E Introduction to

Crypto graphy and Network Security

L->R | R<-L

Crypto=Secret=0,1:1111-ABCD---XYZ:Enc,Dec|Key|MF

Shift by 3: A-D, B-E ABC|XYZ

Graphy=Writing =Code|Prog->set of instruction – while,do while,for,goto,rec-cbis 5:120

Network=LAN, MAN, WAN,=Job/Placement

Security=to protect the data=SA

L->R

Cryptography == secret writing

Data: Information (99.9999)

Data: Raw facts (100% True)

Student data: RegdNo: 1210305001

Name: Rama,DoB:10-Aug-2020,cgpa=5.6 :6

P1---→P2 Communicate ->Language ->TL,EL|HL

P1-TL   P2- P3->TL,EL,T

Computer ->Binary Language (0,1)MLL

ED-EC| power| stats ON(1),OFF(0)

1010101,00001010,

AI-MML-ALGOL: 1960,B,BCPL,

C,C++,Java,.Net

English: a-z, A-Z, 0-9, @,%,^

ASCII- A=65->$65_{(2)=1000001}$

0-255=256 64KB=0-65535=65536

Example: plain text: Welcome

A,b,c,d,e,f,g,h

D E F G H……ABC

A B C D E

Key1: shift by >3

PT	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
CT	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

CT: ZHOFRPH

DC: Key2:shift<3

PT:WELCOME

Q&A Session

Cryptology: The two main branches of cryptology are

Cryptography: The Science & art of creating secret codes.

Cryptanalysis: The Science & art of breaking those codes.

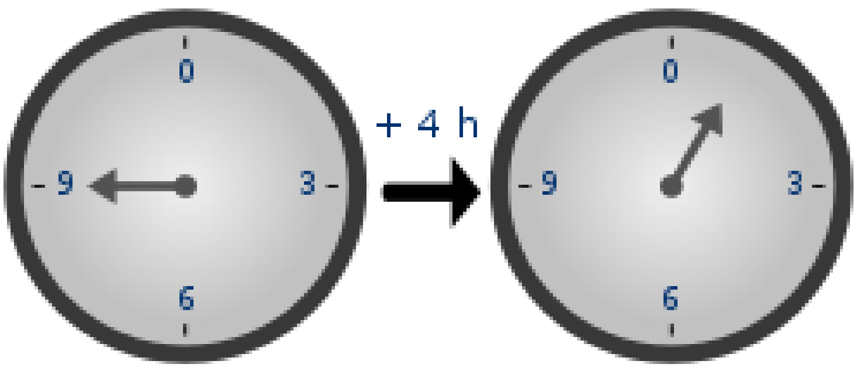
A cryptographic algorithm plus all possible keys and all the protocols that make it work comprise a CRYPTOSYSTEM

Computer security: The security of computers against intruders (e.g., hackers) and malicious software (e.g., viruses). Typically, the computer to be secured is attached to a network and the bulk of the threats arise from the network.

Modular arithmetic is a system of **arithmetic** for integers, which considers the remainder. In **modular arithmetic**, numbers "wrap around" upon reaching a given fixed quantity (this given quantity is known as the **modulus**) to leave a remainder.

The **modulus** is another name for the remainder after division. For **example**, 17 **mod** 5 = 2, since if we divide 17 by 5, we get 3 with remainder 2. **Modular arithmetic** is sometimes called clock **arithmetic**, since analog clocks wrap around times past 12, meaning they work on a **modulus** of 12.

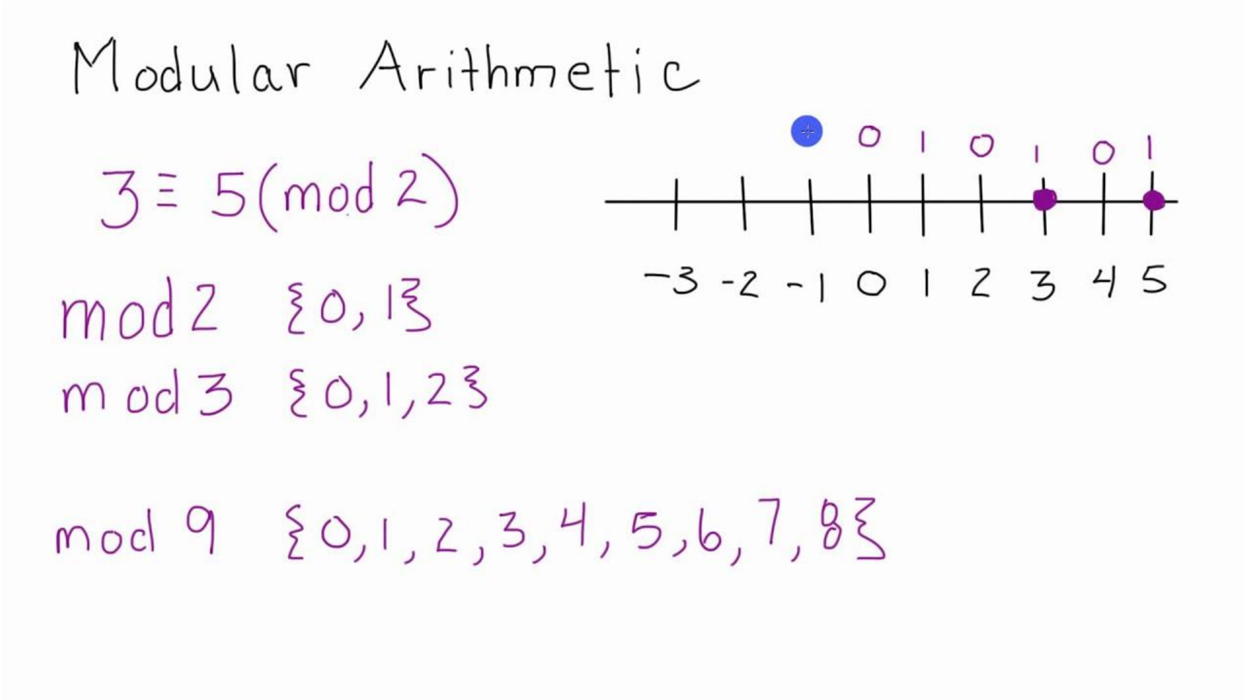
In **mathematics**, **modular arithmetic** is a system of **arithmetic** for integers, where numbers "wrap around" when reaching a certain value, called the modulus. ... A familiar use of **modular arithmetic** is in the 12-hour clock, in which the day is divided into two 12-hour periods.



Modular arithmetic

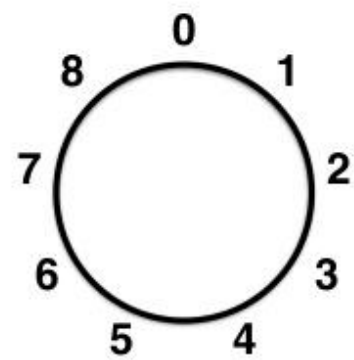
In **mathematics**, **modular arithmetic** is a system of **arithmetic** for **integers,** where numbers "wrap around" when reaching a certain value, called the **modulus**. The modern approach to modular arithmetic was developed by **Carl Friedrich Gauss** in his book **Disquisitiones Arithmeticae**, published in 1801.

A familiar use of modular arithmetic is in the **12-hour clock**, in which the day is divided into two 12-hour periods. If the time is 7:00 now, then 8 hours later it will be 3:00. Simple addition would result in 7 + 8 = 15, but clocks "wrap around" every 12 hours. Because the hour number starts over after it reaches 12, this is arithmetic *modulo* 12. In terms of the definition below, 15 is *congruent* to 3 modulo 12, so "15:00" on a **24-hour clock** is displayed "3:00" on a 12-hour clock.



Modulus 9

0 mod 9 = 0	9 mod 9 = 0
1 mod 9 = 1	10 mod 9 = 1
2 mod 9 = 2	11 mod 9 = 2
3 mod 9 = 3	12 mod 9 = 3
4 mod 9 = 4	13 mod 9 = 4
5 mod 9 = 5	14 mod 9 = 5
6 mod 9 = 6	15 mod 9 = 6
7 mod 9 = 7	16 mod 9 = 7
8 mod 9 = 8	17 mod 9 = 8



Properties of Modular Arithmetic

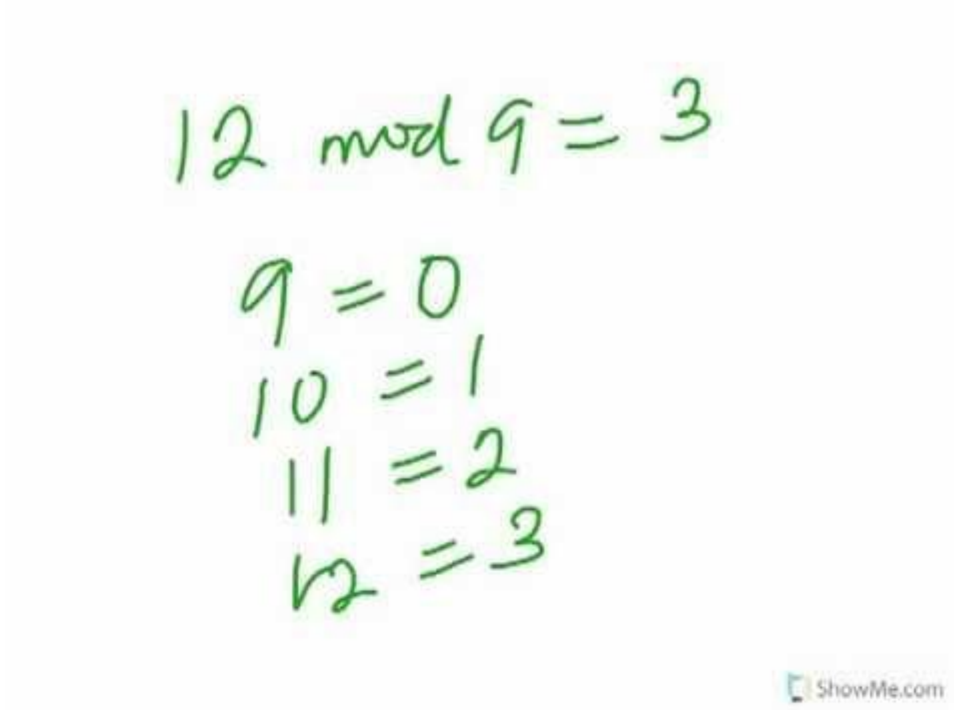
1. $[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$
2. $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$
3. $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$

Proof of 1.

