Chapter-2
Classical Encryption Techniques

A Symmetric encryption scheme has five ingredients.

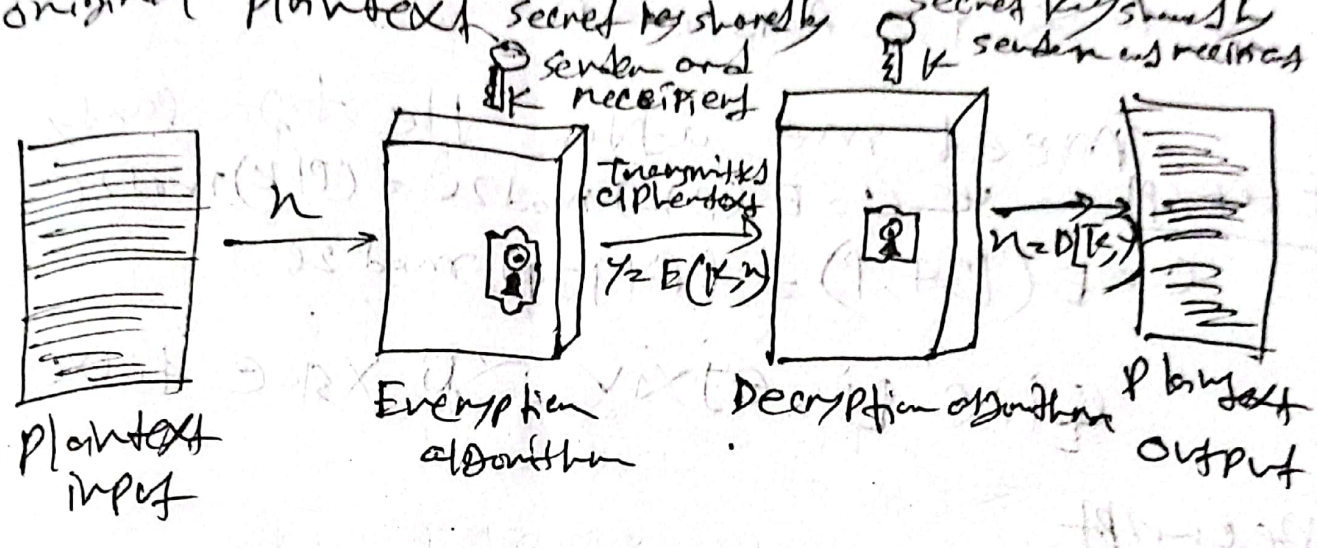
1. **Plaintext**: This is the original message or data that is fed into the algorithm as input.

2. **Encryption algorithm**: The encryption algorithm performs various substitutions and transformations on the plaintext.

3. **Secret key**: The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time.

4. **Ciphertext**: This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts.

2. Decryption algorithm: This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.



3. Cryptoanalysis: Cryptoanalysis attacks based on the nature of the algorithm plus some knowledge of the general characteristics of the plaintext or even some sample plaintext–ciphertext pairs.

Brute-force attack: The attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained. On average, half of all possible keys must be tried to achieve success.

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
A B C D E F G H I J K L M N O P Q
17 18 19 20 21 22 23 24 25
R S T U V W X Y Z
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

meet me after the toga party

Encrypt

$C = E(P, K) = (P + K) \bmod 26$

$C = E(134, P) = (P + 134) \bmod 26$

qjix li ejxiv xli xsqe texc

Decrypt

$P = D(134, C) = (C - 134) \bmod 26$

BUZZI → word key 3

For B

(134+3) mod 26

(1+3) mod 26

4 mod 26

4(E)

Ciphertext EXCC

Decrypt

(E − 3) mod 26

symmetrical — Encrypt/Decrypt same key use.

