CRYPTOGRAPHY

It was coined by combining 2 Greek works

1) 'Krypto' meaning hidden
2) 'graphene' meaning writing.

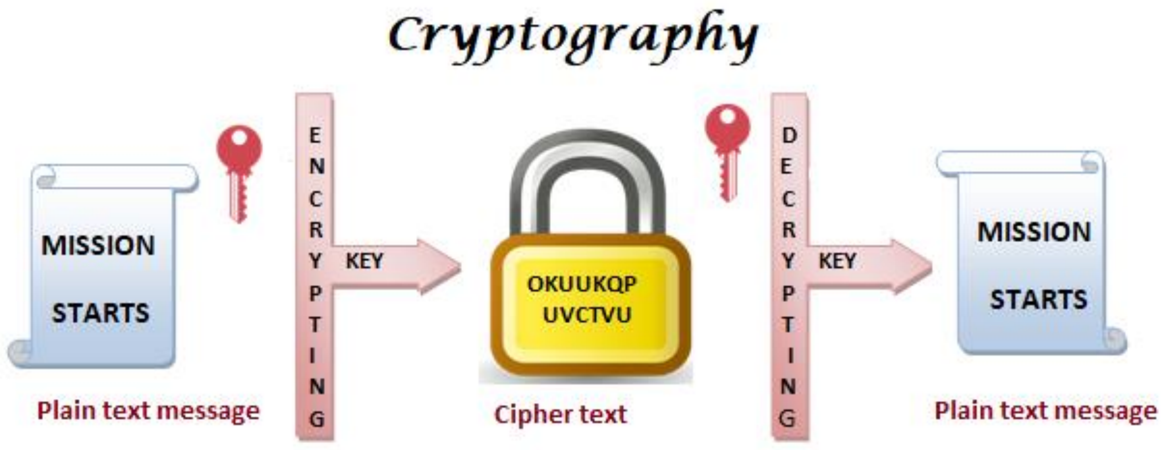
Cryptography is the art and science of making a cryptosystem that is capable of providing information security.

Or

Many schemes used for encryption

Encryption : Process of converting plain text into cipher text

Decryption : Process of converting cipher text into plain text



Key: Value independent of plain text and the Algorithm

2 types of keys :

1) Symmetric key : same keys are used for encrypting and decrypting
2) Asymmetric Key : different keys are used for encrypting and decrypting the information

Traditional Ciphers :

1) All of these systems are based on symmetric key encryption scheme
2) It also called as substitution ciphers

What are traditional ciphers?

1) Caesar Cipher
2) Monoalphabetic cipher’
3) Playfair Cipher
4) Hill Cipher

1) Caesar Cipher :

- each letter of the plaintext is substituted by another letter to form the ciphertext
- in this the key value is numerical and the key called as shift

eg:consider plain text and shift

plain text- welcome

shift= +3

Total alphabets

Give text = WELCOME

Shift = +3

W -> Z L -> O C -> F O -> R

E -> H M -> P E -> H

After perfoming shift the word is = ZHOFRPH

Hence the Cipher Text is "ZHOFRPH"

2) Monoalphabetic Cipher

- Here the size of key is 26

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
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

- In this the every alphabet is mapped with random alphabet which chosen in key

Plain text = WELCOME

W -> Z	E -> B	L -> J	C -> V
O -> M	M -> L	E -> B	

Hence Cipher Text = ZBJVMLB

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

3) Playfair Cipher :

Example: consider ,

Plain-Text = INSTRUMENTS
Key = MONARCHY

Steps :

1) Construct a 5*5 matrix
2) Fill the letters of the key in the matrix and remaining all the letter in the matrix

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

In key alphabets are repeated just omit those

3) Now split the plain text into pair of letters if there are odd letters then add Z to the last letter

   "IN" "ST" "RU" "ME" "NT" "SZ"

4) Follow the rules to find the Cipher Text
   i. If both letters are in same coloumn then take a letter below each one

      "ME" → " CL"

   ii. If both letters are in same row then take a right of each one

“ST” → “TL”

iii. If neither of above rules is true then form a rectangle and take the letter of horizatal opposite corner of rectangle

“NT” → “RQ”
“IN” → “AG”
“RU” → “MZ”
“SZ” → “TX”

INSTRUMENTS - AGTLMZCLTX

4) Hill Cipher

- The key size should be the length of N*N

N= Size of text

Consider,

Plain-Text = ACT

Key = GYBNQKURP

Consider a matrix for the key

G	Y	B
N	Q	K
U	R	P

6	24	1
13	16	10
20	17	15

Now make a matrix for the word

0
2
19

Now multiply those 2 matrices then we get

6	24	1
13	16	10
20	17	15

*

0
2
19

67
222
319

Now just perform mod(26) with the values in the matrix then we can get

15
14
7

The cipher text is = “POH”

1) Vignere Cipher

In this the size of key should be less than or equal to the size of the text

Example : Consider ,

Key = ABC

Plain-Text = DEFGHIJK

Now, the numerical value of a is 0 and the numerical value of z is 25

Plain-Text = D E F G H I J K

Numerical values = 3 4 5 6 7 8 9 10

Numerical Values =0 1 2 0 1 2 0 1

KEY = A B C

Now add both the numerical values of both plain-text and key then we can get the numerical values of cipher-text

The numerical values are

3 5 7 6 8 10 9 11

Hence , the cipher-text is = DFHGIKJL