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

  $$c=E(3,p)=(p+3)\bmod 26$$

gentral caeser algorithm:

  $$c=E(k,p)=(p+k)\bmod 26$$

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

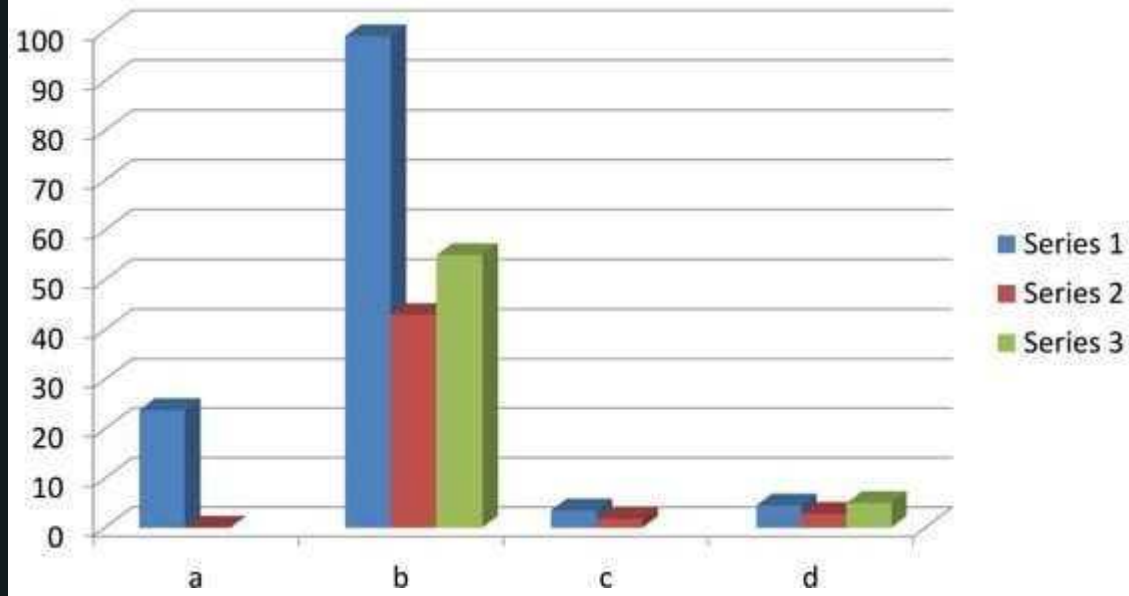| PHHW	PH	WKH
OGGU	OG	VJG

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	

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

16,17,35,21   homophone using rotation randomely
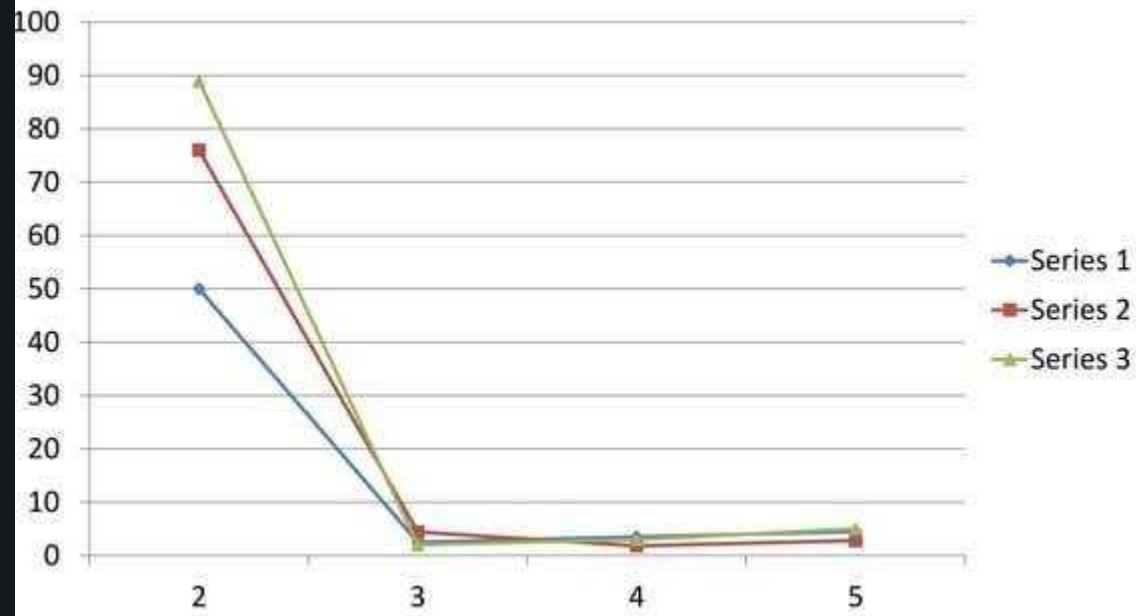
PLAYFAIR CIPHER

the multiple letter encryption is play Fair

The play fair algorithm is based on used construer using keyword

   THE KEYWORD "MONOARCHY"

M C	O H	N 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:

Substitution Techniques/19ECT301 COMMUNICATION NETWORKS /E.CHRISTINA
DALLY/ECE/SNSCT

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)

$$c_1 = (k_{11}p_1 + k_{12}p_2 + k_{13}p_3) \bmod 26$$
$$c_2 = (k_{21}p_1 + k_{22}p_2 + k_{23}p_3) \bmod 26$$
$$c_3 = (k_{31}p_1 + k_{32}p_2 + k_{33}p_3) \bmod 26$$

the column of vectors:

$$\begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix} \quad \begin{bmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{bmatrix} \quad \begin{bmatrix} p_1 \\ p_2 \\ p_3 \end{bmatrix} \bmod 26$$

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

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

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:

p_i = binary digit plaintext

k_i = binary digit key

c_i = binary digit cipher text

THANK YOU