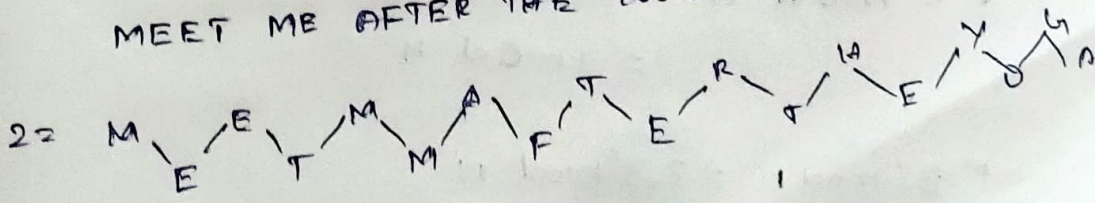
letter L => U X => S

* TRANSPOSITION CIPHER

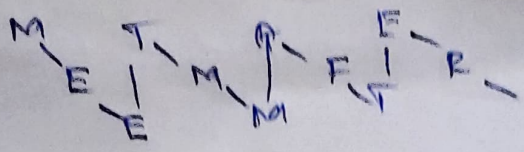
Rail Fence cipher

MEET ME AFTER THE TOGA

2 =



MematHYUETMFETEA

3⇒ 

* Row transposition cipher

ATTACK POSTPONE CB UNTILL

key: 4 3 1 2 5 6 7

A T T A C K P

O S T P O N E

D U N T I L L

X Q U M A X Z

re-arrange the according key

⇒ 15M (DES) or (AES)

UNIT -II

Euler-phi-Function

* $\phi(1) = 0$
* $\phi(p) = p-1$, if p is prime
* $\phi(m \times n) = \phi(m) \times \phi(n)$
* $\phi(p^e) = p^e - p^{e-1}$ p is prime

Format Version

i) $a^{p-1} \equiv 1 \bmod p$ ii) $a^p \equiv a \bmod p$

* $6^{10} \bmod 11 \Rightarrow 6^{11-1} \bmod 11$
$= 1 \bmod 11$

* $3^{12} \bmod 11 = 3.3^{11} \bmod 11$
$= 3.3 = 9$

⇒ multiplicative inverse

$$8 \overline{)11} - 3$$
$$\underline{8}$$
$$3 \overline{)8} - 2$$
$$\underline{6}$$
$$2 \overline{)3} - 1$$
$$\underline{2}$$
$$1$$

$11 = 8(1) + 3$

$8 = 3(2) + 2$

$3 = 2(1) + 1$

⇒ chinese remainder theorem

$x \equiv a_1 \pmod{m_1}$

$x \equiv a_2 \pmod{m_2}$

$\vdots$

$x \equiv a_k \pmod{m_k}$

① ⇒ Find M

$M = m_1 \times m_2 \times m_3$

② ⇒ $M_1 = \frac{M}{m_1}$ $M_2 = \frac{M}{m_2}$ $M_3 = \frac{M}{m_3}$

③ ⇒ multiplicative inverse $\bar{M_1}$

④ $x \equiv (a_1 \times M_1 \times \bar{M_1}) + a_2 \times M_2 \times M_2) \log M$

⇒ order of group, primitive roots

⇒ Diffe-Hellman

⇒ RSA

- P & Q prime
- $n = p * Q$
- $\phi(n) = \phi(n) = (P-1)(Q-1)$
- $\gcd(d, \phi(n)), e) = 1$

$1 < e < \phi(n)$

- $d \cdot e = 1 \mod \phi(n)$

$d = e^{-1} \mod \phi(n)$

Public (e, n) private (d, n)

encryption $\Rightarrow c = m^e \mod n$

decryption $= m = c^d \mod n$

⇒ Quadratic residue

UNIT - III

- Hash function
- Application
- properties of Hash function
- MD5
- SHA

UNIT - IV

- Kerbros
- X.509
- E-MAIL
  - ⇒ PGP
  - S/MIME
- IP security

UNIT - V

⇒ WORMS

⇒ VIRUSES

⇒ FIREWALL

2m or 7m

SSO, DOS, IP routing, [illegible]