Playfair cipher

substitution → 1 for character এর অন্য character এ cipher হয়, একে বলে stream.
substitution block হতে পারে,

Playfair: poly alphabetic 1 for plain character হয় এর বিভিন্ন বিভিন্ন cipher use হতে পারে।

Plain text: Monarchy → Key | balloon
ba lx lo on

text → I am improving

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

CO MZ ME

~~[illegible]~~

যেখানে letter থাকবে C row এ O column letter intersect হবে, সেটাই letter হবে.
O হলে O row এ C column এর intersect হবে সে letter হবে

make pair of plain text)

Pair can not be made with same letter

~~Iam im pr ov in gx~~

~~KX MA EA TO [illegible]~~

A সমস্ত pair এর [illegible] ২ [illegible] একই [illegible] or row
এ ২য় [illegible] পরের letter হিসেবে below letter
হবে [illegible] প্রত্যেক নিচের দিক [illegible] rotate
হবে। উদাহরণ [illegible] [illegible] [illegible]

I am improving

Ja mi mp ro ving → right

SB AE OL MN XFYQ this are given

Caesar cipher

1. Letters are replaced by other letters or symbols. The earliest known and simplest method used be julius caesar replacing each letter of the alphabet with the letter standing three places further down the alphabet.

Example

0	1	2	3						25
A	B	C	D						Z

$$C = E(P,K) \bmod 26 = (P+K) \bmod 26$$

Example: BUZZ?

For B $C_2 = (P+K) \bmod 26$

$= (18+3) \bmod 26$

$= 21 \bmod 26$

$= 21$

C_2 E

Playfair: Manual Symmetric encryption technique. The first literal diagram substitution cipher. Invented in 1854 by Charles Wheatstone. Done the name of Lord Playfair for promoting it. Use multiple letter encryption cipher. 5x5 matrix constructed using a keyword.

1. Diagrams
2. Repeating letters - Filler letter
3. Same column ↓ wrap around
4. Same row → wrap around
5. Rectangle ⇄ swap.

~~Monoalphabetic~~.

Hill ciphen

Another multiletter ciphen is the Hill ciphen developed by the mathematician Lester Hill in 1929. It is a Polygraphic substitution ciphen based on linear algebra It can encrypts a group of letters such as digraph, trigraph or Polygraph

This can be expressed as,

$$C = E(K, P) = PK \bmod 26$$

$$P = D(K, C) = CK^{-1} \bmod 26 = PKK^{-1} \bmod$$

$$= PKK^{-1} \bmod 26$$

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

$$C_1 = (P_1 K_{11} + P_2 K_{21} + P_3 K_{23}) \bmod 26$$

$$C_2 = (P_1 K_{12} + P_2 K_{22} + P_3 K_{32}) \bmod 26$$

$$C_3 = (P_1 K_{13} + P_2 K_{23} + P_3 K_{33}) \bmod 26$$

Example: Encrypt "pay more money" using

Key $\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$

Solution:-1

p	a	y	m	o	n	e	m	o	n	e	y
15	0	24	12	14	17	4	12	14	13	4	24

key = 3×3 matrix

Plaintext = Pay mon emo ney

Encrypting: Pay

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

$$= (15\ 0\ 24)\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \bmod 26$$

$$= (15\times17+0\times21+24\times2 \quad 15\times17+0\times18+24\times2 \quad 15\times5+0\times21+24\times19) \bmod 26$$

$$= (303\ \ 303\ \ 531) \bmod 26$$

$$= (17\ \ 17\ \ 11)$$

$$= (R\ R\ L)$$

Encrypting pay

342,594,298

$$(C_1 C_2 C_3) = (12\ 14\ 17)\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \bmod 26$$

$$= (532\ 490\ 677) \bmod 26$$

$$= (12\ 22\ 1)$$

$$= (M\ W\ B)$$

Encrypting emo

$$(C_1 C_2 C_3) = (4\ 12\ 14)\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \bmod 26$$

$$= (348\ 312\ 538) \bmod 26$$

$$= (10\ 0\ 18)$$

$$= (K\ A\ S)$$

Encrypting rey

$$(C_1 C_2 C_3) = (13\ 4\ 24)\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \bmod 26$$

