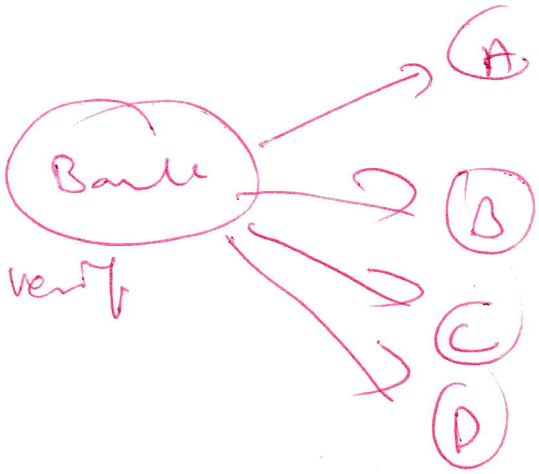
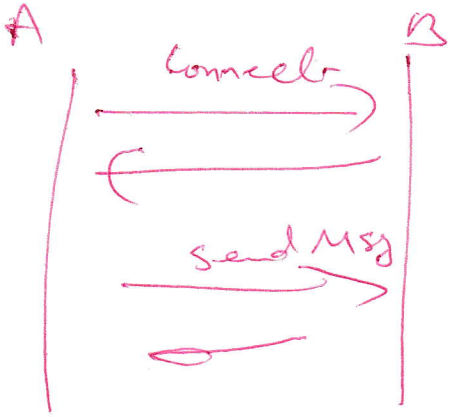
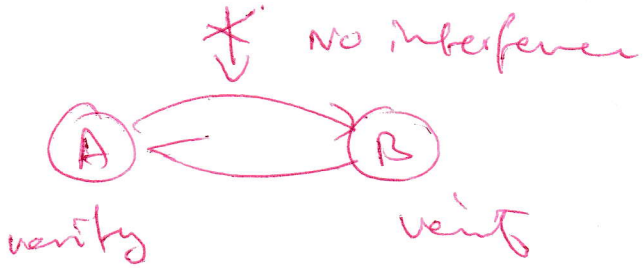
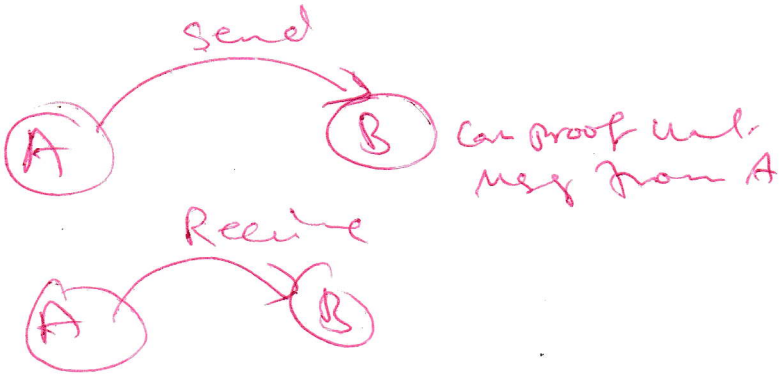






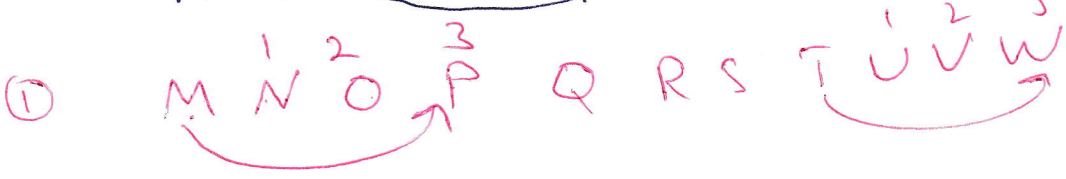


B can proof that Msg from A

A can proof B get Msg

$$C = E(K, X)$$

$$X = D(K, C)$$



$C = E(k, P)$

~~$C = E(3, P) = E(3, 0) \bmod 26$~~

$C = E(3, P) = (P + 3) \bmod 26$

$= (0 + 3) \bmod 26 = 3$ (A)

$= D$

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

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

$(3 - 3) \bmod 26 = 0 \bmod 26 = 0 \Rightarrow A$

① Repeating plain text

balloon

balx

② Same Row go Right.

A → R

R → M

③ M → C, U → M Same Column Replaced By letter beneath

④ Pair ~~has~~ Replace by its own Row + colu

H → B, S → P E A / I M

Brute force

1. Encryption + Decryption Algo known.
2. 25 keys to try.
3. language of plaintext known

⇒ We assume Algorithm known

⇒ Impractical if key is large
DES algo 168 bit key 2^{168}

⇒ Plaintext unknown Output can't be recognizable

Monoalphabetic Cipher

$S = \{a, b, c\}$

Six permutation of S

abc, acb, bac, bca, cab, cba

3 element Means 3! permutation

n element Means n! permutation

26 element $26! = 4 \times 10^{26}$ keys

$$\text{Freq} = \frac{\text{number of occurrence}}{\text{Total Element}} \times 100$$

$$J = \frac{1}{120} \times 100 = 0.83$$

$$Y = \frac{2}{120} \times 100 = 1.67$$

Hill Cipher Example

$$C = E(K, P) = PK \bmod 26$$

$$P = D(K, P) = CK^{-1} \bmod 26$$

Plaintext

15	0	24
P	a	y

Key

$$\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$$

$= 15 \times 17 + 0 \times 21 + 24 \times 2 = 303$

$= 15 \times 17 + 0 \times 18 + 24 \times 2 = 303$

$= 15 \times 5 + 0 \times 21 + 24 \times 19 = 531$

$C = (303\ 303\ 531) \bmod 26 = 17\ 17\ 11$

$R\ R\ L$

$$P = CK^{-1} \bmod 26$$

C

17	17	11
R	R	L

K^{-1}

$$\begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix}$$

$= 17 \times 4 + 17 \times 15 + 11 \times 24 = 587$

$= 17 \times 9 + 17 \times 17 + 11 \times 0 = 442$

$= 17 \times 15 + 17 \times 6 + 11 \times 17 = 544$

$P = (587\ 442\ 544) \bmod 26 = 15\ 0\ 24$

$P\ a\ y$

Vigenere Cipher

Key = d e c
P = w e a
C = z i c

a = 0 b = 1 c = 2 d = 3
e = 4

① w x y z
1 2 3

② e f g h i
1 2 3 4

③ a b c
1 2