Let $(a \bmod n) = Ra$ and $(b \bmod n) = Rb$. Then, we can write

$a = Ra + jn$ for some integer j and $b = Rb + kn$ for some integer k.

$$\begin{aligned}(a + b) \bmod n &= (Ra + jn + Rb + kn) \bmod n \\ &= [Ra + Rb + (k + j)\, n] \bmod n \\ &= (Ra + Rb) \bmod n \\ &= [(a \bmod n) + (b \bmod n)] \bmod n\end{aligned}$$



Modular Arithmetic

- A modulo operator `a mod n` leaves a remainder when a is divided by n
- congruence:
  - Two numbers a and b under some modular operation mod n are said to be **congruent** modulo n if (a mod b) = (b mod n)

- $a \equiv b \pmod{n}$ means n | (a-b)
  - when divided by *n*, a & b have same remainder
  - eg. 100 ≡ 34 mod 11
  - b is called the **residue** of a (mod n)
  - usually have $0 <= b <= n-1$

  Example $-12 \equiv -5 \equiv 2 \equiv 9 \pmod{7}$

1	0	0	0	0	1	1	1	1	0	

Field

File->set of Records ->set of fields -> set of bytes ->set of bit ->2NB----

Student File

Regd.No	Name	Cgpa
1217100310008	K	9.9
1217100310009	D	9.8
1217100310010	M	10
1217100310011	Y	9.98

Caesar Cipher

PT	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
CT	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

Mono alphabetic Cipher: Random cipher text letters

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

Example:

Plain Text: welcome

Cipher Text: RFSVHCF

Total Keys: 26!

In English Most common used letter:

E followed by T,R,N,I,O,A,S

Rare other letters: Z,J,K,Q,X

Most common used DIGRAMS letters are:

th,he,in,en,nt,re,er,an,ti,es,on,at,se,nd,ar,al,te,co,de,to,ra,et, ed,it,sa,em,ro

Most common used TRIGRAMS letters are:

the,and,tha,ent,ing,ion,tio,for,ade,has,nce,edt,tis,oft,sth,men

***** Mono alphabetic Cipher**

Relative letter frequency of

P=Frequency/Total characters x100

P=16/120x100=13.33

CT: {P,Z}={e,t}

P=13.33

Z=11.67

e=12.70

t=9.05

ZWP=the

Playfair cipher

To perform the substitution, apply the following 4 rules, in order, to each pair of letters in the plaintext:

Rule1: If both letters are the same (or only one letter is left), add an "X" after the first letter. Encrypt the new pair and continue.

Some variants of Playfair use "Q" instead of "X", but any letter, itself uncommon as a repeated pair, will do

Rule2:

Shape: Rectangle
Rule: Pick Same Rows,
Opposite Corners

Rule 3:

Shape: Column
Rule: Pick Items Below Each
Letter, Wrap to Top if Needed

Rule4:

Shape: Row
Rule: Pick Items to Right of Each
Letter, Wrap to Left if Needed

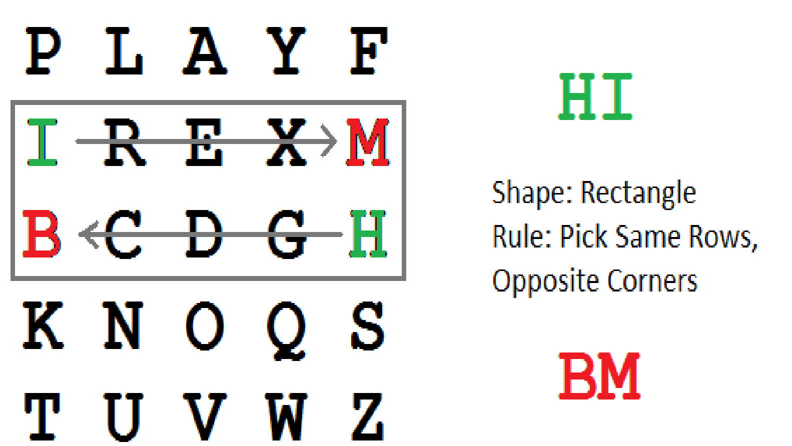
Example:

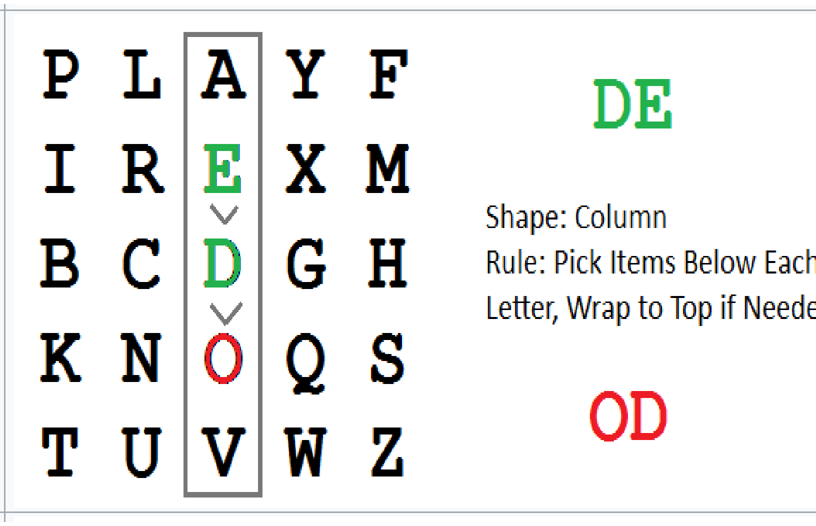
Using "playfair example" as the key (assuming that I and J are interchangeable), the table becomes (omitted letters in red):

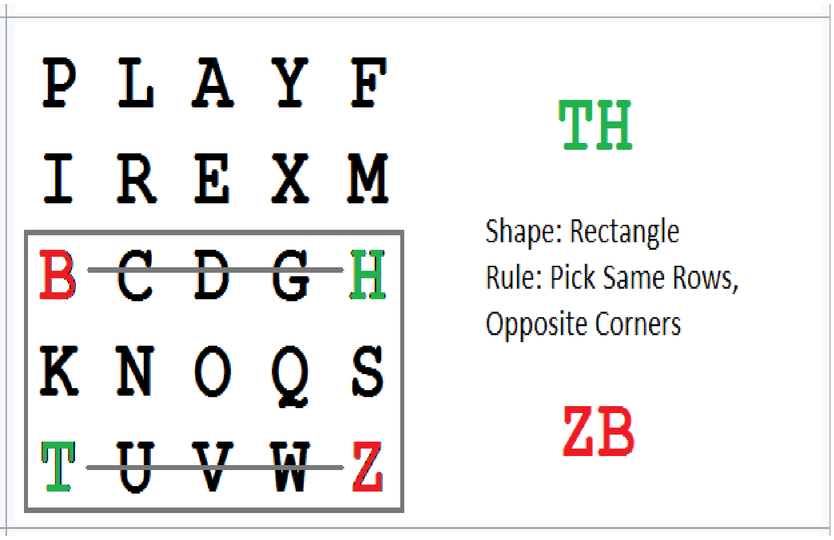

```
P L A Y F
I R E X M
B C D G H
K N O Q S
T U V W Z
```

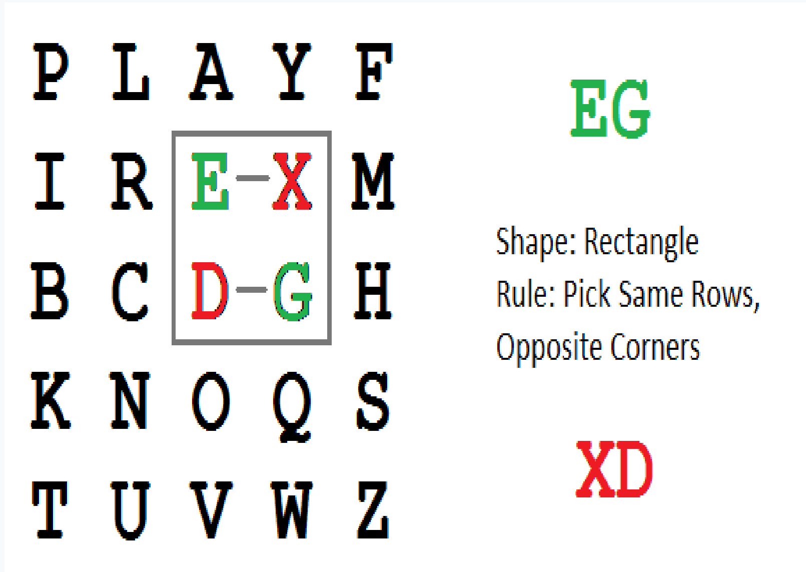
Encrypting the message "Hide the gold in the tree stump" (note the null "X" used to separate the re

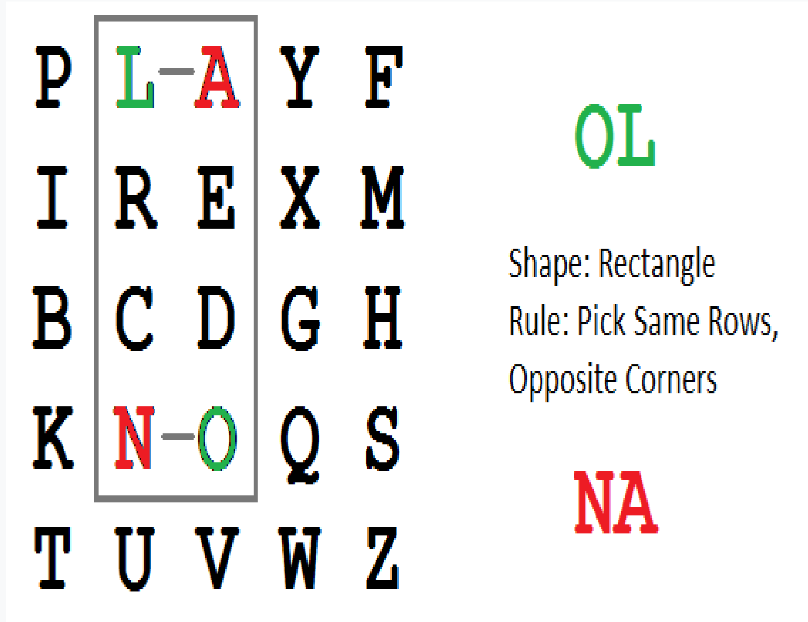
```
HI DE TH EG OL DI NT HE TR EX ES TU MP
                              ^
```

