# Pauline Criste IT 315

# **Caesar Cipher**

It is a substitution technique substituted by other letters or symbols. It replaces each letter with standing three letters places further down the alphabet.

0	1	2	3	4	5	6	7	8	9	10	11	12
А	В	С	D	Е	F	G	н	Ι	J	к	L	М
13	14	15	16	17	18	19	20	21	22	23	24	25
N	0	Р	Q	R	S	Т	U	V	W	х	Y	Z

The algorithm is

"p" means plaintext letter, "C" is ciphertext, "k" is equal to 3, E - encryption D - decryption

 $C = E (p, k) \mod 26 = (p + k) \mod 26$ p= D (C, k) mod 26 = (C - k) mod 26

C = (p + k) mod 26 C = (18 + 3) mod 26 C = 21 mod 26 C = 21

S = V

1.Plaintext = Spiderman Ciphertext = vslghupdq

2.Plaintext = Rudolph Ciphertext = uxgrosk

## **Rail Fence Technique**

The plain text is written down as a sequence of diagonals and then read off as a sequence of rows.

3.Plaintext = November Depth = 2

N		V		М		E	
	0		E		В		R

## Ciphertext = NVMEOEBR

#### **Columnar Transposition**

The message is written out in rows of a fixed length. Read it out column by column. There are 6 rows for example, the key word is NUMBER. We will number the letters in alphabetical order to label the rows.

4	6	3	1	2	5
М	E	E	Т	М	E
А	Т	Т	н	E	L
0	С	к	E	R	S
Ν	0	W	Z	G	R

# 4.Plaintext = MEET ME AT THE LOCKERS NOW (ZGR are filler letters) Ciphertext = THEZ MERG ETKW MAON ELSR ETCO

## **Route Cipher**

Another type of transposition cipher. On a filled table with the letters from the plaintext, spiral inwards starting from the top right then route clockwise.

A	I	Т	А	Т	L	
1	W	Т	т	E	А	
	А	0	А	R	S	
	N	E	F	С	S	$\langle \cdot \rangle$

## 5.Plaintext = I WANT TO EAT AFTER CLASS Ciphertext = LASSC FENAW ITATE RAOTT