# Cryptography:-

plaintext – message in its original form.

ciphertext – disguised form of the message.

## Encryption (enciphering):-

– The process of converting a plaintext into ciphertext.

Decryption:- The reverse process.

## Message units:-

### Single letter message units:-

– each alphabet is considered as a message unit.

digraphs:- a pair of letters (alphabets) are considered as a message unit.

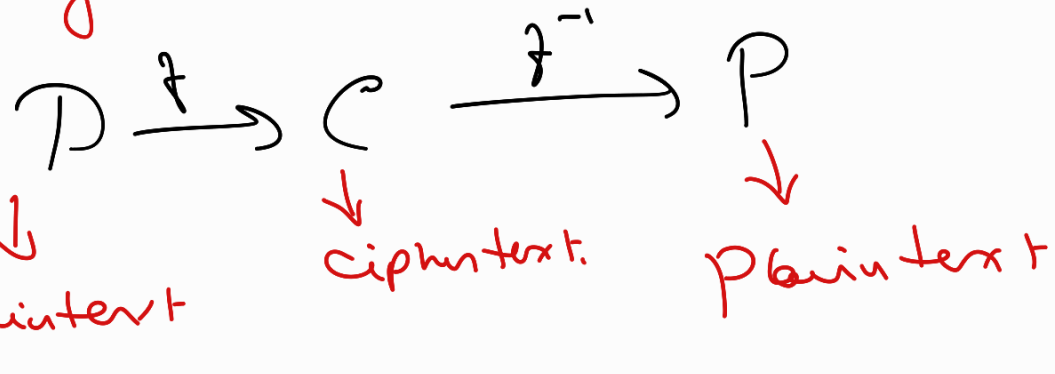
ex:- COME

CO → 1st digraph.

ME → 2nd digraph.

Trigraphs:- A triple of letters (alphabets).

Crypto-system




$f \rightarrow$ encryption mapping

$f^{-1} \rightarrow$ decryption mapping.

## Labelling of plaintext/ciphertext:-

A-Z can be labelled as 0, 1, 2, ..., 25. as numerical equivalents.

Special characters may be labelled as 26, 27, .... etc.

Digraphs may be labelled as $Nx+y$, where N is number of alphabets, x and y are

numerical equivalents of first and second letters of the digraph.

Ex:- In 26 letter alphabet 'ON' is calculated as $26 \times 14 + 13$

$= 377$

## Affine mapping:-

$$C \equiv aP + b \pmod{N}.$$

Ex:- $a = 7$ and $b = 12$

The plaintext "PAYMENOW" can be encrypted as:

15 - 0 - 24 - 12 - 4 - 13 - 14 - 22

$C \equiv aP + b \pmod{26}$ → 13 - 12 - 24 - 18 - 14 - 25 - 6 - 10

$\Rightarrow$ "NMYSOZGK"

Ex:- You intercept the ciphertext = "APNULPZTQANHF", which you know was encrypted using an affine map on digraphs in 26-letter alphabet. An extensive statistical analysis of earlier ciphertexts which had been coded by the same enciphering map shows that the most frequently occuring digraphs in all of that ciphertext are "IX" and "TQ", in that order. It is known that the most common digraphs in the English Language are "TH" and "HE", in that order. Read the message.

$$C \equiv aP + b \pmod{N^2} \rightarrow \text{encryption scheme.}$$

$IX \Rightarrow 26\times 8 + 23 = 231$
$TQ \Rightarrow 26\times 19 + 16 = 510$

$TH \Rightarrow 26\times 19 + 7 = 501$
$HE \Rightarrow 26\times 7 + 4 = 186$

$$P \equiv a^{-1}C - a^{-1}b$$

$\Rightarrow$
$$\left.\begin{aligned} 501 &\equiv 231\,a^{-1} - a^{-1}b \\ 186 &\equiv 510\,a^{-1} - a^{-1}b \end{aligned}\right\} \text{ Subtracting } \Rightarrow$$

$$\Rightarrow 279\,a^{-1} \equiv -315 \equiv 361 \pmod{26^2}$$

$$\therefore a^{-1} \equiv 361 \times 279^{-1} \pmod{676}$$
$$\equiv 361 \times 63 \equiv \underline{435} \pmod{676}$$

Now $-a^{-1}b = 501 - 231a^{-1}$

$= 501 - 231 \times 435 \equiv 64 \pmod{676}$

∴ Decryption scheme:

$P \equiv a^{-1}C - a^{-1}b$

$\Rightarrow P \equiv 435C + 64 \pmod{676}$

PW $\Rightarrow 26 \times 15 + 22 = 412 \rightarrow P = 144 = 26 \times 5 + 14$

VL $\Rightarrow 26 \times 20 + 11 = 531 \rightarrow = 533 = 26 \times 20 + 13$

PZ $\Rightarrow 26 \times 15 + 25 = 415 \Rightarrow 97 = 26 \times 3 + 19$

TQ $\Rightarrow 26 \times 19 + 16 = 510 \rightarrow 186 = 26 \times 7 + 4$

AW $\Rightarrow 26 \times 0 + 22 = 22 \rightarrow 170 = 26 \times 6 + 14$

HF $\Rightarrow 26 \times 7 + 5 = 187 \rightarrow 289 = 26 \times 11 + 3$

Required plaintext is "FOUNDTHEGOLD"