$$= (348\ 312\ 538) \bmod 26$$

$$= (15\ 3\ 7)$$

$$= (P\ D\ H)$$

Plaintext = pay more money

Ciphertext = RRLMWBKASPDH

$$\begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix} = \begin{bmatrix} 126+70 & 177+77 \end{bmatrix}$$

$$= \begin{bmatrix} 203 & 221 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 21 & 13 \end{bmatrix}$$

$$K^{-1} = \frac{1}{|K|} \text{adj}(K)$$

$$\frac{1}{|K|} = d^{-1}$$

$$|K| = 5$$

$$d \times d^{-1} = 1 \bmod 26$$

$$\frac{1}{5} \begin{vmatrix} 12 & 13 \\ & \end{vmatrix}$$

determinant of matrix

$$K^{-1} \quad \frac{15}{2}$$

From question

$$\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 7 \\ 24 & 0 & 17 \end{pmatrix} = \begin{pmatrix} 443 & 442 & 442 \\ 858 & 495 & 780 \\ 494 & 52 & 365 \end{pmatrix} \bmod$$

$$= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Polyalphabetic Ciphers → Vernam (one time Pad) Vigenere.

Vernam Length of the key words = Length of the plaintext.

System works on binary bits rather than letters

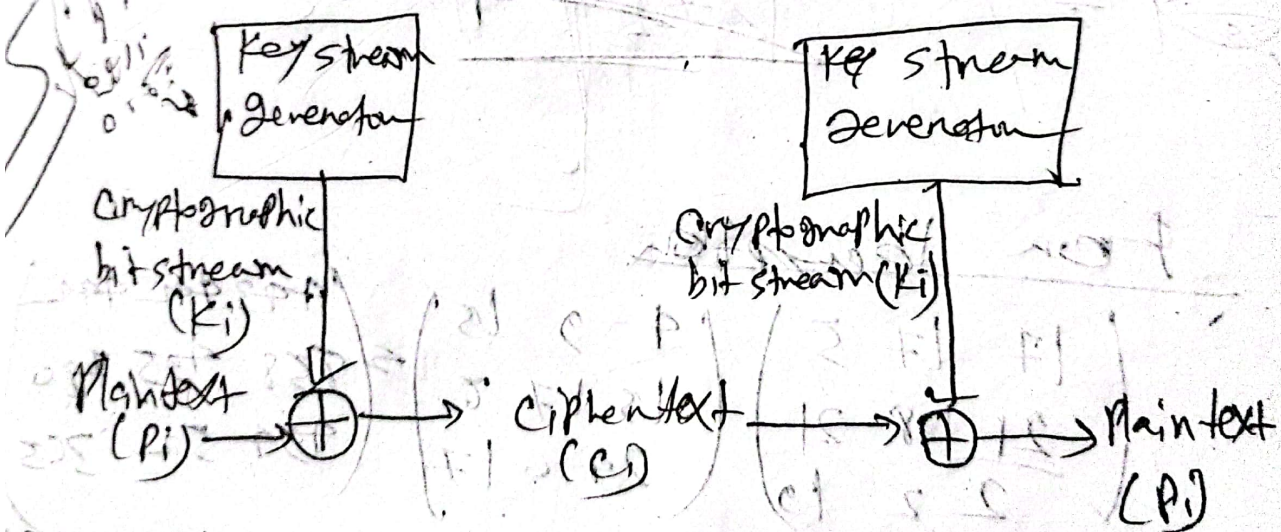
The system expressed as $C_i = P_i \oplus K_i$ → Exor

P_i = i^{th} binary of the plaintext

K_i = i^{th} binary of the ~~key~~ Key.

C_i = i^{th} " " " Ciphertext.

$\oplus$ = XOR operation.



The ciphertext is generated & decrypted by performing the bitwise XOR of the plain text and the key. Because of the properties of the XOR decryption simply

involves the same bitwise operation.