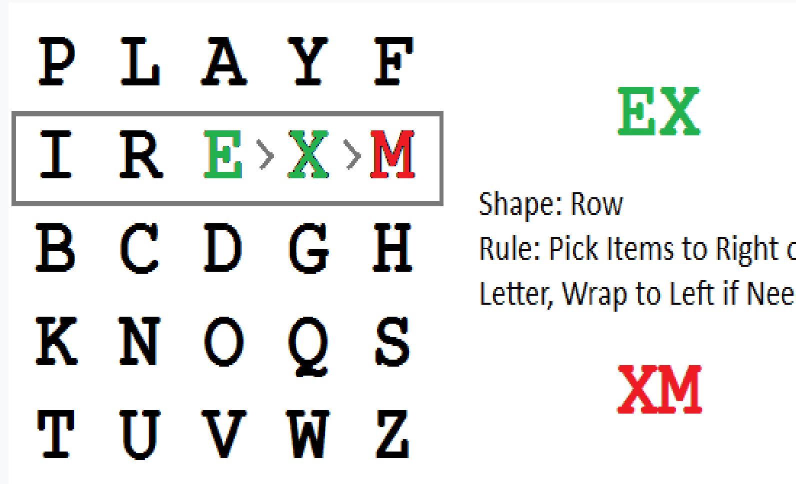
1. The pair HI forms a rectangle, replace it with BM	

2. The pair DE is in a column, replace it with OD	

3. The pair TH forms a rectangle, replace it with ZB	

4. The pair EG forms a rectangle, replace it with XD	

5. The pair OL forms a rectangle, replace it with NA	
6. The pair DI forms a rectangle, replace it with BE	
7. The pair NT forms a rectangle, replace it with KU	
8. The pair HE forms a rectangle, replace it with DM	
9. The pair TR forms a rectangle, replace it with UI	

10. The pair EX (X inserted to split EE) is in a row, replace it with XM	
11. The pair ES forms a rectangle, replace it with MO	
12. The pair TU is in a row, replace it with UV	
13. The pair MP forms a rectangle, replace it with IF	

```
BM OD ZB XD NA BE KU DM UI XM MO UV IF
```

Thus the message "Hide the gold in the tree stump" becomes "BMODZ BXDNA BEKUD MUIXM MOUVI F". (Breaks included for ease of reading the cipher text

Cryptanalysis

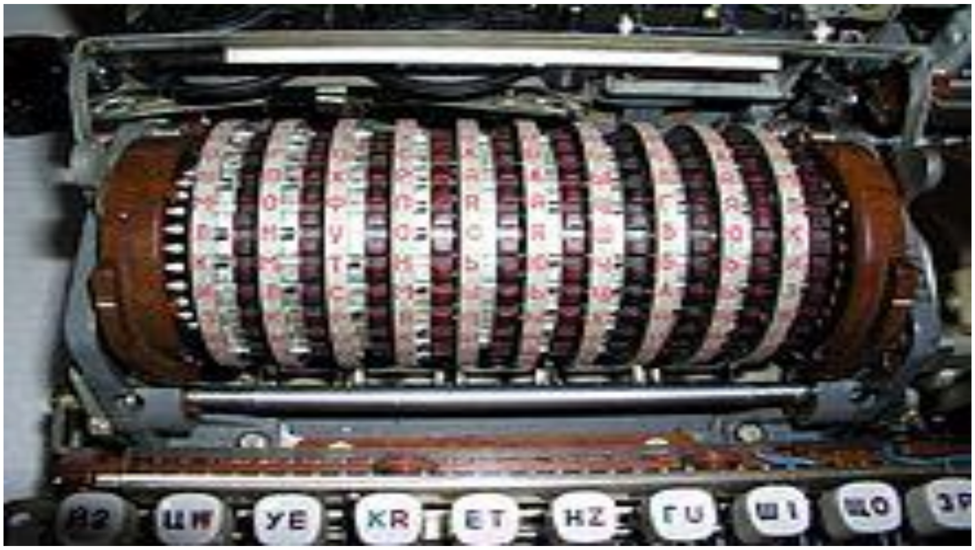
Like most classical ciphers, the Playfair cipher can be easily cracked if there is enough text.

Obtaining the key is relatively straightforward if both plaintext and ciphertext are known.

When only the ciphertext is known, brute force cryptanalysis of the cipher involves searching through

the key space for matches between the frequency of occurrence of digrams (pairs of letters) and

the known frequency of occurrence of digrams in the assumed language of the original message.



Cryptanalysis of Playfair is similar to that of [four-square] and [two-square] ciphers,

though the relative simplicity of the Playfair system makes identifying candidate plaintext strings easier.

Most notably, a Playfair digraph and its reverse (e.g. AB and BA)

will decrypt to the same letter pattern in the plaintext (e.g. RE and ER).

In English, there are many words which contain these reversed digraphs

such as REceivER and DEpartED. Identifying nearby reversed digraphs in the ciphertext and matching

the pattern to a list of known plaintext words containing the pattern is an easy way to generate

possible plaintext strings with which to begin constructing the key.

4 HILL CIPHER

- This was invented by lester S. Hill in 192
- This is based on linear Algebra.
- Hill used matrices and matrix multiplicat
  to mix up the plain text.
- His major Contribution was to use mathemat
  to design and analyse Crypto Systems

- The mathematics involved is "Number Theory".
- All values resulting from multiplication & addition are reduced by modulo 26, to keep them within the range of '26'

As an Example let us discuss Handling 3 letters at a time for Encryption & Decryption.

Given 3 plaintext letters p1, p2, p3.

we are to Encrypt these using relevant keys.

The Ciphertext letters are Called C1, C2, C3.

The relationship Can be Expressed as

The relationship can be expressed as

$$c_1 = (k_{11} \cdot p_1 + k_{12} \cdot p_2 + k_{13} \cdot p_3) \bmod 26$$

$$c_2 = (k_{21} \cdot p_1 + k_{22} \cdot p_2 + k_{23} \cdot p_3) \bmod 26$$

$$c_3 = (k_{31} \cdot p_1 + k_{32} \cdot p_2 + k_{33} \cdot p_3) \bmod 26$$

Rewriting in matrix form

$$\begin{vmatrix} C_1 \\ C_2 \\ C_3 \end{vmatrix} = \begin{vmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{vmatrix} \begin{vmatrix} P_1 \\ P_2 \\ P_3 \end{vmatrix} \bmod 26$$

In short hand notation : $\boxed{C = k \cdot P \bmod 26}$

Consider a plain Text 'ACT' which is the column Vectors.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

r	s	t	u	v	w	x	y	z
17	18	19	20	21	22	23	24	25

$$\therefore \quad ACT \Rightarrow \quad P = \begin{vmatrix} 0 \\ 2 \\ 19 \end{vmatrix}$$

let the Key be Expressed as 3×3 square matrix

$$K = \begin{vmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{vmatrix}$$ GYBNQKURP

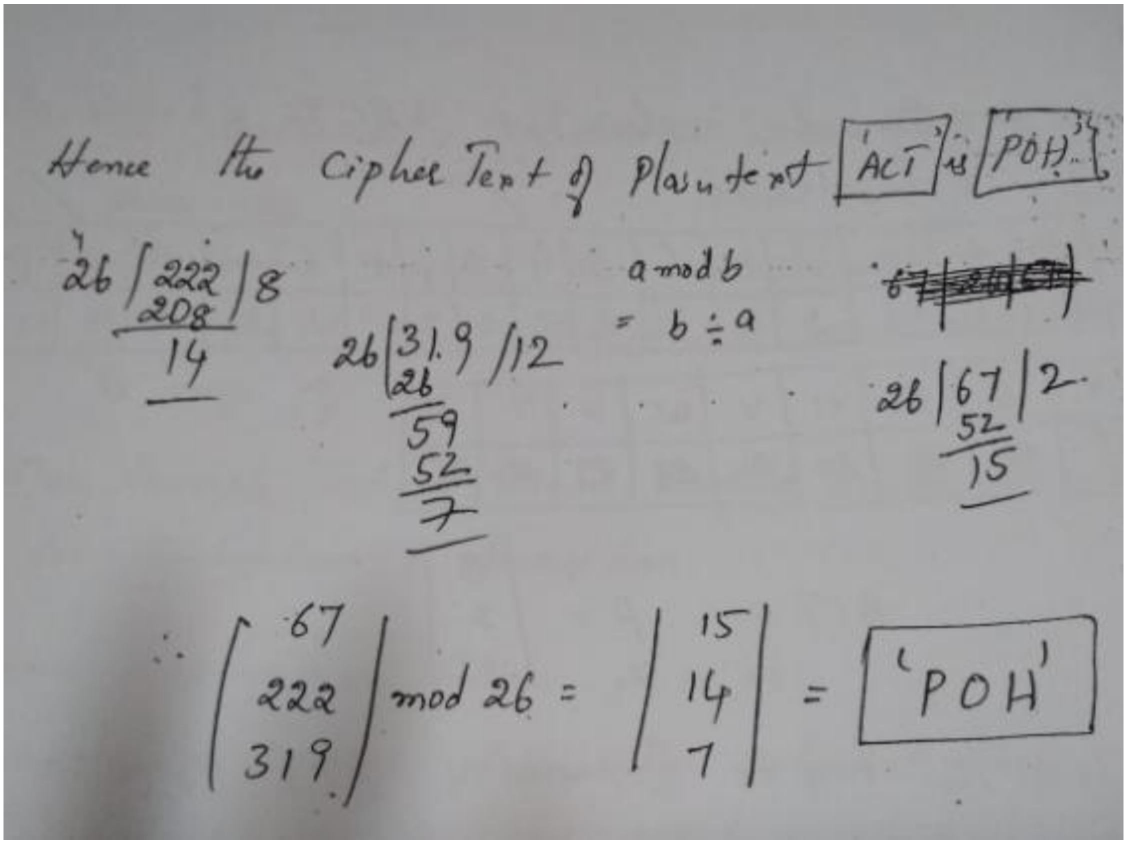
$$\boxed{C = K.P \bmod 26}$$

$$C = \begin{vmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{vmatrix} \times \begin{vmatrix} 0 \\ 2 \\ 19 \end{vmatrix} \bmod 26$$

