Name: Sudesh Pawar
BE Comp A
F17111037(24)

ICS A1 cipher

1) What do you mean by Shift Cipher? Discuss various shift available.

Ans. Shift cipher is one of the easiest & simplest cryptography.
- A given plaintext is encrypted into a ciphertext by shifting each letter of given plain text by n positions.

* Caesar Cipher is a type of shift cipher. Shift ciphers work by using modulo operator to encrypt & decrypt messages
* Shift entire alphabet by the number you picked & write it down below original alphabet.
* The ROT13 cipher is a substitution cipher with specific key where letters of the alphabet are offset 13 places

Q.2) Discuss Caesar Cipher in detail.

Ans In this technique each letter is replaced by the letter / alphabet which is 3 places next to that letter which is to be substituted.
- Each alphabet of a plaintext is replaced with another alphabet but 3 places down the line

Plain Text	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Cipher Text	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Mathematically, Caesar Cipher can be expressed as:

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

$P = D(3, C) = (C - 3) \bmod 26$ C: Cipher, D: Decrypt)

Q.3) What do you mean by monoalphabetic & polyalphabetic ciphers? Give examples of each of them.

Ans) In this Cipher, substitution of letter of the alphabet with any random letter from alphabet.

- It is not necessary that if A is substituted with B, then compulsorily B has to be substituted with C. It can be replaced with any other letter of alphabet.

For eg:

A can be replaced by: d, j, r, y

B can be replaced by: h, u, m, p

- It is a way to use more than 1 alphabet & switching between them.

Keyword: COMP COMP IT IT IT

Plain: We need more supplies fast

Cipher: IIPQ IF YS TQS WW BTN UI URE VT.

Q.4) What are different Substitution Ciphers?

Ans. i) Caesar Cipher: Each letter is replaced by letter/alphabet which is 3 places next to that letter which is to be substituted.

ii) Monoalphabetic Cipher: It substitutes one letter of the alphabet with any random letter from the alphabet.

iii) Polyalphabetic Cipher: It is a way to use more than one alphabet & ~~way~~ switching between them systematically.

iv) Playfair Cipher: It is multi-letter encryption technique which uses 5 x 5 matrix table to store the letters of the phrase given for encryption which latter on becomes key for encryption & decryption.

v) Vernam Cipher: This cipher improves security over substitution & transposition techniques.

vi) Hill Cipher: It is a polygraphic substitution cipher based on linear algebra. Each letter is represented by no. modulo 26.