SNS COLLEGE OF TECHNOLOGY

Coimbatore-35

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A++' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

# 19ECT301-COMMUNICATION NETWORKS III YEAR/ V SEMESTER

## UNIT 4- NETWORK & DATA SECURITY

## TOPIC –Substitution Techniques

# SUBTITUTION TECHNIQUES

- The two basic building block of all the encryption techniques are substitution and transposition
- A substitution techniques is one in which the letter of plaintext are replaced by other letter or by number or symbols
- The subsitution techniques have a four techniques

caeser cipher

monoalphabetic cipher

play fair cipher

hill cipher

polyalphabetic cipher

# Caeser cipher

- caeser cipher involves replacing each letter of the alphabet with the letter standing three place further down the alphabet

plain : meet me after the to go party

cipher: DREFR JUKHI TYRTY ELKJH VFDCB

we can define transposition listing

plain: a b c d e f g h I j k l m

cipher :DE F G H I K L M N O P Q R S T U

- The algorithm can be expressed:

plain text p,subsitution the cipher text c2

$$c=E(3,p)=(p+3)\mathrm{mod}\ 26$$

gentral caeser algorithm:

$$c=E(k,p)=(p+k)\mathrm{mod}\ 26$$

three important characteristics of this problem

1.encryption and decryption algorithm

2.there are 25 key

3.the language are plaintext

the text file comprressed using algorithm called ZIP

EX:BRUTE FORCE CRYPTANALYSIS OF CAESER CIPHER

| PHHW | PH | WKH |
|---|---|---|
| OGGU | OG | VJG |

# MONOALPHABETIC CIPHER

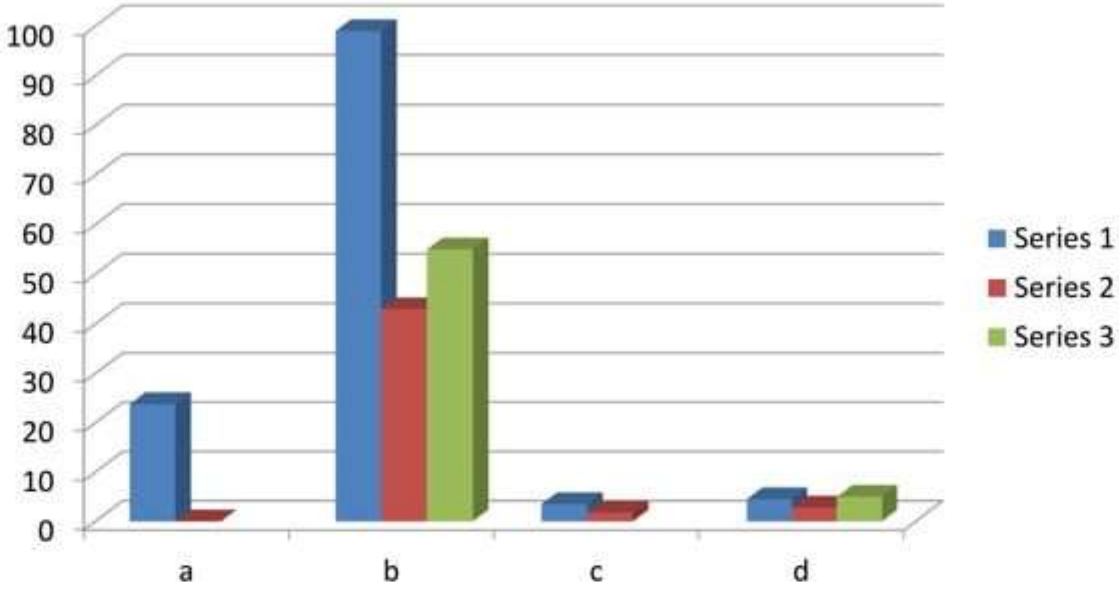
- The can 25 key possible key ,caeser cipher is far from secure,
- The are 26 alphabetic characters ,10 order of magnitude greater then key space DES
- this also called monoalphabetic subsitution cipher
- Ex:

NYUTGHREDSWACXZFGHJKLIOLPMNBGTYREFCVXD

LOIKUJYTRGFDCVBHNUYTREWASEDXZCDSFREDFVBNMKOLP

The realtive frequency on cipher text in (percentage)

| | |
|---|---|
| P 13.33 | F 3.33 |
| Z 11.67 | W 3.33 |
| S 8.33 | Q 2.50 |
| U 8.33 | T 2.50 |
| O 7.50 | |


100
90
80
70
60
50
40
30
20
10
0
a
b
c
d
Series 1
Series 2
Series 3

- Monoalphabet cipher reficect frequency data original alphabet
- Multiple subsitution know as homophones
- EX: different cipher models

16,17,35,21 homophone using rotation randomely

# PLAYFAIR CIPHER

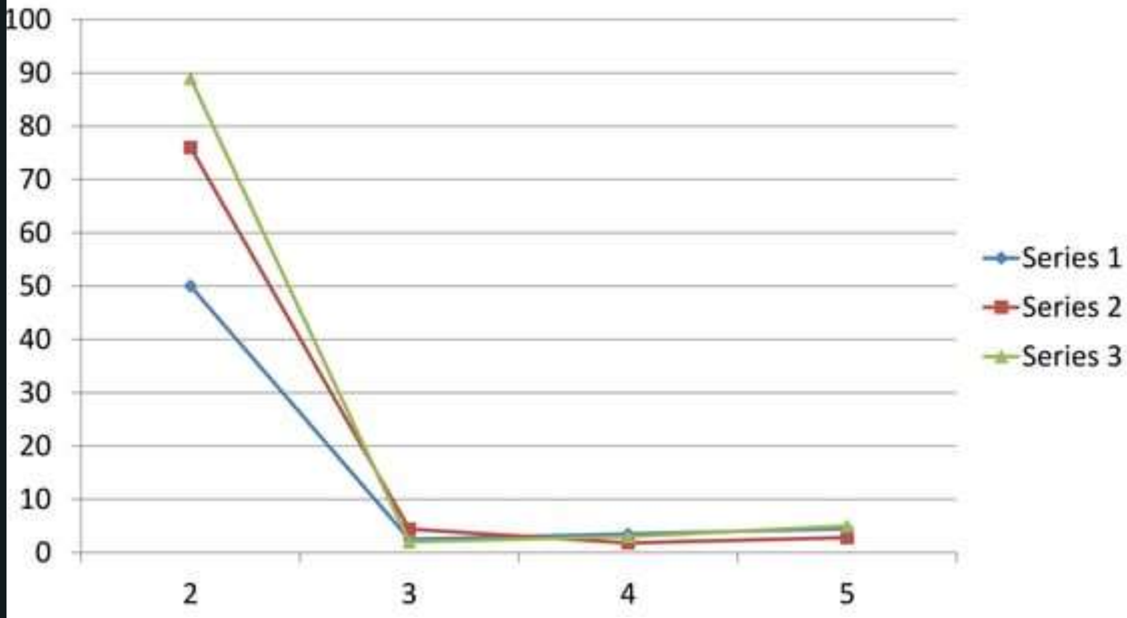
the multiple letter encryption is play Fair

The play fair algorithm is based  on used construer using keyword

THE KEYWORD “MONOARCHY”

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

- THE FOLLOWING RUIE IN PLAY FAIR:
- 1. repeating plaintext letter are the same pair filltering letter
- 2. two plaintext letter in same row of the matrix are replaced the letter to the right
- 3.top the element colum circulary from the last
- Play fair text easy to break
- Ex:relative frequency of occurrence of letters:


100
90
80
70
60
50
40
30
20
10
0
2
3
4
5
Series 1
Series 2
Series 3

# HILL CIPHER

.The multiletter cipher hill cipher developed by the mathematician Lester hill in 1929.