$$= \begin{vmatrix} 6\times 0 + 24\times 2 + 1\times 19 \\ 13\times 0 + 16\times 2 + 10\times 19 \\ 20\times 0 + 17\times 2 + 15\times 19 \end{vmatrix} \bmod 26 = \begin{vmatrix} 0 + 48 + 19 \\ 0 + 32 + 190 \\ 0 + 34 + 285 \end{vmatrix} \bmod 26$$

$$= \begin{vmatrix} 67 \\ 222 \\ 319 \end{vmatrix} \bmod 26 = \begin{vmatrix} 15 \\ 14 \\ 7 \end{vmatrix} = \text{'POH'}$$

B. Prakash



Hence the Cipher Text of Plaintext $\boxed{\text{'ACT'}}$ is $\boxed{\text{'POH'}}$

$$26 \,\overline{)\, 222 \,}\, 8 \qquad 222 - 208 = 14$$

$$26 \,\overline{)\, 319 \,}\, 12 \qquad 319 - 26 = 59, \quad 59 - 52 = 7$$

a mod b = b ÷ a

$$26 \,\overline{)\, 67 \,}\, 2 \qquad 67 - 52 = 15$$

$$\therefore \begin{pmatrix} 67 \\ 222 \\ 319 \end{pmatrix} \bmod 26 = \begin{vmatrix} 15 \\ 14 \\ 7 \end{vmatrix} = \boxed{\text{'POH'}}$$

8	**5**	**10**	**15**	**P**
21	**8**	**21**	**14**	**O mod 26**
21	**12**	**8**	**7**	**H**

K^{-1}= 1/det(K) adj(K)

260		**0**	**A**
574	**mod 26**	**2**	**C**
539		**19**	**T**

Polyalphabetic Ciphers

Polyalphabetic Ciphers:

polyalphabetic cipher is based on Substitution of multipl Substitution alphabets.

*. VIGENERE Cipher is the best Example of polyalphabetic Cipher.

VIGENERE Cipher makes use of a table Consisting of 26 alphabets, where alphabets are shifted by one position in Successive rows.

Shown in below table

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

- let us Examine the application of Vigenere cipher for Encryption and Decryption.
- A KEY is generated as Row
  - A Key Can be made up of any number of alphabets, but Should be Extended as long as the plain text.
- A plaintext is generated in the next Row.
- Cipher text is Generated in another Row.

* The alphabet in key row is used as ROW INDEX
* The plaintext letters are used as COLUMN INDEX
* The intersection of Row & COLUMN is the CIPHER TEXT

Example.

(key) K P O E T R Y P O E T R Y P O E T R Y P O E T R Y P O

(plain text) P T H E C H I L D I S T H E F A T H E R O F T H E . M A

(cipher text) C I V I V Y G A R M L K F T T E M Y C G C J M Y C B O

Key : POETRYPOETRYPOETRYPOETRYPOE → Row Index

PlainText : THECHILDISTHEFATHEROFTHEMAN → Column Index

CipherText : IVIVYGARMLKFTTEMYCGCJMYCBOR → Intersection.

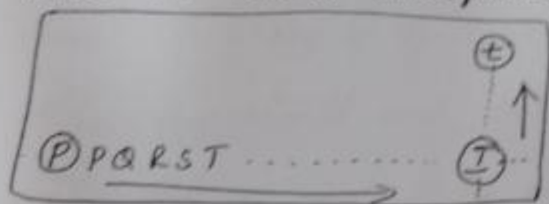
Decryption :

* Use the key letter to access the row
* Use Cipher text to access the Column
* The Intersection yields the plainText

ie for the Key P and Ciphertext I The plaintext will be t

∴ Consider the 'P' row in that row find "I"

∴ Now the value Corresponding to "I" will be the PlainText



VIGENERE cipher Can also be delt with Algebrically mathematically.

Consider the letter A to Z with position values 0 to 25

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U

21	22	23	24	25
V	W	X	Y	Z

Encryption of Plain text "P" using Key "T" is done as follows

$$\boxed{P = E_K(P, T)}$$

$= (P + T) \bmod 26 \Rightarrow (19 + 15) \bmod 26$

$= 34 \bmod 26 \Rightarrow 8 \bmod 26$

∴ Value of 8 = I which is the Cipher Text

Decryption of Ciphertext "I" using the Key "T" is

$C = D_K(I, T)$

$= (I - T) \bmod 26$

$= (8 - 19) \bmod 26$

$= -11 \bmod 26$

$= 15 \bmod 26 \Rightarrow$ "P"

∴ The Corresponding (value) letter of 15 is "P" which represents the 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
A	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	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
C	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	B
D	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
E	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	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	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

KEY: POETRY

Plain Text: THECHI

Cipher Text:IVIVYG

One-Time Pad (OTP)

Encryption Technique

One time Pad.

An improvement on Vigenere Cipher was suggested by Joseph Mauborgne, which gave ultimate Security.

- Here The key is of the Same length as the message
- The key should not be repeated or reused.
- The key is used Only once for Encryption and decryption, and there after discarded.
- This Scheme is Called "One-Time-Pad"
- As the ciphertext does not Contain any information about the plaintext, Breaking the Code becomes impossible.

- Here A table similar to "Vigenere" is used but with an additional character as 27th charac
- Hence we generate 27 × 27 table.
- The 27th character he suggested was a "SPACE
- A one time key which is as long as "key" is used.

Encryption Process.

- Encryption process is same as the "Vigenere" Cipher
- The only difference is we are using a "Blank" colum

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

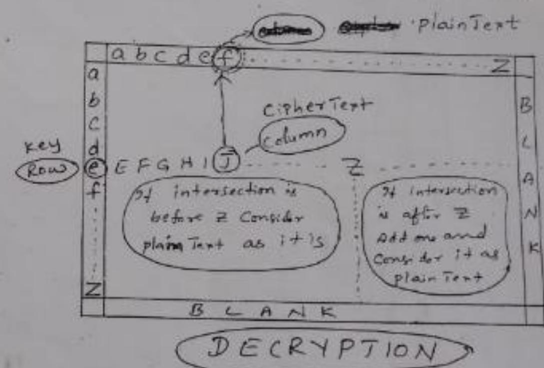
- Consider the Key as Row Index
- Consider the plainText as Column Index
- The intersection of Row and Column gives CipherText
- But Since Blank Space is used, If the intersection block is after "Z" then Subtract 1 from the

Encryption. (Key ⇒ Row , Plain Text ⇒ Column , Intersection ⇒ Cipher)

key: p x l m v m s y d o f u y r v z w c t n l e b n e c v g d u p a h f z z l m n y i

plain: m r   m u s t a r d   w i t h   t h e   c a n d l e s t i c k   i n   t h e   h a l l

