Cryptography

Developed and Presented By:

Dileep Kumar Yadav
Assistant Professor
Dept. of CSE
V.B.S Purvanchal
University Jaunpur

Security Mechanism

- Security mechanism deals with identification of any breach i.e break in security and after identification it also helps in removing the security breakdown. There are various security mechanism like:
- Encipherment
- Digital signature
- Access control
- Data integrity
- Routing control

Encipherment

- It is also known as encryption. It is the process of using mathematical formula’s, algorithms and the keys to transform the simple message in to a message that is not easily understood by each and every one.

Digital Signature

- These are similar to signature on paper done in real life but are done in computer documents and in cryptographic formats to ensure the principal of security services.

Access Control

- It includes a variety of techniques used to avoid unauthorized access or granting only limited access to data and network resources.

Data Integrity

- It ensure that the data received on receiver side is same as sent by the original data sender.

Routing Control

- It is computer network technique that uses variety of techniques to avoid the traffic congestion in the network.

Classical Encryption Technique

- Substitution Technique
- Transposition Technique

Substitution Techniques

- It involves replacing one or more entities to an other entities.
- Caesar Cipher
- Modified Caesar Cipher
- Mono alphabetic Cipher
- Homophonic Cipher
- Polygram Cipher
- Play fair Cipher
- Poly alphabetic Cipher
- Hill Cipher

Caesar Cipher

- In this technique replaces each alphabet with the three places down or up.
- For example: Replace each A with D, B with E and C with F and so on…
- HI KUNDAN -PT
- KL NXQGDQ -CT

Modified Caesar Cipher

- In modified Caesar cipher original plain text alphabet may not be necessarily three places up or down but instead can be any places down or up.
- In this technique step size is variable but fixed for one session is called modified cipher.
- Thus an alphabet A in plain text would not necessarily be replaced by D. It can be replaced by any valid alphabet i.e. E or F or G and so on…

Mono Alphabetic Cipher

- In this technique we decide to use random substitution. This means that in a given plain text message each A can be replaced by any other alphabet i.e.(B to Z) and each B can be replaced A or (C to Z) and so on…
- To put it mathematical there is 26 permutation or combination occurs. i.e. 26! Possibilities.

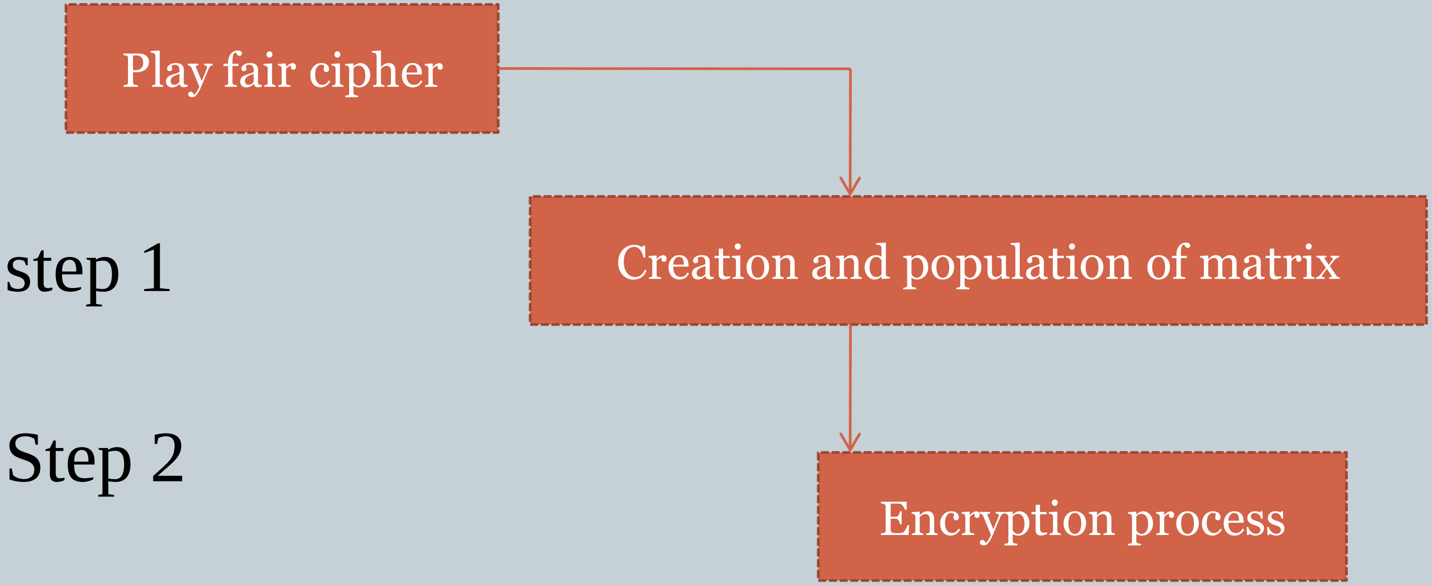
Polygram Cipher

- This technique replaces one block of plain text with a block cipher text. It does not work on character by character basis.
- For example:

- HELLO → POLYGRAM → YUQQW
- HELL → POLYGRAM → TEUI

Play fair Cipher

- It is also called play fair square which is designed by Charles Wheatstone in 1854. It is used in world war I by British army and world war II by Australians army.
- This technique have done by two main process.



