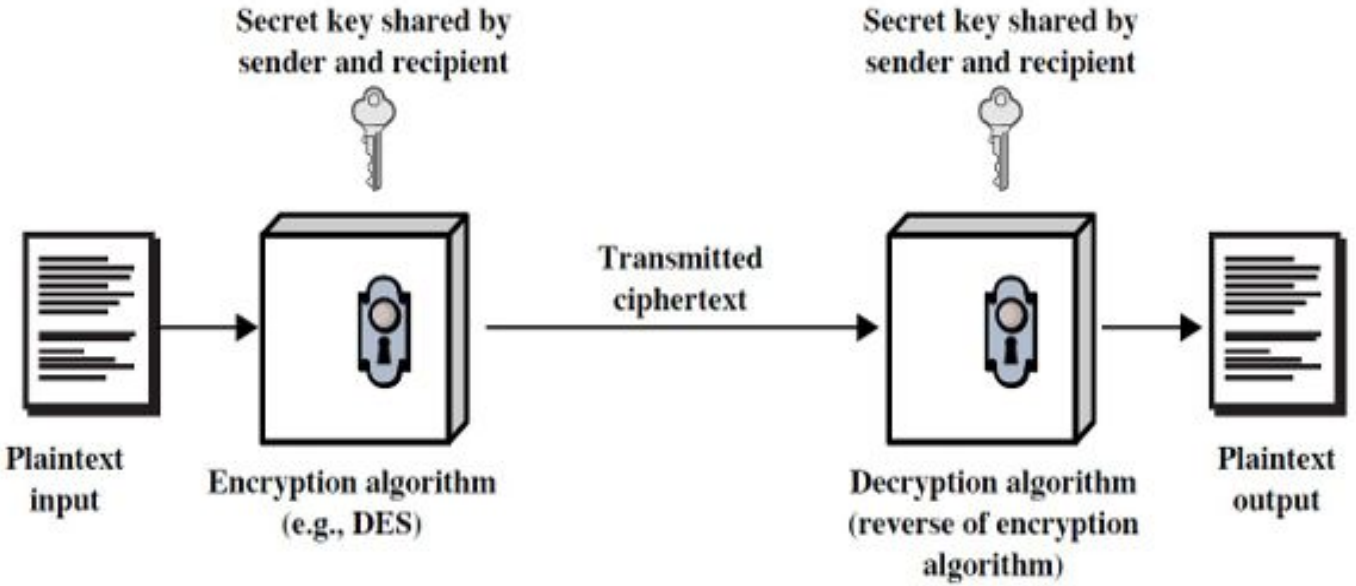
Symmetric Cipher Model



Symmetric Cipher Cont…

- Substitution Techniques:
  - Shift Cipher(Caesar Cipher)
  - Monoalphabetic Ciphers
  - Playfair Cipher
  - Hill Cipher
  - Polyalphabetic Cipher
  - One- Time Pad
- Transposition Techniques
- Steganography

Classical Substitution Ciphers

Where letters of plaintext are replaced by other letters or by numbers or symbols or if plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with cipher text bit patterns

Caesar Cipher

Earliest known substitution cipher.

It was developed by Julius Caesar First attested use in military affairs Replaces each letter by a letter three places down the alphabet

Example:

meet me after the toga party

PHHW PH DIWHU WKH WRJD SDUWB

Caesar Cipher

can define transformation as:

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	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

mathematically give each letter a number

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
0	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

$$E(p) = (p + k) \bmod (26)$$

$$D(C) = (C - k) \bmod (26)$$

Caesar Cipher

Encryption and Decryption : MEET

Encryption k=3 $E(p) = (p + k) \bmod (26)$	Result	Cipher Text $D(C) = (C - k) \bmod (26)$	Result
M=E(M)=(12+3)mod26	15=P	D(P)=(15-3)mod26	12=m
E=E(E)=((4+3)mod26	7=H	D(H)=(7-3)mod26	4=e
E= E(E)=((4+3)mod26	7=H	D(H)=(7-3)mod26	4=e
T=E(T)=((19+3)mod26	21=V	D(V)=(21-3)mod26	19=t

This cipher can be broken

If we know one plaintext-cipher text pair since the difference will be same.