cipher: A N K Y O D K Y U R E P F J B Y O J D S P L R E Y I U N O F D O I U E R F P L U Y T S

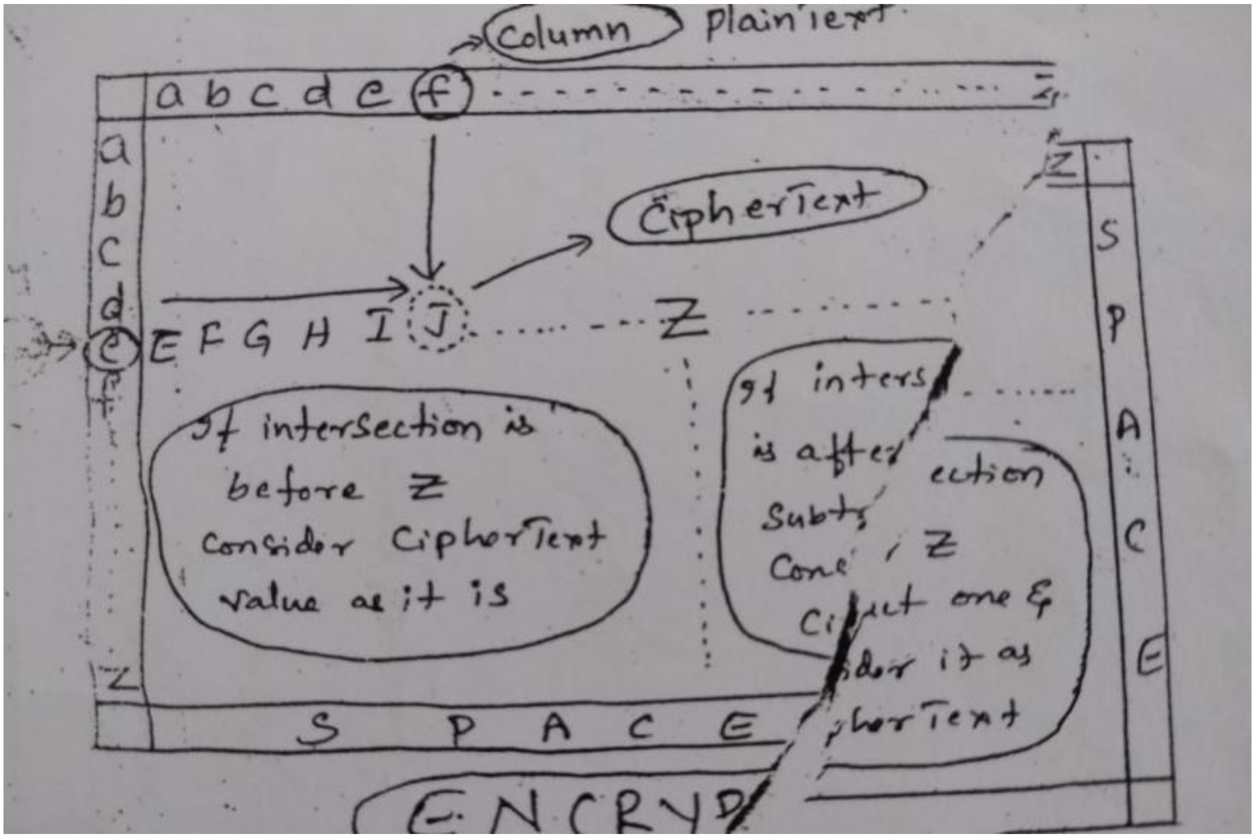


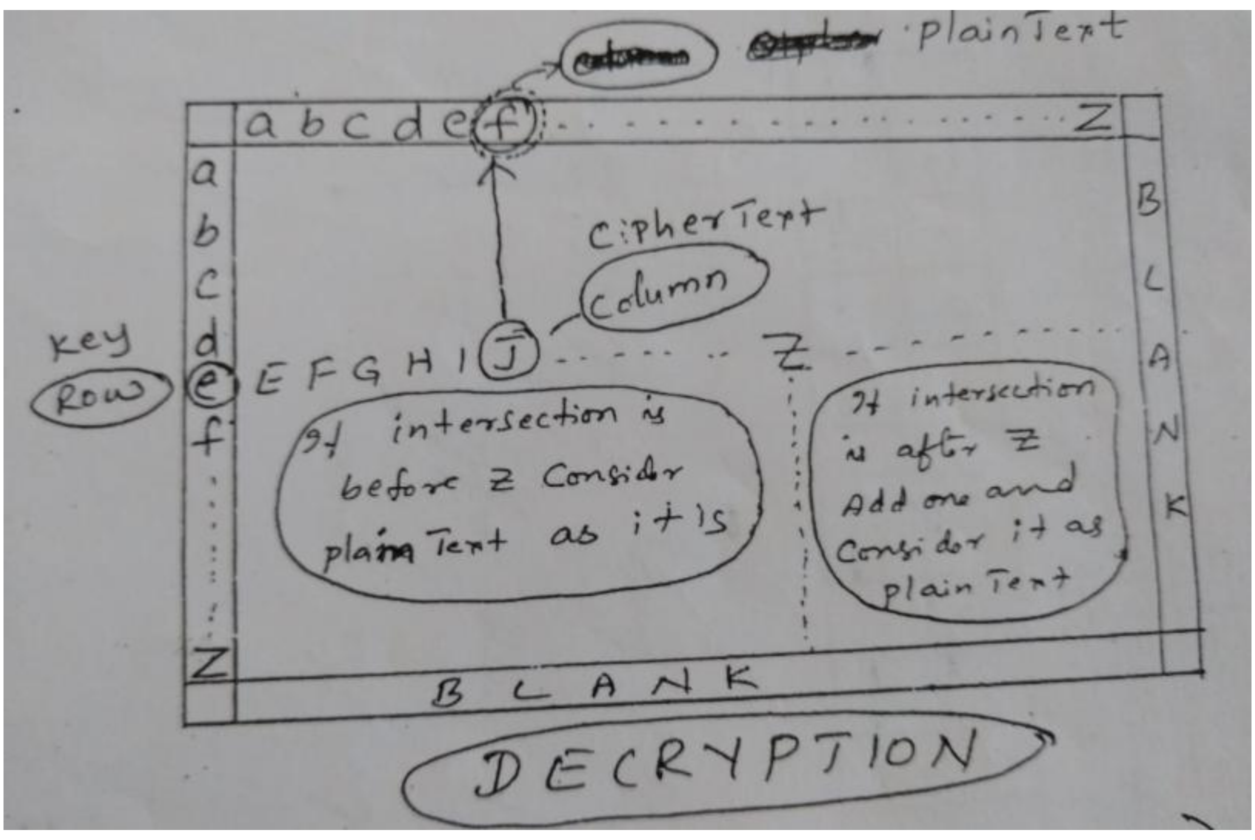
Decryption (Key ⇒ Row, Cipher ⇒ Column , Intersection ⇒ PlainText).

key: p x l m v m s y d o f u y r v z w c t n l e b n e c v g d u p a h f z z l m n y i h

cipher: A N K Y O D K Y U R E P F J B Y O J D S P L R E Y I U N O F D O I U E R F ? Y T S

plain: m r   m u s t a r d   w i t h   t h e   c a n d l e s t i c k   i n


Column
PlainText
a b c d e f ... z
CipherText
E F G H I J ... Z
If intersection is before Z consider CipherText value as it is
If inters
is after
ection
Z
ct one &
der it as
pherText
S P A C E
ENCRYP


PlainText
a b c d e f ... Z
CipherText
Column
Key
Row
E F G H I J ... Z
If intersection is before Z Consider plain Text as it is
If intersection is after Z Add one and Consider it as plain Text
B L A N K
DECRYPTION

Transposition Techniques

Rail Fence Technique

SITION TECHNIQUES. Unit I - 2 part

Mono

Kind of mapping achieved by performing Some Sort of permutation on the plain text letters is referred as Transposition Cipher.

(7) The Simplest of this Cipher is "Rail fence" Technique.

Rail Fence

- Here the Plaintext is written down as a Sequence of diagonals and then read off as a Sequence of rows.

Example . .

Consider the message

" meet me after the toga Party "

with the "Rail fence" of depth "2" we write as follows.

m		e		m		a		t		r		h		t		g		p		r		y
	e		t		e		f		e		t		e		o		a		a		t	

Encrypted message is

[illegible] rhtgp [illegible] tef [illegible] t."

Encryption & Decryption Pro[illegible]

Step 1.

Write down your plaintext message on a piece of Pa[illegible]

- Write Each letter of the plaintext on two Separ[illegible] Lines.
- The first letter goes on the first line
- The Second on the Second line
- The Third letter goes back on the first line
- and So on until we run out of letters.

Plain Text : 'CRYPTOLOGY IS FUN'

LINE1	C		Y		T		L		G		I		F		N	
LINE2		R		P		O		O		Y		S		U		

Step2

Count the total number of letters Used.

- The total number of letters should be Equal to multiple of 4 (ie, 8, 12, 16, 20...)
- If not you should add Extra letters Called "NULLS" until it is multiple of 4

LINE1	C		Y		T		L		G		I		F		N	
LINE2		R		P		[illegible]		O		[illegible]		S		[illegible]		X

Step3

- Begining with Line 1, Combine the letters from both lines to Create the 'Cipher Text'

Divide the letters into as many groups as you wish

Hence Cipher Text have been Created

Plain Text : "CRYPTOLOGY IS FUN"

LINE1	C		Y		T		L		G		I		F		N		
LINE2		R		P		O		O		Y		S		U		X	=NULL

Cipher Text : CYTLGIFNRPOOYSUX

⇒ CYTL GIFN RPO OYS UX

DECRYPTION

STEP 1 Divide the letters in half by drawing a line through the Cipher text

- Write the first half of the message on line and the Second half on Line 2
- Make sure you leave space between Each letter

1 2 3 4 5 6 7 8 | 9 10 11 12 13 14 15 16

Cipher Text: CYTL GIFN | RPO OYS UX.

Line 1	C		Y		T		L		G		I		F		N	
Line 2		R		P		O		O		Y		S		U		X

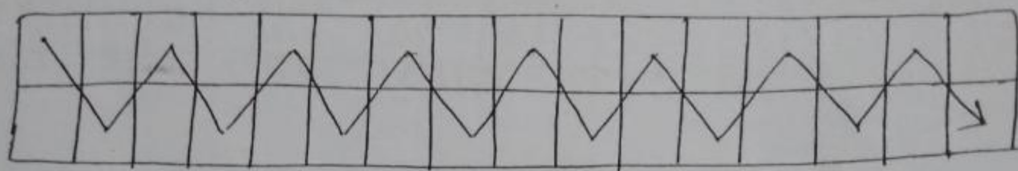
= NULL

Step 2.

Rewrite the message by Combining letters from Line 1 and Line 2

- make Sure that you alternate between Lines and leave out any "NULLS" that are included at the end.

Line1
Line2



Line1	C		Y		T		L		G		I		F		N	
Line2		R		P		O		O		Y		S		U		

Plain Text : CRYPTOLOGYISFUN

which is the Decrypted Plain text.

Multi Stage Transpositions

(05)

II. Multi Stage Transpositions.

- Here we perform the Transpositions for multipl times.

- Consider the plain Text

"attack postponed until twoamxyz"

Step 1

write the message in a rectangle row by row and read the message off column by column.

1	2	3	4	5	6	7
a	t	t	a	c	k	p
o	s	t	p	o	n	e
d	u	n	t	i	l	t
w	o	a	m	x	y	z

Step 2

Permute the order of columns (Rearrange)

The Order of the column becomes key to Algorithm.

Key	4	3	1	2	5	6	7
plaintext	a	t	t	a	c	k	p
	o	s	t	p	o	n	e
	d	u	n	t	i	l	t
	w	o	a	m	x	y	z

Ciphertext: $\underbrace{TTNA}_{1}\ \underbrace{APTM}_{2}\ \underbrace{TSUO}_{3}\ \underbrace{AODW}_{4}\ \underbrace{COIX}_{5}\ \underbrace{KNLY}_{6}\ \underbrace{PETZ}_{7}$

In this Example the Key is "4312567"
1234567

To Encrypt,

- Start with column that is labelled '1' (in this case column 3)

write down all the letters of that column.

- proceed to column no 4 which is labeled '2'.
- Then column 2, then column 1, then columns 5, 6 and 7.

Step:3

* Transposition Cipher Can be made more Secure by performing more than One stage of Transpositions.

