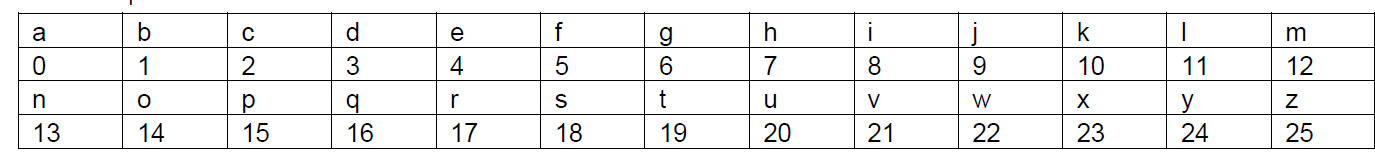
Substitution cipher

1.Caesar Cipher



**E(𝑝) = (𝑝 + 𝑘) mod (26)**

**P: plaintext... hello h-7, e- 4, l-11, 0-14**

**h= (7+)mod 26=10**

**e= (4+3)mod 26=7**

**l= (11+3)mod 26**

**0=(14+3)mod 26**

**K: 3,C=? KHOOR**

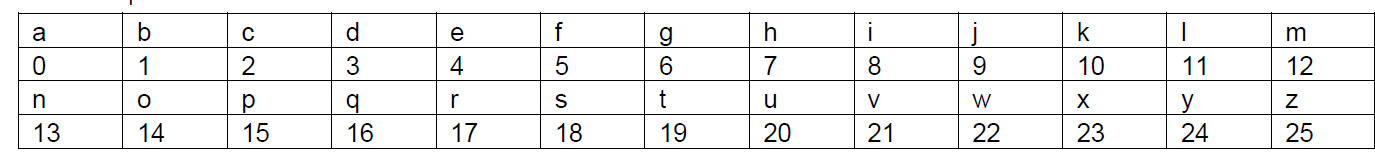
1. **Paintext= hello**

**K=3**

**C= KHOOR**

**D(C) = (C – 𝑘) mod (26)**

**K= (10-3) mod 26 hello**



**2) Paintext : attend the meeting at ten**

**K= 5**

**C=?**

**FYYJSI YMJ RJJYNSL FY YJS**

**E(𝑝) or C = (𝑝 + 𝑘) mod 26**

**D(c)or p= (c-k)mod 26**

a: (0+5) mod 26 F

FYYJSI YMJ RJJYNSL FY YJS

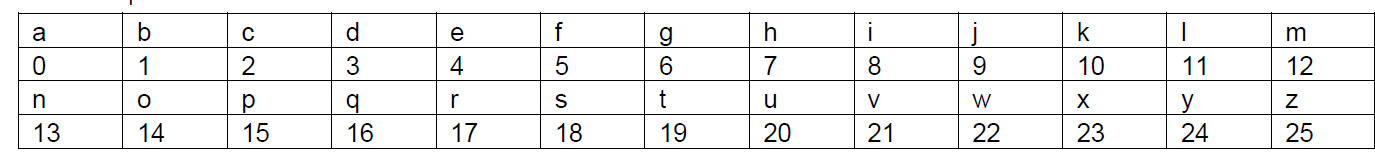
**D(C) or p = (C – 𝑘) mod (26)**

**3)**

**Plaintext ,p sathyabama**

**K=3**

**C=? D(C) = (C – 𝑘) mod (26)**



**VDWKBDEDPD**

**Example 4) P=kingdom**

**K=4**

**C=?**

**C=(p+k)mod 26**

**Monoalphabetic Substitution Cipher**

**P=db**

**C=?E**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **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** |
| **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** | **a** |

Playfair cipher

Example 1



**Plaintext : balloon**

**Keyword :monarchy**

**P= ba ll oo n**

**P= ba lx lo on**

**C = I/JB**

Example 2:

**P=Hi friends**

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

**K=Hello**

**hi fr ie nd sx**

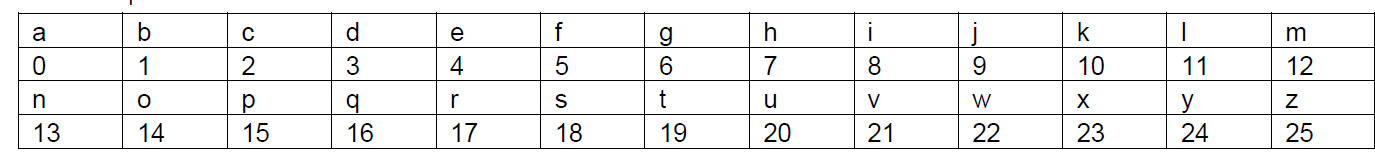
**BQ CT KH MF XL**

**HILL CIPHER**

This example will rely on some linear algebra and some number theory. The key for a hill cipher is a matrix e.g.

**2 12**

**1 7**



* **C =(k.p) mod 26**
* **P=K-1c mod 26**
* **Plaintext sathya**

**Sa th ya**

**C = 2 12 18 mod 26**

**1 7 0**

C= 2\*18 + 2\*0 mod 26

1\*18+7\*0

C= 36 mod 26

18

**KSSQWY**

C= 10

18

th c = 2 12 19

1 7 7

2 12 24

1 7 0

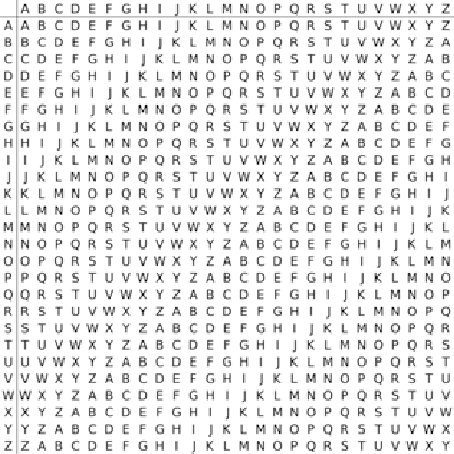
Example 2

k= 4 12 2

5 3 7

4 8 1

P= attack in dawn

* ****
* **Vignere cipher**

Keyword :hello

Plaintext:network security

Plaintext : networksecurity

Keyword: hellohellohello

K:deceptive

P:we are discovered

ZICVT WQNGRZGVTW

Vernam cipher

c=p xor k

p= 10011001

K= 11101011

C=01110010

One Time pad

C= ((P + K)-1) mod 27

Plaintext: the knife 20

12

Keyword: lllhsqdq

:ascgbhyd

C= (20+12)-1 mod 27 DSPREYIU

C= 31 mod 27

C=4

C=(8+12)mod27

20

Transposition technique

1.Columnar technique Transposition(plaintext)

P:hi hello how are you

41235

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| h | i | h | e | l |
| l | o | h | o | w |
| a | r | e | y | o |
| u | d | e | a | r |

C=EOYAHLAUIORDHHEELWOR

2. Double Columnar technique

Transposition(transposition(plaintext))

P:hi hello how are you

K:41235

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| h | i | h | e | l |
| l | o | h | o | w |
| a | r | e | y | o |
| u | d | e | a | r |

C=EOYAHLAUIORDHHEELWOR

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| E | O | Y | A | H |
| L | A | U | I | O |
| R | D | H | H | E |
| E | L | W | O | R |

AIHOELREOADLYUHWHOER