By applying Brute Force attack as there are only 26 possible keys.

Cryptanalysis of Caesar Cipher

Limitations:

- Only have 26 possible keys

  Could shift K = 0, 1, 2, …, 25 slots

- could simply try each in turn
- a brute force search
- given ciphertext, just try all shifts of letters
- do need to recognize when have plaintext
- Test: 1

Cryptanalysis of Caesar Cipher

Try Yourself:-

Convert the plain text “COMMUNICATION” to Cipher text with key = 5.

Monoalphabetic Cipher Security

With only 25 possible keys, the Caesar cipher is far from secure.

- A dramatic increase in the key space can be achieved by allowing an arbitrary substitution.
- Before proceeding, we define the term permutation.
- A permutation of a finite set of elements is an ordered sequence of all the elements of , with each element appearing exactly once.
- For example, if S = {a, b, c} , there are six permutations of : abc, acb, bac, bca, cab, cba
- In general, there are n! permutations of a set of n elements, because the first element can be chosen in one of n ways, the second in n-1 ways, the third in n-2 ways, and so on

Monoalphabetic Cipher Security

- If, instead, the “cipher” line can be any permutation of the 26 alphabetic characters, then there are 26! or greater than possible keys.
- This is 10 orders of magnitude greater than the key space for DES and would seem to eliminate brute-force techniques for cryptanalysis.
- Such an approach is referred to as a monoalphabetic substitution cipher, because a single cipher alphabet (mapping from plain alphabet to cipher alphabet) is used per message

Monoalphabetic Substitution Cipher

Shuffle the letters and map each plaintext letter to a different random ciphertext letter:

Plain letters: abcdefghijklmnopqrstuvwxyz

Cipher letters: DKVQFIBJWPESCXHTMYAUOLRGZN

Plaintext: ifwewishtoreplaceletters

Ciphertext: WIRFRWAJUHYFTSDVFSFUUFYA

- What does a key look like?

Frequency Analysis

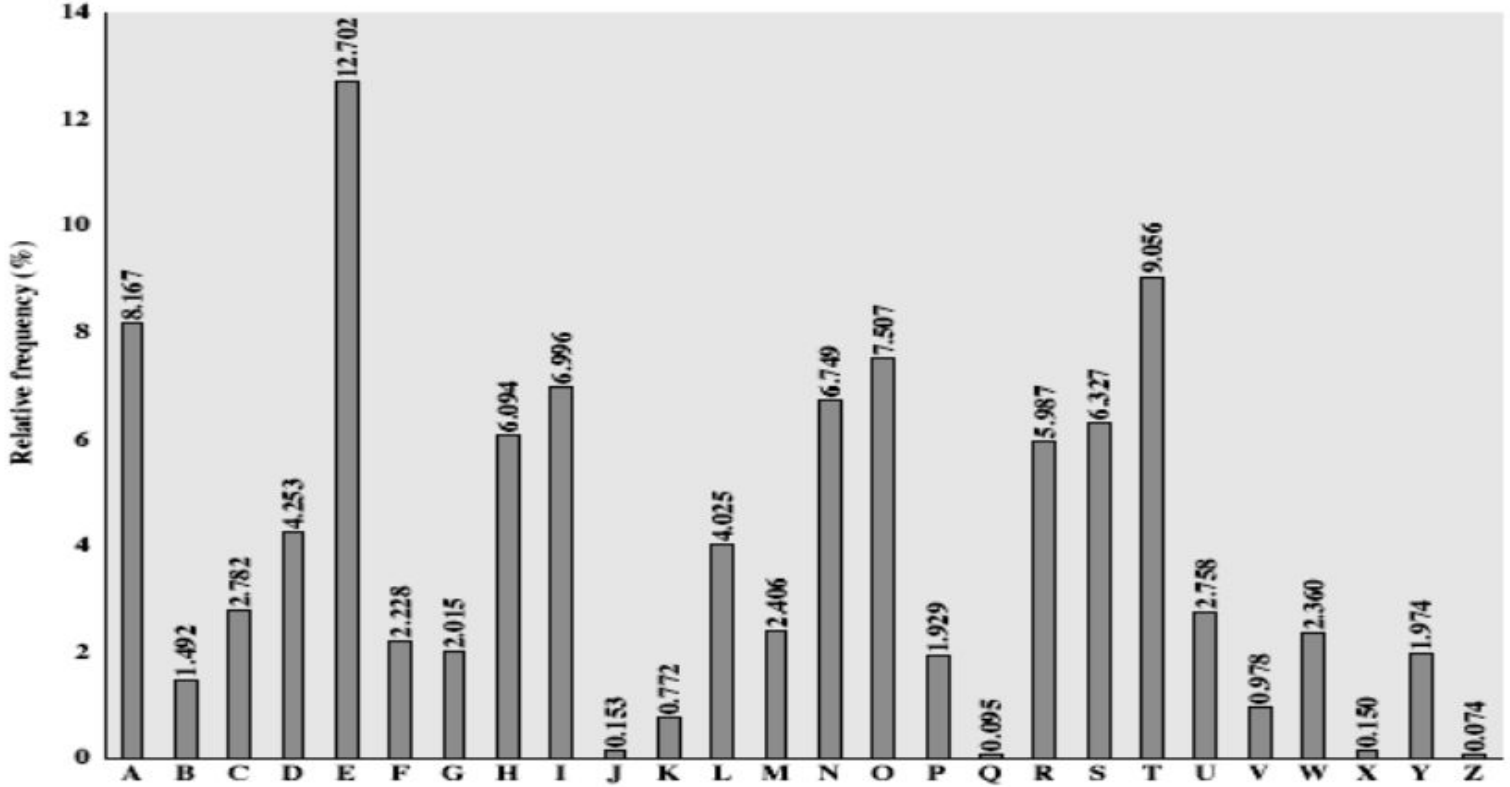
The ciphertext to be solved is
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