- The result is more Complex that is not Easily reconstructed.

* If the above Cipher Text is re-encrypted Using Same k

$$\begin{array}{ll} \text{Key} & 4\ 3\ 1\ 2\ 5\ 6\ 7 \\ \text{PlainText} & \begin{cases} t\ t\ n\ a\ a\ p\ t \\ m\ t\ s\ u\ o\ a\ o \\ d\ w\ c\ o\ i\ x\ k \\ n\ l\ y\ p\ e\ t\ z \end{cases} \end{array}$$

Step:4 Re-Encrypt the Re-Encrypted Cipher Text

CipherText: NSCYAUOPTTWLTMDNAOIEPAXTTOKZ

$$\begin{array}{ll} \text{Key} & 4\ 3\ 1\ 2\ 5\ 6\ 7 \\ \text{plainText} & \begin{cases} n\ s\ c\ y\ a\ u\ o \\ p\ t\ t\ w\ l\ t\ m \\ d\ n\ a\ o\ l\ e\ p \\ a\ x\ t\ t\ o\ k\ z \end{cases} \end{array}$$

CipherText : $\underbrace{CTAT}_{1}$ $\underbrace{YWOT}_{2}$ $\underbrace{STNX}_{3}$ $\underbrace{NPDA}_{4}$ $\underbrace{ALID}_{5}$ $\underbrace{UTEK}_{6}$ $\underbrace{OMPZ}_{7}$

Step 5 Re-Encrypt the Re-Re-Encrypted CipherText

CipherText: $\underbrace{CTAT}_{1}$ $\underbrace{YWOT}_{2}$ $\underbrace{STNX}_{3}$ $\underbrace{NPDA}_{4}$ $\underbrace{ALIO}_{5}$ $\underbrace{UTEK}_{6}$ $\underbrace{OMPZ}_{7}$

key	4	3	1	2	5	6	7
	c	t	a	t	y	w	o
	t	s	t	n	x	n	p
	d	a	a	l	i	o	u
	t	e	k	o	m	p	z

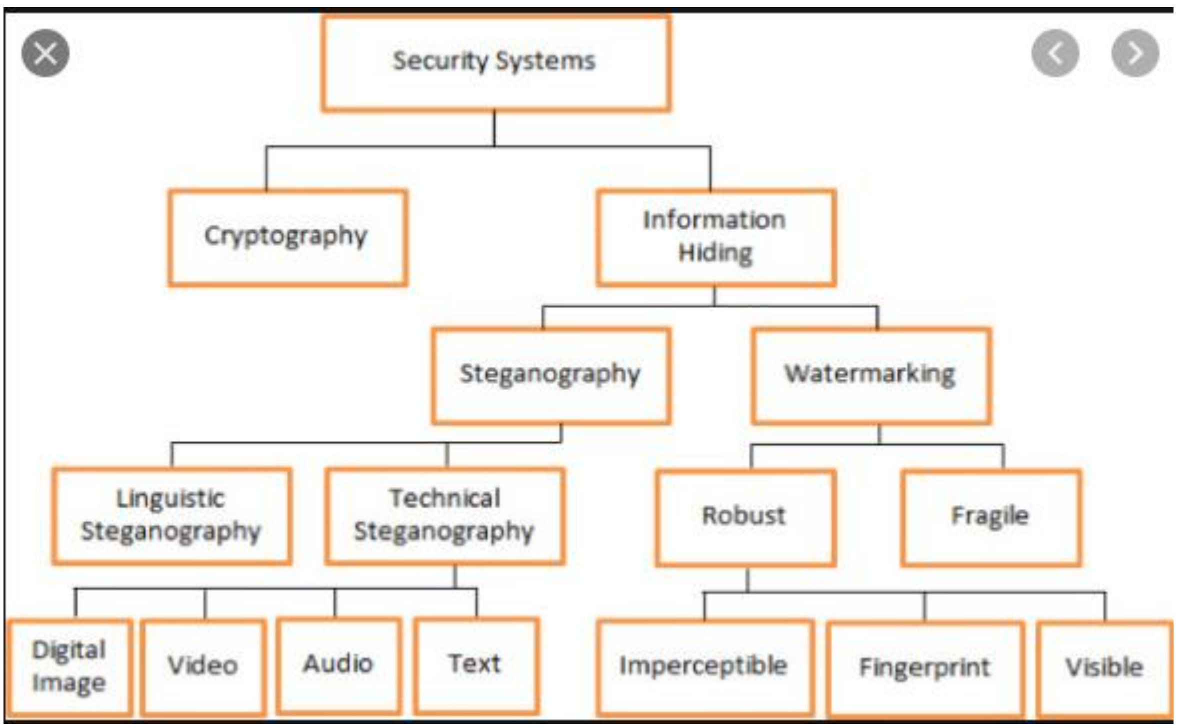
CipherText: $\underbrace{ATAK}_{1}$ $\underbrace{TNLO}_{2}$ $\underbrace{TSAE}_{3}$ $\underbrace{CTDT}_{4}$ $\underbrace{YXIM}_{5}$ $\underbrace{WNOP}_{6}$ $\underbrace{OPU}_{7}$

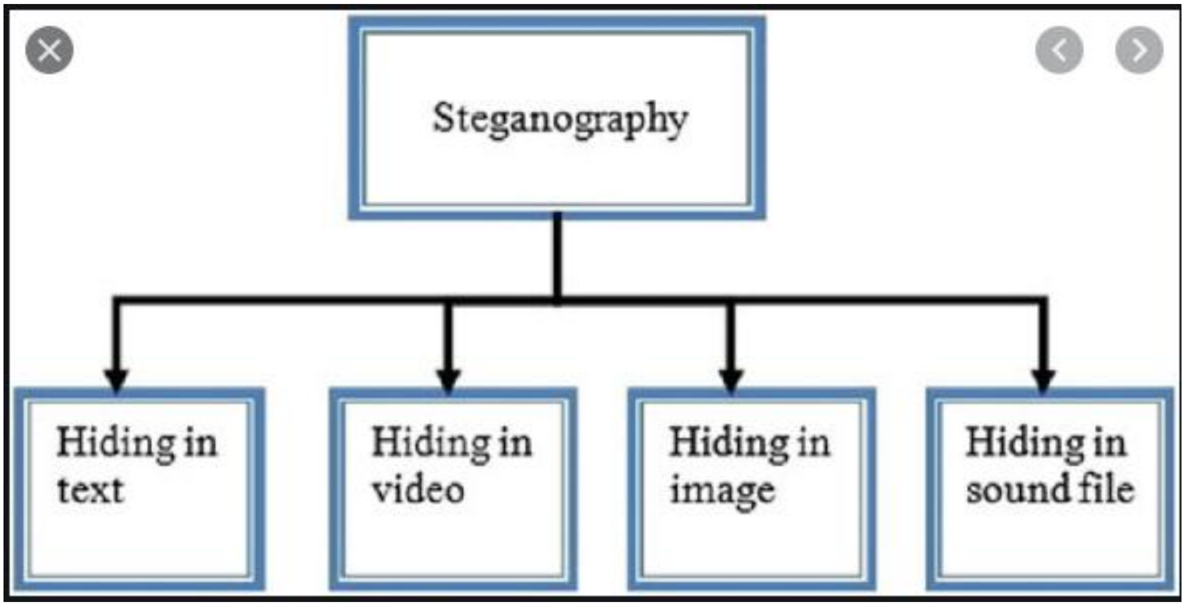
This is much more difficult to Cryptanalyze.

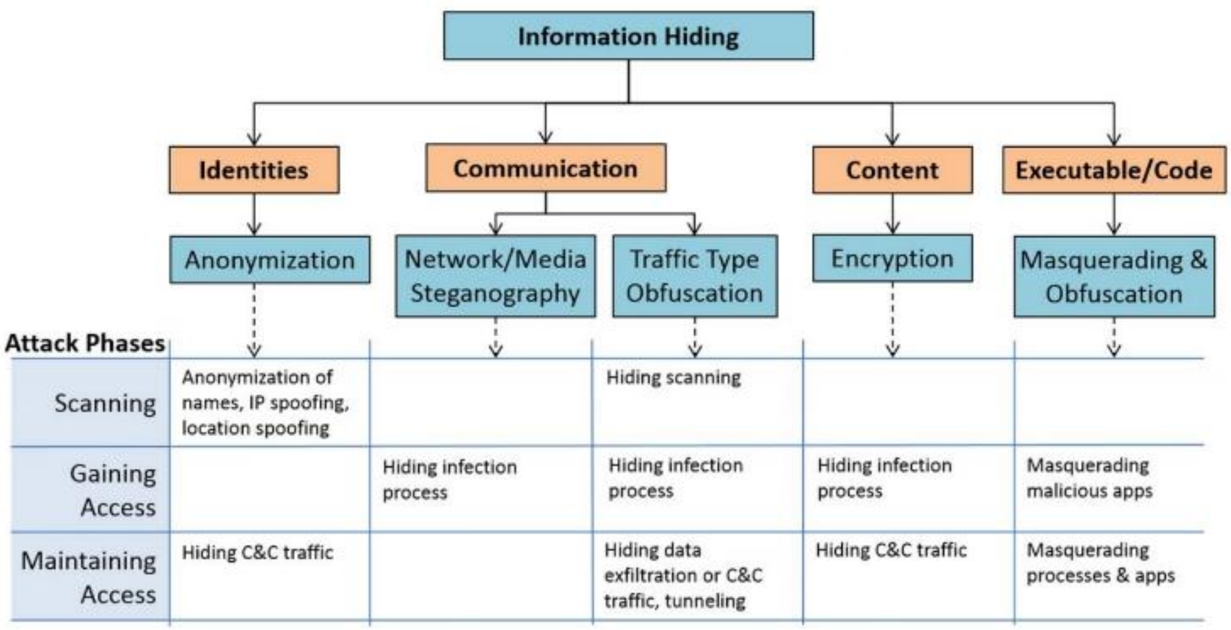
STEGANOGRAPHY

What Is Steganography?

