JAYOTI VIDYAPEETH WOMEN'S UNIVERSITY, JAIPUR
Government of Rajasthan established
Through ACT No. 17 of 2008 as per UGC ACT 1956
NAAC Accredited University

Faculty of Education and methodology

Department of Science and Technology

Faculty Name- Jv'n Narendra Kumar Chahar (Assistant Professor)

Program- B.Tech 8thSemester

Course Name – Cryptography and Network Security

Session no.: 08

Session Name- Classical Encryption Techniques (Substitution Techniques)

Academic Day starts with –

- Greeting with saying **'Namaste'** by joining Hands together following by 2-3 Minutes Happy session, Celebrating birthday of any student of respective class and **National Anthem**.

Lecture starts with- quotations' answer writing

Review of previous Session **– Conventional Encryption**

Topic to be discussed today- Today We will discuss about **Classical Encryption Techniques (Substitution Techniques)**

Lesson deliverance (ICT, Diagrams & Live Example)-

- Diagrams

Introduction & Brief Discussion about the Topic **– Classical Encryption Techniques**

Classical Encryption Techniques

There are two basic building blocks of all encryption techniques: substitution and transposition.

SUBSTITUTION TECHNIQUES

A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols. If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with cipher text bit patterns.

1. Caesar cipher (or) shift cipher

The earliest known use of a substitution cipher and the simplest was by Julius Caesar. The Caesar cipher involves replacing each letter of the alphabet with the letter standing 3 places further down the alphabet.

e.g., plain text: pay more money Cipher text: SDB PRUH PRQHB

Note that the alphabet is wrapped around, so that letter following „z" is „a". For each plaintext letter p, substitute the cipher text letter c such that

$$C = E(p) = (p+3) \bmod 26$$

A shift may be any amount, so that general Caesar algorithm is C = E (p) = (p+k) mod 26

Where k takes on a value in the range 1 to 25. The decryption algorithm is simply P = D(C) = (C-k) mod 26

2. Playfair cipher

The best-known multiple letter encryption cipher is the Playfair, which treats diagrams in the plaintext as single units and translates these units into cipher text diagrams. The Playfair algorithm is based on the use of 5x5 matrix of letters constructed using a keyword. Let the keyword be „monarchy". The matrix is constructed by filling in the letters of the keyword (minus duplicates) from left to right and from top to bottom, and then filling in the remainder of the matrix with the remaining letters in alphabetical order.

The letter „i" and „j" count as one letter. Plaintext is encrypted two letters at a time According to the following rules:

Repeating plaintext letters that would fall in the same pair are separated with a Filler letter such as „x".

Plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row following the last.

Plaintext letters that fall in the same column are replaced by the letter beneath, with the top element of the column following the last.

Otherwise, each plaintext letter is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter.

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

Plaintext = meet me at the school house

Splitting two letters as a unit => me et me at th es ch o x ol ho us ex

Corresponding cipher text => CL KL CL RS PD IL HY AV MP HF XL IU

Strength of Playfair cipher

Playfair cipher is a great advance over simple mono alphabetic ciphers.

Since there are 26 letters, 26x26 = 676 diagrams are possible, so identification of individual diagram is more difficult.

3. Polyalphabetic ciphers

Another way to improve on the simple monoalphabetic technique is to use different monoalphabetic substitutions as one proceeds through the plaintext message. The general name for this approach is polyalphabetic cipher. All the techniques have the following features in common.

A set of related monoalphabetic substitution rules are used

A key determines which particular rule is chosen for a given transformation.

4. Vigenère cipher

In this scheme, the set of related monoalphabetic substitution rules consisting of 26 Caesar ciphers with shifts of 0 through 25. Each cipher is denoted by a key letter. e.g., Caesar cipher with a shift of 3 is denoted by the key value 'd‟ (since a=0, b=1, c=2 and so on). To aid in understanding the scheme, a matrix known as Vigenère tableau is Constructed Each of the 26 ciphers is laid out horizontally, with the key letter for each cipher to its left. A normal alphabet for the plaintext runs across the top. The process of Encryption is simple: Given a key letter X and a plaintext letter y, the cipher text is at the intersection of the row labeled x and the column labeled y; in this case, the ciphertext is V.

	PLAIN TEXT															
KEY LETTERS		a	b	c	d	e	f	g	h	i	j	k	…	x	y	z
	a	A	B	C	D	E	F	G	H	I	J	K	…	X	Y	Z
	b	B	C	D	E	F	G	H	I	J	K	L	…	Y	Z	A
	c	C	D	E	F	G	H	I	J	K	L	M	…	Z	A	B
	d	D	E	F	G	H	I	J	K	L	M	N	…	A	B	C
	e	E	F	G	H	I	J	K	L	M	N	O	…	B	C	D
	f	F	G	H	I	J	K	L	M	N	O	P	…	C	D	E
	g	G	H	I	J	K	L	M	N	O	P	Q	…	D	E	F
	: :	: :	: :	: :	: :	: :	: :	: :	: :	: :	: :	: :	…	: :	: :	: :
	x	X	Y	Z	A	B	C	D	E	F	G	H	…			W
	y	Y	Z	A	B	C	D	E	F	G	H	I	…			X
	z	Z	A	B	C	D	E	F	G	H	I	J	…			Y

To encrypt a message, a key is needed that is as long as the message. Usually, the key is a repeating keyword.

e.g., key = d e c e p t i v e d e c e p t i v e d e c e p t i v e PT = w e a r e d i s c o v e r e d s a v e y o u r s e l f CT = ZICVTWQNGRZGVTWAVZHCQYGLMGJ

Decryption is equally simple. The key letter again identifies the row. The position of the cipher text letter in that row determines the column, and the plaintext letter is at the top of that column.

Strength of Vigenère cipher

There are multiple cipher text letters for each plaintext letter.

Letter frequency information is obscured.

5. **One Time Pad Cipher**

It is an unbreakable cryptosystem. It represents the message as a sequence of 0s and 1s. this can be accomplished by writing all numbers in binary, for example, or by using ASCII. The key is a random sequence of 0"s and 1"s of same length as the message. Once a key is used, it is discarded and never used again. The system can be expressed as

Follows:

$C_i = P_i \oplus K_i$ C_i - i^{th} binary digit of cipher text P_i - i^{th} binary digit of plaintext K_i - i^{th} binary digit of key

Exclusive OR operation

Thus, the cipher text is generated by performing the bitwise XOR of the plaintext and the key. Decryption uses the same key. Because of the properties of XOR, decryption simply involves the same bitwise operation:

$P_i = C_i \oplus K_i$

e.g.,

plaintext = 0 0 1 0 1 0 0 1

Key = 1 0 1 0 1 1 0 0

---

ciphertext = 1 0 0 0 0 1 0 1

Advantage:

Encryption method is completely unbreakable for a ciphertext only attack.

Disadvantages

It requires a very long key which is expensive to produce and expensive to transmit.

Once a key is used, it is dangerous to reuse it for a second message; any knowledge on the first message would give knowledge of the second.

Reference-

1. **Book:** William Stallings, "Cryptography & Network Security", Pearson Education, 4th Edition 2006.

QUESTIONS: -

Q1. What are the types of classical Encryption techniques?

Q2. What are different substitutional techniques?

Q3. What are advantages and disadvantages of encryption?

Next, we will discuss about Transposition Techniques.

- Academic Day ends with-
  National song 'Vande Mataram'