As a first step, the relative frequency of the letters can be determined and compared to a standard frequency distribution for English.

• letters are not equally commonly used in English e is by far the most common letter then T,R,N,I,O,A,S .

Other letters are fairly rare cf. Z,J,K,Q,X have tables of single, double & triple letter frequencies

English Letter Frequencies



Example Cryptanalysis

Given ciphertext:

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSX
AIZVUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHS
XEPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

Count relative letter frequencies

Guess P & Z are e and t

Guess ZW is th and hence ZWP is the

Proceeding with trial and error

finally get: it was disclosed yesterday that several informal but direct contacts have been made with political representatives of the viet cong in moscow

Cipher Text

```
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
 t a          e   e te   a that e e a        a
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
   e t    ta t ha e ee   a e   th     t   a
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
 e   e e tat   e    the    t
```

Plain Text

it was disclosed yesterday that several informal but direct contacts have been made with political representatives of the viet cong in moscow

Limitations of Monoalphabetic ciphers

Monoalphabetic ciphers are easy to break because they reflect the frequency data of the original alphabet

A countermeasure is to provide multiple substitutes, known as homophones, for a single letter

Playfair Cipher

The algorithm consists of 2 steps:

1.Generate the key Square (5x5):

- The key square is a 5×5 grid of alphabets that acts as the key for encrypting the plaintext.
- Each of the 25 alphabets must be unique and one letter of the alphabet (usually J) is omitted from the table (as the table can hold only 25 alphabets).
- If the plaintext contains J, then it is replaced by I.

Playfair Cipher Cont…

The initial alphabets in the key square are the unique alphabets of the key in the order in which they appear followed by the remaining letters of the alphabet in order.

2.Algorithm to encrypt the plain text:

The plaintext is split into pairs of two letters (digraphs).

If there is an odd number of letters, a Z is added to the last letter.

Playfair Cipher Cont…

PlainText: "**instruments**"

After Split: 'in' 'st' 'ru' 'me' 'nt' 'sz'

Explanation:

- Pair cannot be made with same letter.
- Break the letter in single and add a bogus letter to the previous letter.
- Here 'z' is the bogus letter

Playfair cipher cont…

Plain Text: "hello"

• After Split: 'he' 'lx' 'lo'

Explanation: Here 'x' is the bogus letter.