. The algorithm m plaintext letter substitution cipher text m ,numerical value(a=0,b=1,....z=25)

$$c1=(k11p1+k12p2+k13p3)\text{mod } 26$$

$$c2=(k21p1+k22p2+k23p3)\text{mod } 26$$

$$c3=(k31p1+k32p2+k33p3)\text{mod } 26$$

the column of vectors:

$$\begin{pmatrix} c1 \\ c2 \\ c3 \end{pmatrix} \begin{pmatrix} k11 & k12 & k13 \\ k21 & k22 & k23 \\ k31 & k32 & k33 \end{pmatrix} \begin{pmatrix} p1 \\ p2 \\ p3 \end{pmatrix} \text{mod } 26$$

- c=kp mod 26
- c and p colum of vectorsog length 3,plaintext cipher text and k represent encryption key
- Ex:

$$k=\begin{pmatrix}17&17&5\\21&18&21\\2&2&19\end{pmatrix}\begin{bmatrix}15\\ \% \quad 0\\24\end{bmatrix}\begin{bmatrix}375\\ =819\\486\end{bmatrix}\quad \text{mod } 26\begin{bmatrix}11\\13\\18\end{bmatrix}$$

The square matrix determinate matrix equals sum of all the product can be one element each colum from each row on element .

EX: matrix

$$\begin{pmatrix} k11 & k12 \\ k21 & k22 \end{pmatrix}$$

# POLALPHABETIC CIPHER

- The general name approach is polyalphabetic subsitution cipher
- the feature:
  1. monoalphabetic rule is used
  2. choose given transformation

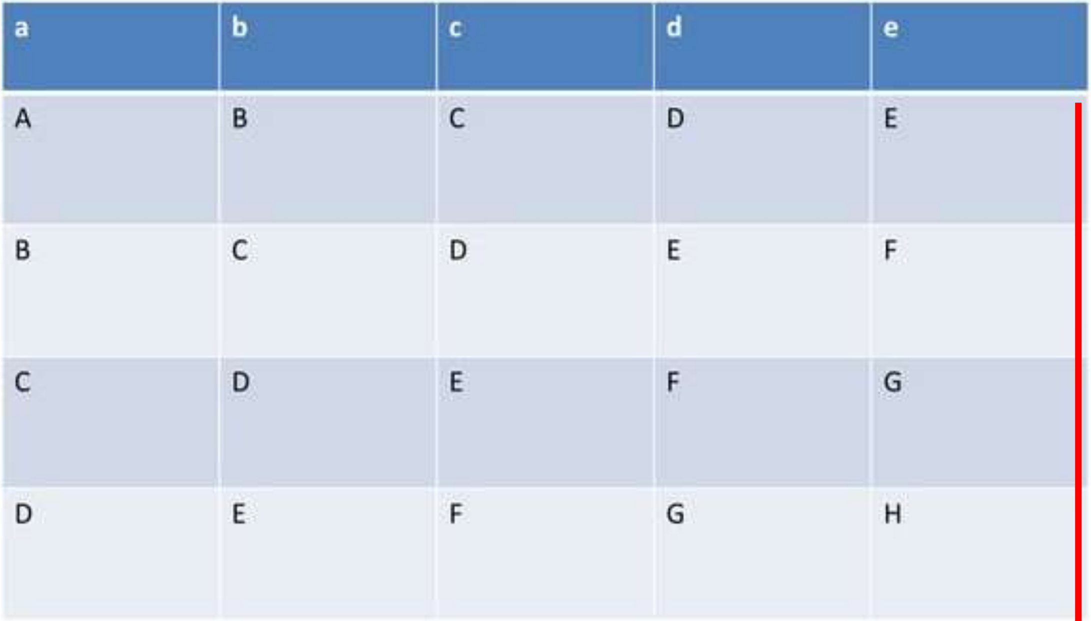
key:meetmemeetmemeetme

plaintext:ewrdsfhthyujkikllolol

ciphertext:ZCSDEFRGTHBVNJUIKMNK

The ciphertext row determined column and plain text top of the column

vigenere proposed is refereed to auto key system



| a | b | c | d | e |
|---|---|---|---|---|
| A | B | C | D | E |
| B | C | D | E | F |
| C | D | E | F | G |
| D | E | F | G | H |

- This system works on binary data ,the system expressed follows:

$$c_i=p_i+k_i$$

Where:

pi=binary digit plaintext

ki=binary digit key

ci=binary digit cipher text

# THANK YOU