Play fair cipher

step 1

Creation and population of matrix

Step 2

Encryption process

Step 1-Creation and Population of Matrix

- The play fair cipher makes use of a 5×5 matrix table, which is used to store a keyword or phrases that becomes the key for encryption and decryption.
- Enter the keyword in the matrix row wise, left to right and top to bottom. matrix
- Drop duplicate letters.
- Fill the remaining spaces in the matrix with the rest of the English alphabet i.e.(A to Z).

Cont…

- For example: PURVANCHAL

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

Step 2-Encryption Process

- Before executing these step the plain text message that we want to encrypt needs to be broken down into groups of two alphabet.
- If both alphabets are the same or only one is left add an x after the ist alphabet. Encrypt the new pair and continue..
- If both the alphabets in the pair appear in the same row of our matrix, replace them with alphabets to their immediate right respectively. If the original pair is on the right side of the row them wrapping around the left side of the row happens.

Cont…

- If both the alphabets in the pair appear in the same column of our matrix, replace them with alphabets to their immediate below respectively. If the original pair is on the bottom side of the row them wrapping around the left side of the row happens.
- If the alphabets are not in the same row or column replace them with the alphabets in the same row respectively, but at the other pair of corners of the rectangle defined by the original pair.

Cont…

- For example –PURVANCHAL-KEY WORD
- Plain text-UNIVERSITY
- UN IV ER SI TY-PT
- PC GA FU ZS WZ-CT

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

Cont…

- For example-
- Keyword-monarchy
- PT-come home tomorrow

Hill Cipher

- Treat every letter in the plain text message as a number so that A=0,B=1,C=2,…….Z=25.
- The plain text message is organized as a matrix of numbers based on the above conversion. For example if our PT is CAT then from above conversion C=2, A=0 and T=19.

$$\begin{bmatrix} 2 \\ 0 \\ 19 \end{bmatrix}_{3\times1}$$

Cont…

- Now we have randomly chosen key. The key matrix consists of size n×n where n is the number of rows in our plain text matrix. For example we take the following key.

$$\text{key}=\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}_{3\times3}$$

- Now CT=[key] ×[PT] mod 26

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

Cont…

$$CT = \begin{bmatrix} 12+0+19 \\ 26+0+190 \\ 40+0+285 \end{bmatrix} \bmod 26$$

$$CT = \begin{bmatrix} 31 \\ 216 \\ 325 \end{bmatrix} \bmod 26$$

$$CT = \begin{bmatrix} 5 \\ 8 \\ 13 \end{bmatrix}$$

Cont…

- Now translating the numbers to alphabets i.e.

5=F,8=I,13=N

So CT=FIN

- Now PT=[K¯1]*[CT]mod 26

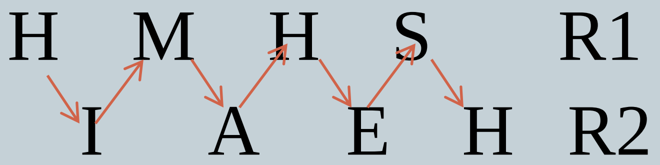
Transposition Technique

- Rail Fence Technique
- Simple Columnar Technique
- Vernam Cipher(One Time Pad)

Rail Fence Technique

- This technique involves writing plain text as a sequence of diagonals and then reading it row by row to produce cipher text.
- For example:

HI MAHESH-PT



H M H S R1

I A E H R2

- Then CT=HMHSIAEH
- PT=COME HOME TOMORROW
- Find CT=?

Vernam Cipher(OTP)

- It is implemented using a random set of non repeating characters as the input cipher text.
- The most significant point here is that once an input cipher text for transposition is used , it is never used again for any other message.
- The length of the input cipher text is equal to the length of the original plain text.

Algorithms for Vernam Cipher

- Treat each plain text alphabet as a number in an increasing sequence i.e. A=0,B=1,……Z=25.
- Do the same for each character of the input cipher text.
- Add each no. corresponding to the plain text alphabet to the corresponding input cipher text alphabet number.
- If the sum thus produced is greater than 26, subtract 26 from it.
- Translate each number of the sum back to the corresponding alphabet. This gives the output cipher text.

Cont…

- For example:
- Plain text--- HOW ARE YOU
- OTP----- NCB TZQ ARX

PT---	H	O	W	A	R	E	Y	O	U
	7	14	22	0	17	4	24	14	20
OTP-	N	C	B	T	Z	Q	A	R	X
	13	2	1	19	25	16	0	17	23
ADD	20	16	23	19	42	20	24	31	43
SUB 26	20	16	23	19	16	20	24	05	17
CT…	U	Q	X	T	Q	U	Y	F	R

Cont…

- For example:
- Plain text– COME HOME TOMORROW
- OTP- WABD AMNT EFGHCYPR
- Find the CT….?