• Plain Text: "helloe"

• After Split: 'he' 'lx' 'lo' 'ez'

Explanation:

If the letter is standing alone in the process of pairing, then add an extra bogus letter with the alone letter.

- Here 'x' and 'z' are the bogus letters

Playfair Cipher-Encryption Rules

Generate the key Square (5x5):

Keyword :Monarchy

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

Playfair Cipher-Encryption Rules

If both the letters are in the same column:

Take the letter below each one (going back to the top if at the bottom).

For example:

Diagraph: "me"

Encrypted Text: cl

Encryption: m -> c e -> l

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

Playfair Cipher-Encryption Rules

If both the letters are in the same row:

Take the letter to the right of each one (going back to the leftmost if at the rightmost position).

For example:

Diagraph: "st"

Encrypted Text: tl

Encryption: s -> t t -> l

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

Playfair Cipher-Encryption Rules

If neither of the above rules is true:

Form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.

For example:

Diagraph: "nt"

Encrypted Text: rq

Encryption: n -> r t -> q

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

Playfair Cipher-Encryption Rules

For example:

i -> g

r -> m

u -> z

m -> c

e -> l

n -> r

t -> q

s -> t

z -> x

n -> a

s -> t

t -> l

Playfair Cipher-Encryption Rules

Try Yourself:

Plain Text: "instruments”

Keyword: monarchy

Playfair Cipher-Decryption Rules

Step 1: Generate the 5x5 Key Square

1. Input the keyword (e.g., MONARCHY).
2. Remove duplicates from the keyword.
3. Replace ‘J’ with ‘I’ in both keyword and ciphertext.
4. Fill the grid with unique letters from the keyword, left to right, top to bottom.
5. Fill remaining letters (A–Z excluding J) not already in the key

Playfair Cipher-Decryption Rules

Step 2: Prepare the Ciphertext

1. Split ciphertext into digraphs (two-letter pairs).

2. If a pair is a double letter (e.g., LL), insert a filler like X between them

Step 3: Decrypt Each Digraph

For each digraph (e.g., GAT L MZ):

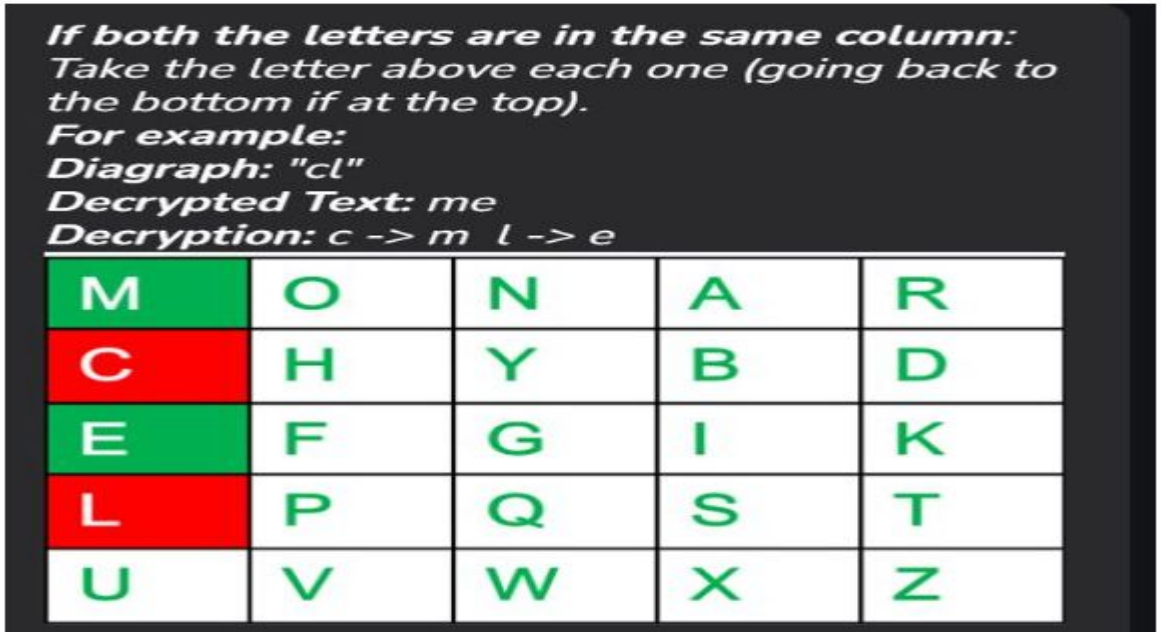
Same Row: Replace each letter with the letter to its left (wrap around if needed).