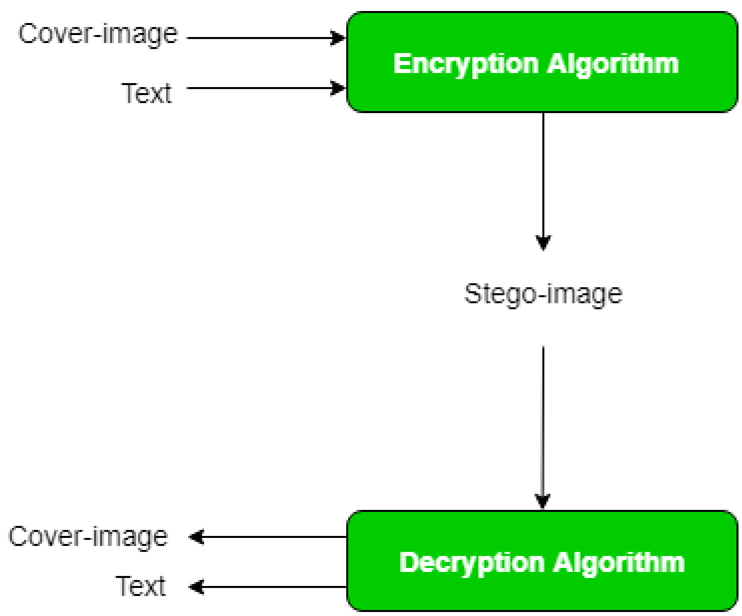
It's basically hiding bad things in good things.



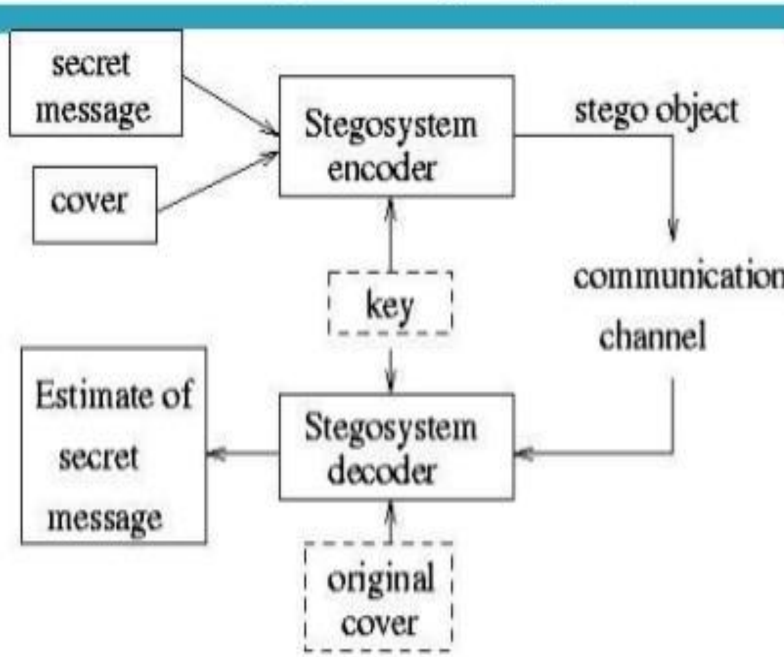

Steganography
Hiding in text
Hiding in video
Hiding in image
Hiding in sound file

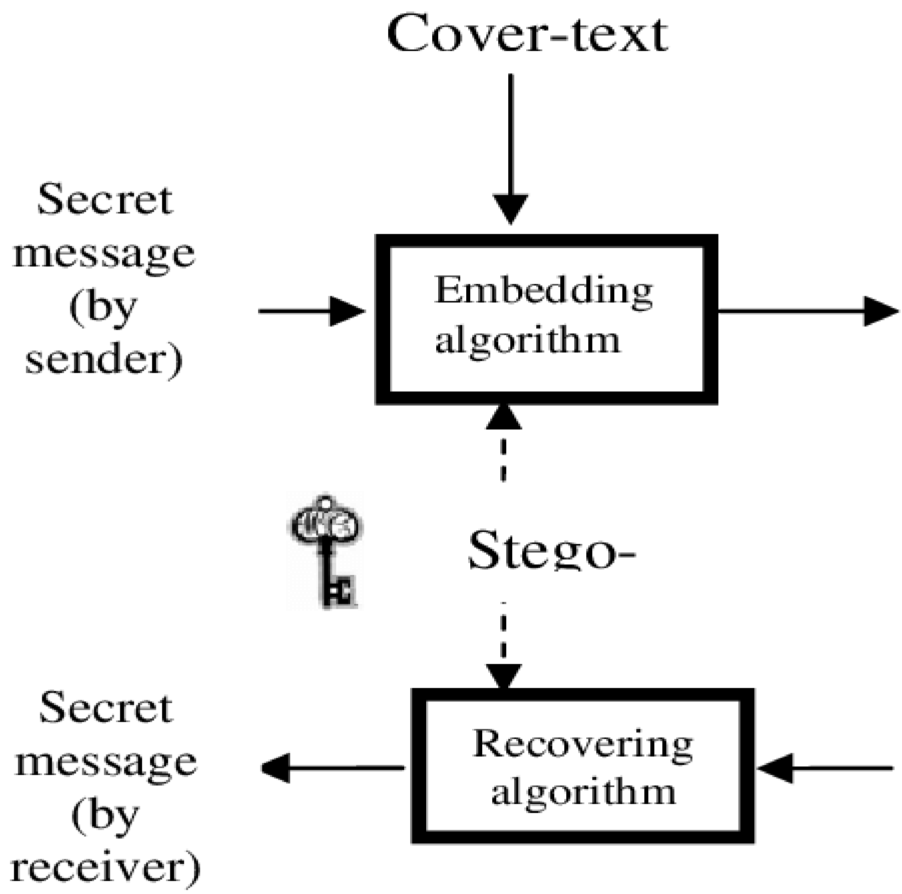

Information Hiding
Identities
Communication
Content
Executable/Code
Anonymization
Network/Media Steganography
Traffic Type Obfuscation
Encryption
Masquerading & Obfuscation
Attack Phases
Scanning
Anonymization of names, IP spoofing, location spoofing
Hiding scanning
Gaining Access
Hiding infection process
Hiding infection process
Hiding infection process
Masquerading malicious apps
Maintaining Access
Hiding C&C traffic
Hiding data exfiltration or C&C traffic, tunneling
Hiding C&C traffic
Masquerading processes & apps

	STEGANOGRAPHY	CRYPTOGRAPHY
Definition	It is a technique to hide the existence of communication	It's a technique to convert data into an incomprehensible form
Purpose	Keep communication secure	Provide data protection
Data Visibility	Never	Always
Data Structure	Doesn't alter the overall structure of data	Alters the overall structure of data
Key	Optional, but offers more security if used	Necessary requirement
Failure	Once the presence of a secret message is discovered, anyone can use the secret data	If you possess the decryption key, then you can figure out original message from the ciphertext



Basic Steganography Model




Cover-text
Secret message (by sender)
Embedding algorithm
Stego-
Secret message (by receiver)
Recovering algorithm

Examples: 

YOU KNOW ALL too well at this point that all sorts of digital attacks are lurking on the internet. You could encounter ransomware, a virus, or a sketchy phish at any moment. Even creepier, though, some malicious code can actually hide inside other, benign software and be programmed to jump out when you aren't expecting it. Hackers are increasingly using this technique, known as steganography, to trick internet users and smuggle malicious payloads past security scanners and firewalls. Unlike cryptography, which works to obscure content so it can't be understood, steganography's goal is to hide the fact that content exists at all by embedding it in something else. And since steganography is a concept, not a specific method of clandestine data delivery, it can be used in all sorts of ingenious (and worrying) attacks.

Steganography is an ancient practice. When spies in the Revolutionary War wrote in invisible ink or when Da Vinci embedded secret meaning in a painting that was steganography. This works in the digital world, too, where a file like an image can be stealthily encoded with information. For example, pixel values, brightness, and filter settings for an image are normally changed to affect the image's aesthetic look. But hackers can also manipulate them based on a secret code with no regard for how the inputs make the image look visually.

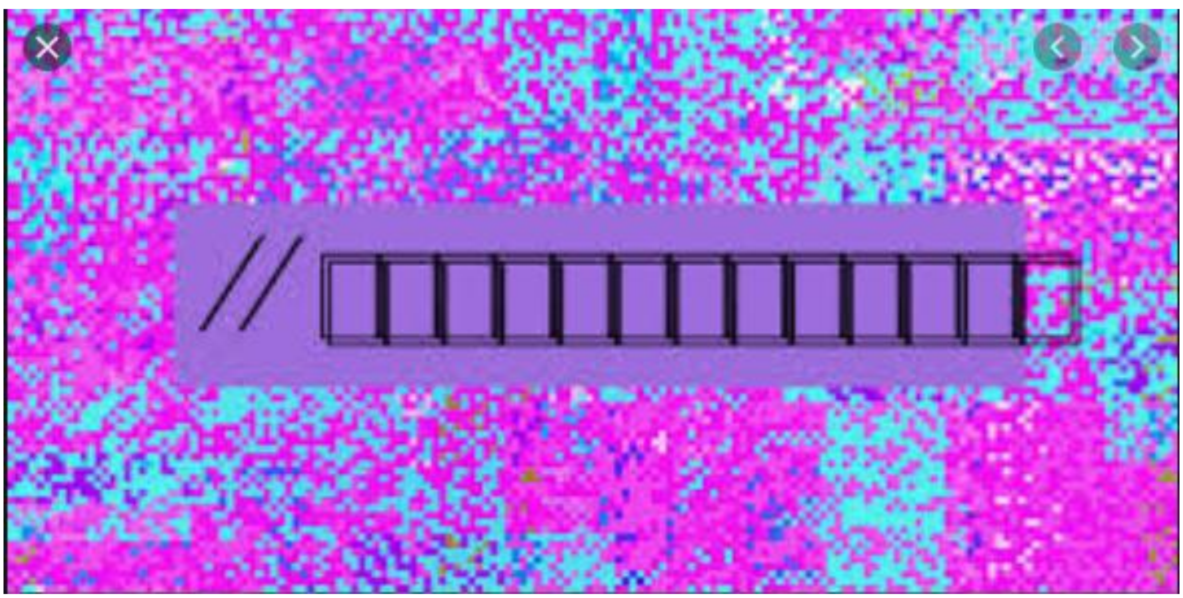
This technique can be used for ethical reasons.