$p_i = c_i \oplus k_i$

Vernam proposed the use of a running loop of tape that eventually repeated the key, so that the system worked with a very long but repeating keyword.

Cryptanalysis of Vernam ciphers

1. construction of the key.

2. The use of a a running loop of tape that eventually repeated the key.

3. The system worked with a very long but repeating keyword.

4. This technique can be broken with sufficient ciphertext, the use of known or probable plaintext sequences or both.

Example. one time pad এ কি use করেনি হবে। just one time pad এ key repeating format হয় না but vernam এ repeating হয় কারণ যখন key প্রত্যেকবার use হয় কিন্তু 'one time pad এ যখন key only একবারই ব্যবহার হয়।

One time pad (vernam) uses XOR over stream

1. Improvement to the vernam cipher
2. It yields the ultimate in security
3. Random key that is as long as the message
4. The key need not be repeated.
5. In addition the key is to be used to encrypt and decrypt a single message, and then is discarded
6. Each new message requires a new key of the same length as the new message
7. Such a scheme, known as a one time pad, is unbreakable.
8. It produces random output
9. No statistical relationship to the plaintext
10. Because the ciphertext contains no information whatever about the plaintext, there is simply no way to break the code
11. The code is unbreakable
12. The security of the one time pad

is entirely due to the randomness of the key

Plaintext H E L L O

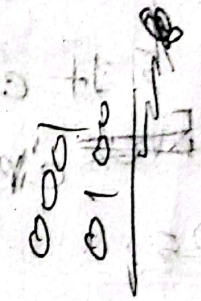
7 4 11 11 14

Key b a r n y

1 0 23 24 2

Add 8 4 34 35 16

Subtract 8 4 8 9 16



ciphertext i e i j q

For Decryption

ciphertext

key

c-k

if (c-k) number goes negative then add 26 with it.

10111
-10111
10000

01101
10000
11101

01100
-1100
0000

Vigenere cipher / Polyalphabetic substitution cipher

1. To improve on the simple monoalphabetic technique.
2. Several names: polyalphabetic substitution cipher
3. A set of related monoalphabetic substitution rules is used
4. A key determines which particular rule is chosen for a given transformation.
5. It consists of the 26 ~~cesse~~ ~~Ceser~~ ciphers with shifts of 0 through 25.

Encryption process:

$$C_i = (P_i + K_{i \bmod m}) \bmod 26$$

Decryption Process:

$$P_i = (C_i - K_{i \bmod m}) \bmod 26$$

Example:

Key: deceptivedeceptivedeceptive

Plaintext: wearediscoveredsaveyourself

Ciphertext: ZICVTWQNGRZGVTWAVZH

(often solid) CQYGLMGJ

PT	22	4	0	17	4	3	8	18	2	14	21	4	17	
key	3	4	2	4	15	19	8	21	4	3	4	2	4	
CT	25	8	2	21	19	22	16	13	6	17	25	6	21	

1. Determining the length of the keyword
2. keyword the plaintext share the same frequency distribution of letters, a statistical technique can be applied

Auto key system,

1. The periodic nature of the keyword can be eliminated by using a non repeating keyword that is as long as the message itself.

2. Vigenere proposed auto key system, in which a keyword is concatenated with plaintext itself to provide a running key

Example: deceptiveweare discoveredsav

Monoalphabetic

1. The ciphen line can be any Permutation of the 26 alphabetic characters

permutation of, S = {a, b, c}

There are six permutations of S = abc, acb, bac, bca, cab, cba.

this would eliminate brute force techniques for cryptanalysis. A single ciphen alphabet (mapping from plain alphabet to ciphen alphabet) is used Per message

Any It was disclosed Yesterday that several illustrated but direct contacts have been made with Political representatives of the viet cong in moscow