Same Column: Replace each letter with the letter above it (wrap around if needed).

Rectangle Rule: Replace each letter with the letter in the same row but in the column of the other letter

Playfair Cipher-Decryption Rules

- Combine All Digraphs
- Reassemble the plaintext from all decrypted digraphs.
- Optionally remove filler letters (X or Z) if used



Playfair Cipher-Decryption

Try Yourself:

Key Text: HISTORY

Cipher: BKTJAVGXCFRV

Plain Text : ?

Polyalphabetic Substitution Cipher

- A sequence of monoalphabetic ciphers (M1 , M2 , M3 , ..., Mk) is used in turn to encrypt letters.
- A key determines which sequence of ciphers to use.
- Each plaintext letter has multiple corresponding ciphertext letters.
- This makes cryptanalysis harder since the letter frequency distribution will be flatter.

Hill Cipher

- The algo takes n x n matrix.
- The cipher C of P derived by multiplying P by K.
- When decrypt the message the inverse of K is used.
- C=(KP) mod (26)
- P= K-1 C mod (26)

Hill Cipher-Encryption Algorithm

Steps: 1. Plaintext Preprocessing:

1. Convert each letter of the plaintext to its corresponding numerical value using A=0,B=1,…,Z=25A = 0, B = 1, \ldots, Z = 25A=0, B=1,…,Z=25.

2. If the plaintext length is not a multiple of nnn, pad it with a filler character (e.g., 'X').

2. Form plaintext Vectors:

Divide the numeric plaintext into column vector Pi of length n.

3.Matrix Multiplication:

- For each plaintext vector Pi, compute:
- Ci = K Pi mod 26
- Where Ci is the encrypted ciphertext vector corresponding to Pi.

4. Convert to cipher text

- Convert the resulting numeric values of each ci back to letter using the inverse mapping 0 = A ,1 =B, 2 =C ..25 = Z.
- Concatenate the cipher text vectors to form the final encrypted message.

Decryption Algorithm

Inputs:

Ciphertext message divides into block of size n.

Key matrix K and its inverse K^-1 mod 26

Steps:

1.Ciphertext preprocessing:

Convert ciphertext letters to numerical equivalents.

2.Form Ciphertext Vectors.

Divide the numeric ciphertext column vector Ci of length n.

3. Matrix Multiplication with inverse:

For each ciphertext vector Ci, compute:

Pi =k^-1 ci mod 26

Where Pi is the decrypted plaintext vector.

4.Convert to Plaintext:

- Map each numeric value in Pi back to its alphabetic characters
- Concatenate the plaintext vector to retrieve the original message(excluding any padding).

Input:

Plaintext : **ACT**

Key : **GYBNQKURP**

Step 1: Key Matrix Generation

The key `GYBNQKURP` is 9 letters long, so we form a **3x3 matrix**:

We assign numbers to each letter using A=0, B=1, ..., Z=25:

Letter	**G**	**Y**	**B**
Value	6	24	1
Letter	**N**	**Q**	**K**
Value	13	16	10
Letter	**U**	**R**	**P**
Value	20	17	15

So the Key Matrix (K) is:

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

Step 2: Plaintext Vector Formation

Plaintext is `ACT`. Convert to numbers:

- A = 0
- C = 2
- T = 19

So the **Plaintext Vector (P)** is:

$$P = \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix}$$

Step 3: Matrix Multiplication

Multiply the Key Matrix `K` with the Plaintext Vector `P`:

$$C = K \cdot P \mod 26$$

$$C = \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} \mod 26$$

Perform multiplication:

- Row 1: $6 \times 0 + 24 \times 2 + 1 \times 19 = 0 + 48 + 19 = 67$
- Row 2: $13 \times 0 + 16 \times 2 + 10 \times 19 = 0 + 32 + 190 = 222$
- Row 3: $20 \times 0 + 17 \times 2 + 15 \times 19 = 0 + 34 + 285 = 319$

Now apply mod 26:

- $67 \mod 26 = 15$
- $222 \mod 26 = 14$
- $319 \mod 26 = 7$

So, the **Cipher Vector (C)** is:

$$C = \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix}$$

Step 4: Convert Numbers to Letters

- 15 → P
- 14 → O
- 7 → H

Final Output:

Ciphertext = `POH`

Try Yourself

Plaintext: PAY

Key String: HILLMAGIC

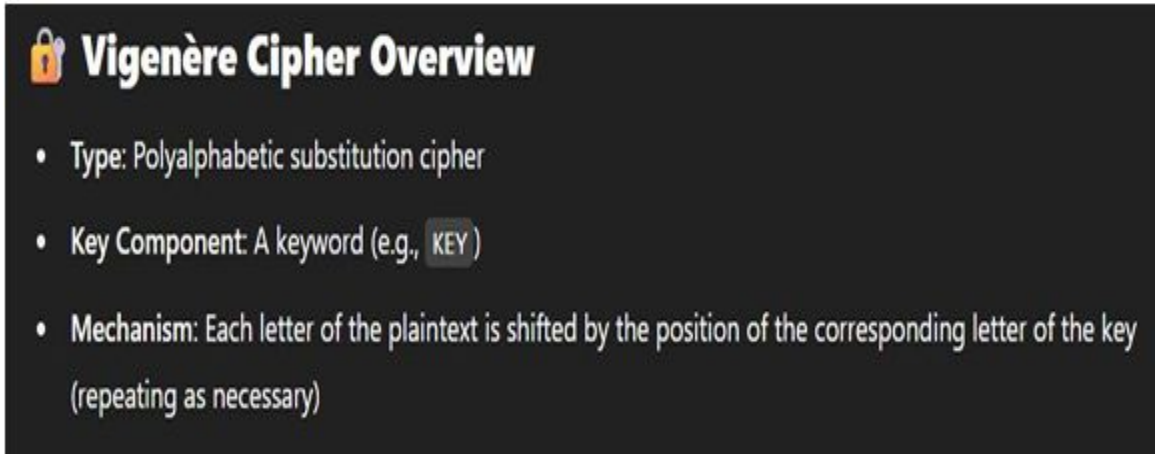
Cipher Text:????

FJI

Vigenère Cipher

- Simplest polyalphabetic substitution cipher
- Consider the set of all Caesar ciphers:

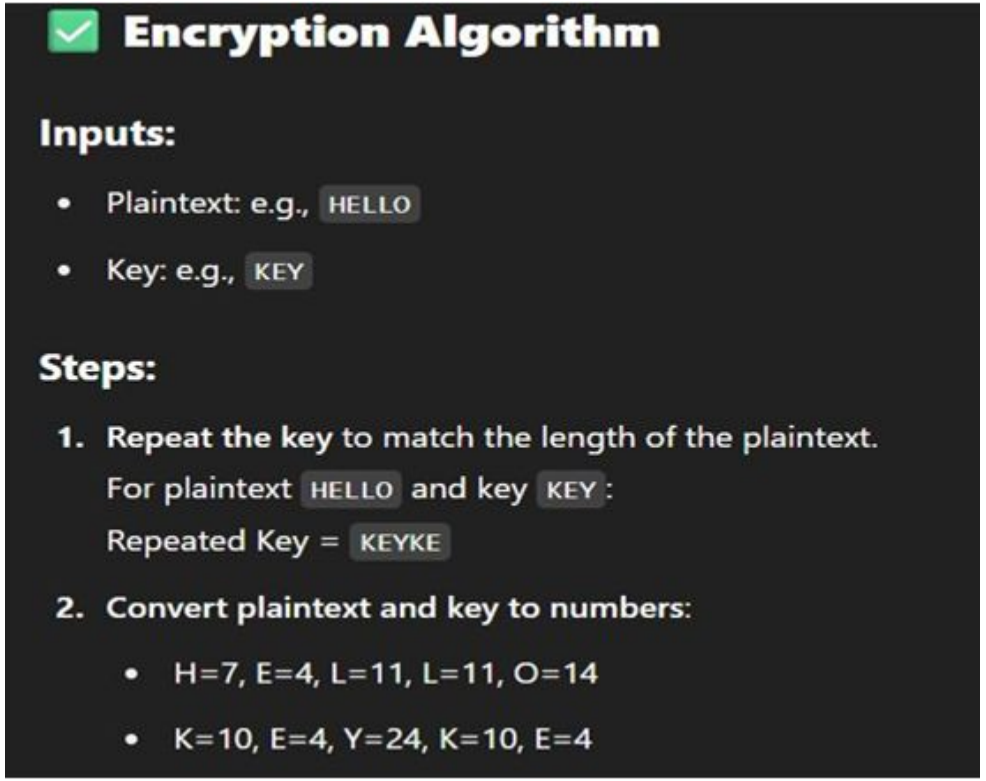
{ Ca , Cb , Cc , ..., Cz }



Example of Vigenère Cipher

Alphabet Mapping
Use a simple

A=0, B=1, ...,
Z=25 mapping.



Example of Vigenère Cipher

3. **Apply encryption formula:**

$$C_i = (P_i + K_i) \mod 26$$

So:

- (7 + 10) % 26 = 17 → R
- (4 + 4) % 26 = 8 → I
- (11 + 24) % 26 = 9 → J
- (11 + 10) % 26 = 21 → V
- (14 + 4) % 26 = 18 → S

4. **Ciphertext:** `RIJVS`

Vernam Cipher

This system works on binary data (bits) rather than letters.

The technique can be expressed as follows:

$$C_i = P_i \oplus K_i$$

Where P_i = ith binary digit of plaintext.

- K_i = i th binary digit of key.
- C_i = i th binary digit of ciphertext.
- $\oplus$ = exclusive-or (XOR) operation

Thus, the ciphertext is generated by performing the bitwise XOR of the plaintext and the key.

Vernam Cipher

- Decryption simply involves the same bitwise operation:
  - $P\mathbf{i} = C\mathbf{i} \oplus K\mathbf{i}$
- The essence of this technique is the means of construction of the key.
- It was produced by the use of a running loop of tape that eventually repeated the key, so that in fact the system worked with a very long but repeating keyword.
- Although such a scheme has cryptanalytic difficulties, but it can be broken with a very long ciphertext or known plaintext as the key is repeated.

Vernam Cipher- Encryption

Example: 1

Plain-Text: O A K

Key: S O N

O ==> 14 = 0 1 1 1 0

S ==> 18 = 1 0 0 1 0

Bitwise XOR Result: 1 1 1 0 0 = 28

Since the resulting number is greater than 26, subtract 26 from it. Then convert the Cipher-Text character number to the Cipher-Text character.

28 - 26 = 2 ==> C

CIPHER-TEXT: C

One- Time Pad

- Similar to Vigenere, but use random key as long as plaintext
- Only known scheme that is unbreakable (unconditional security)
  - Ciphertext has no statistical relationship with plaintext
  - Given two potential plaintext messages, attacker cannot identify the correct message
- Two practical limitations:
  - 1. Difficult to provide large number of random keys
  - 2. Distributing unique long random keys is difficult
- Limited practical use

One-Time pad-Example

Attacker knows the ciphertext:

ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS

Attacker tries all possible keys.

Two examples:

key1: pxlmvmsydofuyrvzwc tnlebnecvgdupahfzzlmnyih

plaintext1: mr mustard with the candlestick in the hall

key2: mfugpmiydgaxgoufhkllmhsqdqogtewbqfgyovuhwt

plaintext2: miss scarlet with the knife in the library

There are many other legible plaintexts obtained with other keys. No way for attacker to know the correct plaintext