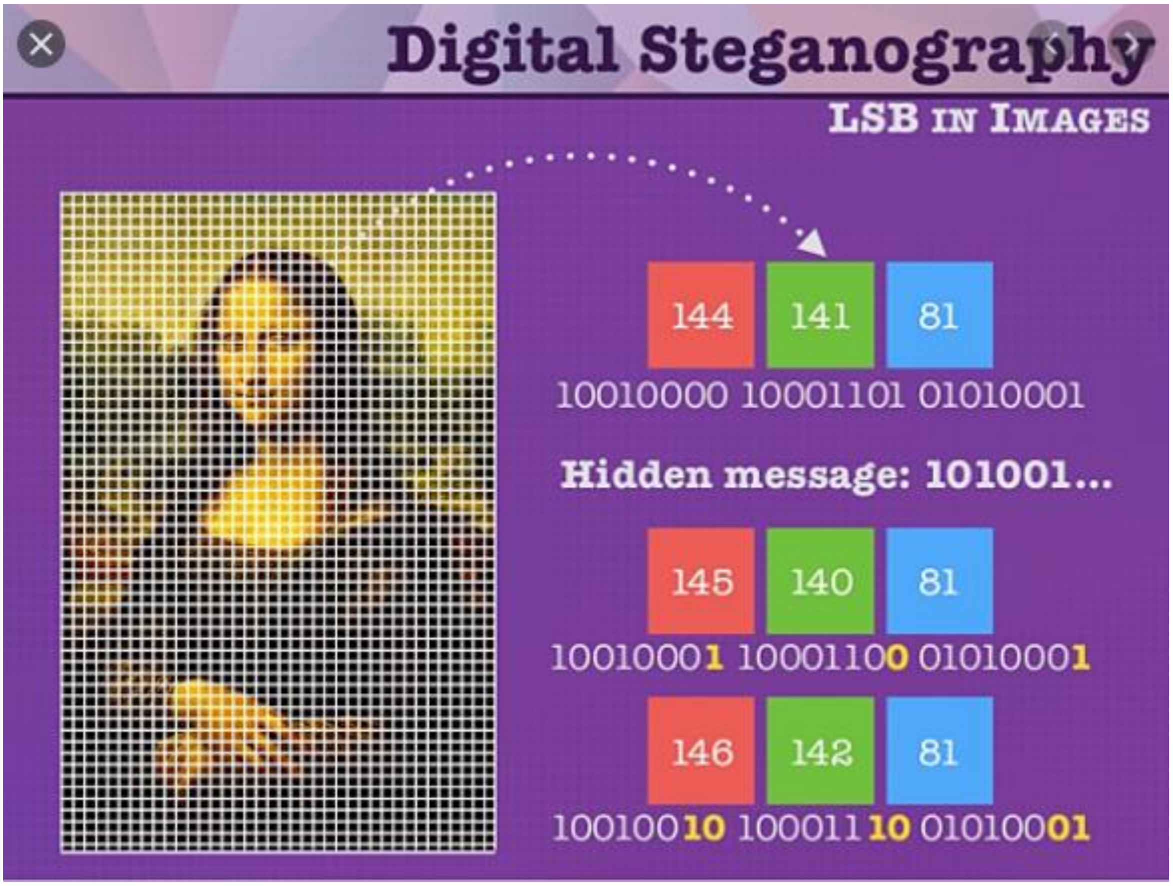
Such as to evade censorship (escape or avoid (someone or something))

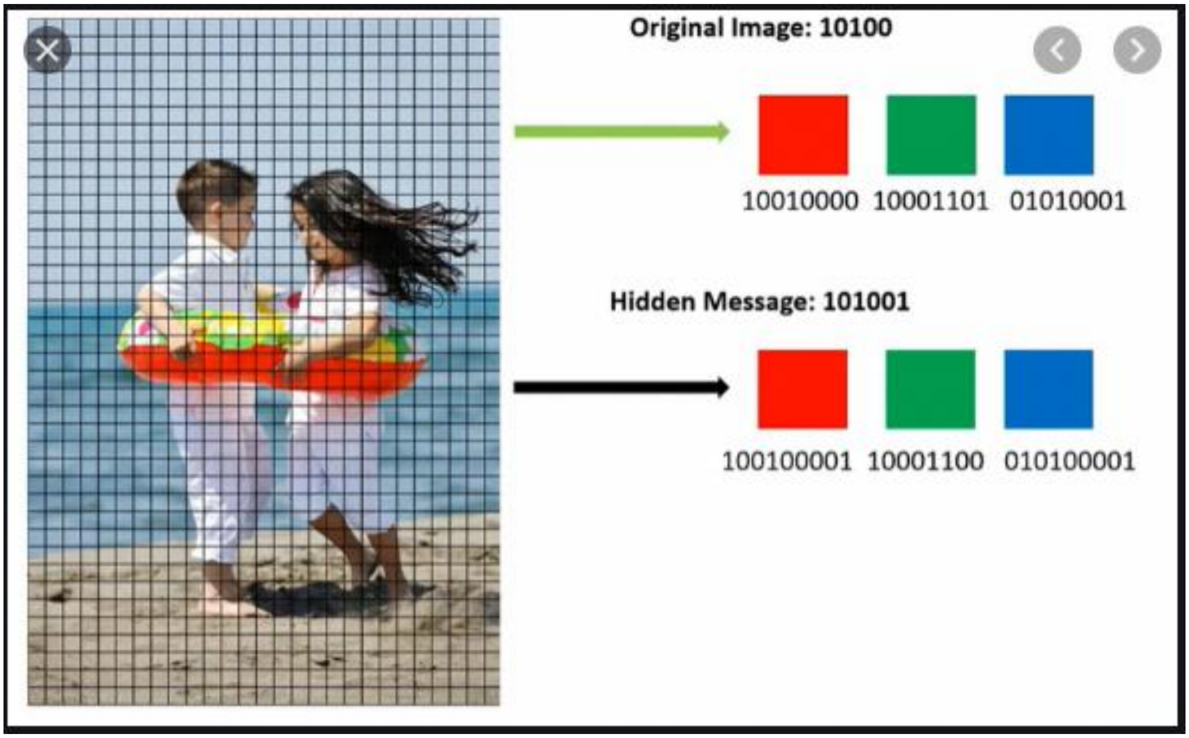
or

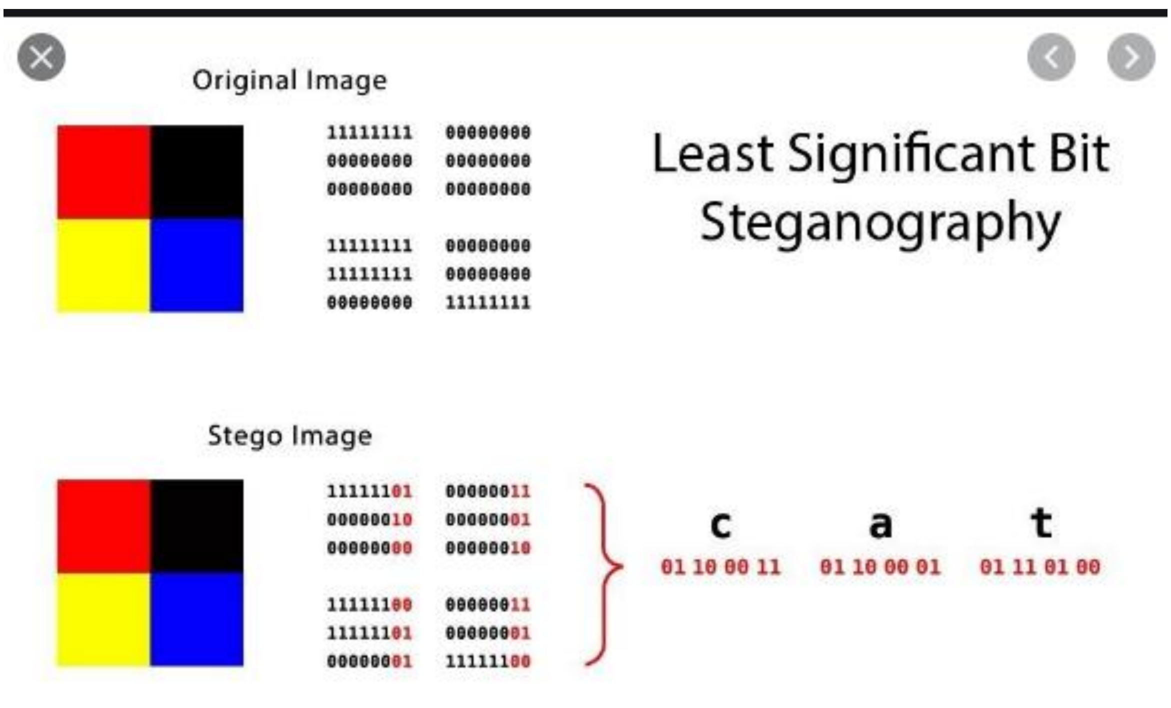
Embed messages in Facebook photos.


//·<STEGANOGRAPHY>


//


Digital Steganography
LSB in Images
144
141
81
10010000 10001101 01010001
Hidden message: 101001...
145
140
81
10010001 10001100 01010001
146
142
81
10010010 10001110 01010001


Original Image: 10100
10010000 10001101 01010001
Hidden Message: 101001
100100001 10001100 010100001


Original Image
11111111 00000000
00000000 00000000
00000000 00000000
11111111 00000000
11111111 00000000
00000000 11111111
Least Significant Bit Steganography
Stego Image
11111101 00000011
00000010 00000001
00000000 00000010
11111100 00000011
11111101 00000001
00000001 11111100
c a t
01 10 00 11 01 10 00 01 01 11 01 00


Original
Steg