Example: CZAE WVGBNCP — plaintext

EXECUTEPLAN — ciphen text

CT	C	Z	A	E	W	V	C	B	N	C	P
PT	E		E				E				
PT	E		E								
PT	E		E			T	E				
PT	E		E			T	E				
PT	E		E			T	E			A	
PT	E	X	E	C	V	T	E	P	L	A	N

>T>A>O>I>N>H>D>

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

A single ciphered alphabet for each plain text alphabet is used throughout the process

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

x	y	z		
O	N	M		

hello → PT
vexxm → CT

PT Attack postponed to tomorrow and do not use our secret paper until further info.

key: The quick brown fox jumps over the lazy dog

CT: THH TEQ VJCHUJKBR HJ HJOJWWJN TKR
RJ KJH FCB IFW CBEWBH UTUBW FKHXJ
XKJJI

Transposition

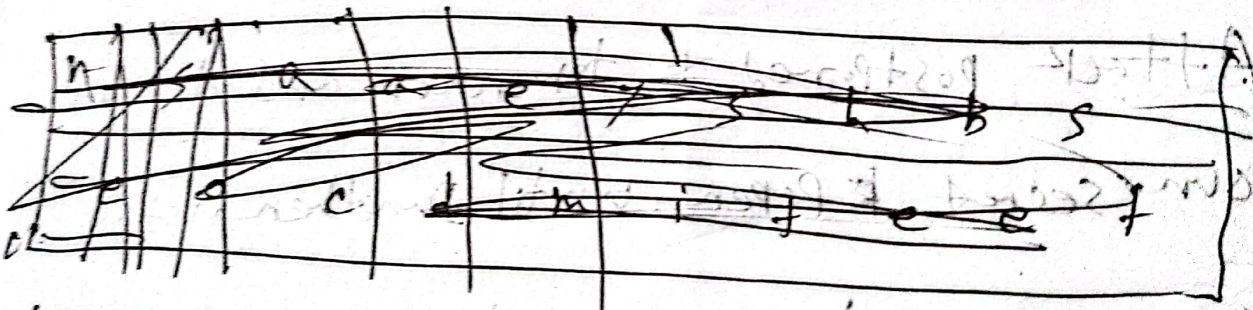
Some sort of permutation applied on the plaintext letters. This technique is referred to as a transposition cipher. The simplest such cipher is the rail fence.

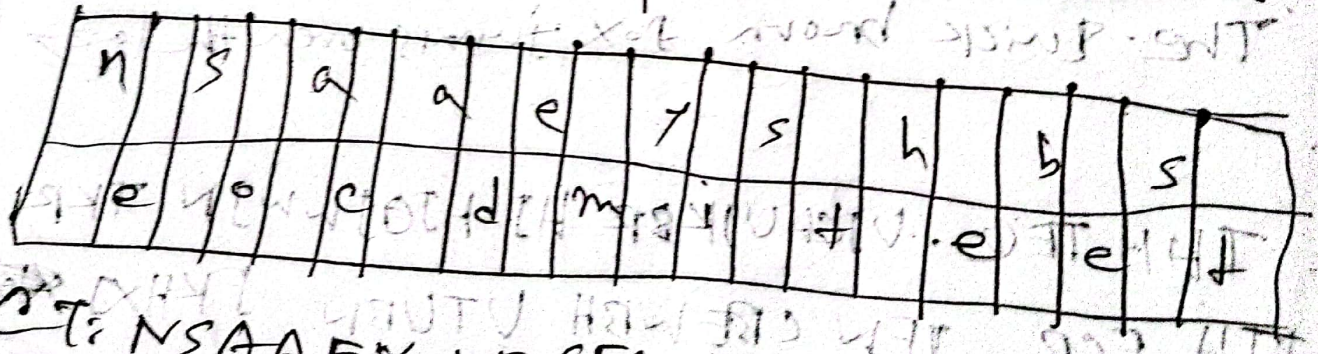
Rail Fence: The plaintext is written down as a sequence of diagonals and then read off as sequence of rows.

Example

Plaintext: meg academy is the best

Depth : 2

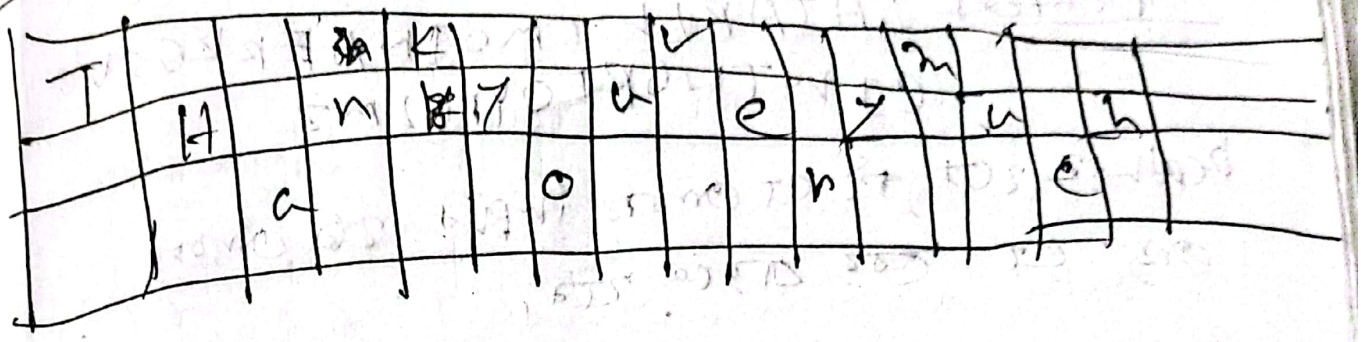




CT: NSAAEYSHBSEO@MJTEET

Thank you very much

Part! 3



Row Columns

1. A more complex scheme
2. The matrix row and column are decided by the sender and receiver
3. Write row by row
4. Read column by column
5. Key: order of the column

Example → Kill corona virus of twelve am to morning

Key: 4312567 (order of the column)

4	3	1	2	5	6	7
K	i	l	l	c	o	r
o	n	a	v	i	r	u
s	a	t	t	w	e	l
v	e	a	n	t	o	n
o	r	n	o	w	7	2

random

Read column by column follow the order of the column which is in the key

Ciphertext LATARLVTHOJNAERKOSVO
CJWTHOREOYRVLMZ

Decrypt the cipher text to original text.

Example of vernam (XOR)

PT = OAK
KY = SON

XOR - same = 0
not same = 1

'A' = 0 = 0000

O(14) = 1110

AXOR O = 1110 (14) = O

Value! O(14) = 1110
S(18) = 1010
O XOR S = 1100 (28)
28 - 26 = 2 (C) = O XOR S

'K' (10) = 1010
N(13) = 1101
K XOR N = 0111 (7) = H

Cryptography is the practice of securing communication by encoding information to make it unreadable to unauthorized users. It involves techniques and algorithms for encrypting data to ensure confidentiality, integrity, and authentication

1. The type of operations used for transforming plaintext to ciphertext. : All encryption algorithms are based on two general principles substitution, in which each element in the plaintext is mapped into another element and transposition, in which elements in the plaintext are rearranged. The fundamental requirement is that no information be lost
2. The number of keys used : If both sender and receiver use the same key, the system is referred to as symmetric, single-key, secret key or conventional encryption. If the sender and receiver use different keys the system is referred to as symmetric, two key or public key encryption

3. The way in which the plaintext is processed. A block cipher processes the input one block of elements at a time, producing an output block for each input block. A stream cipher processes the input elements continuously, producing output one element at a time as it goes along.

Decryption Hill Cipher

$d \times d^{-1} = 1 \bmod 26$

$(d \times d^{-1}) \bmod 26 = 1$

$(3 \times 9) \bmod 26 = 1$

$27 \bmod 26 = 1$

$d^{-1} = 9$

$(b24 \times d^{-1}) \bmod 26 = 0$