SNS COLLEGE OF TECHNOLOGY

Coimbatore-35
An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with ‘A+’ Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF INFORMATION TECHNOLOGY

19ITB302-Cryptography and Network Security

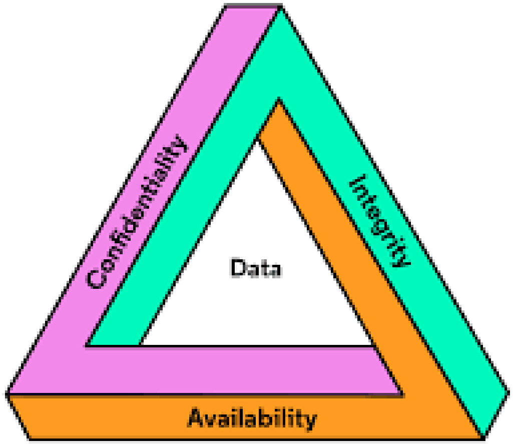
UNIT-1 INTRODUCTION TO ENCRYPTION STANDARD

Computer Security Concepts

Cryptography-”crypt” means hidden “graphy” means writing

CIA Triad

- Three Key principles which should be guaranteed in any kind of secure systems



Confidentiality

Confidentiality is defined as the process of protecting sensitive information from unauthorized access by converting it into an unreadable form. This process ensures that only authorized persons can decrypt and read the information.

Integrity

Integrity refers to the assurance that information is trustworthy and accurate. It ensures that the data remains unchanged from its original form during transmission or storage.

Availability

Ensuring timely and reliable access to and use of information. This means that information should be available whenever it is required by an authorized user or system.

The OSI Security Architecture

Security attack: Any action that compromises the security of information owned by an organization.

Security mechanism: A process that is designed to detect, prevent, or recover from a security attack.

Security service: Security services refer to the different services available for maintaining the security and safety of an organization.

Security Attacks

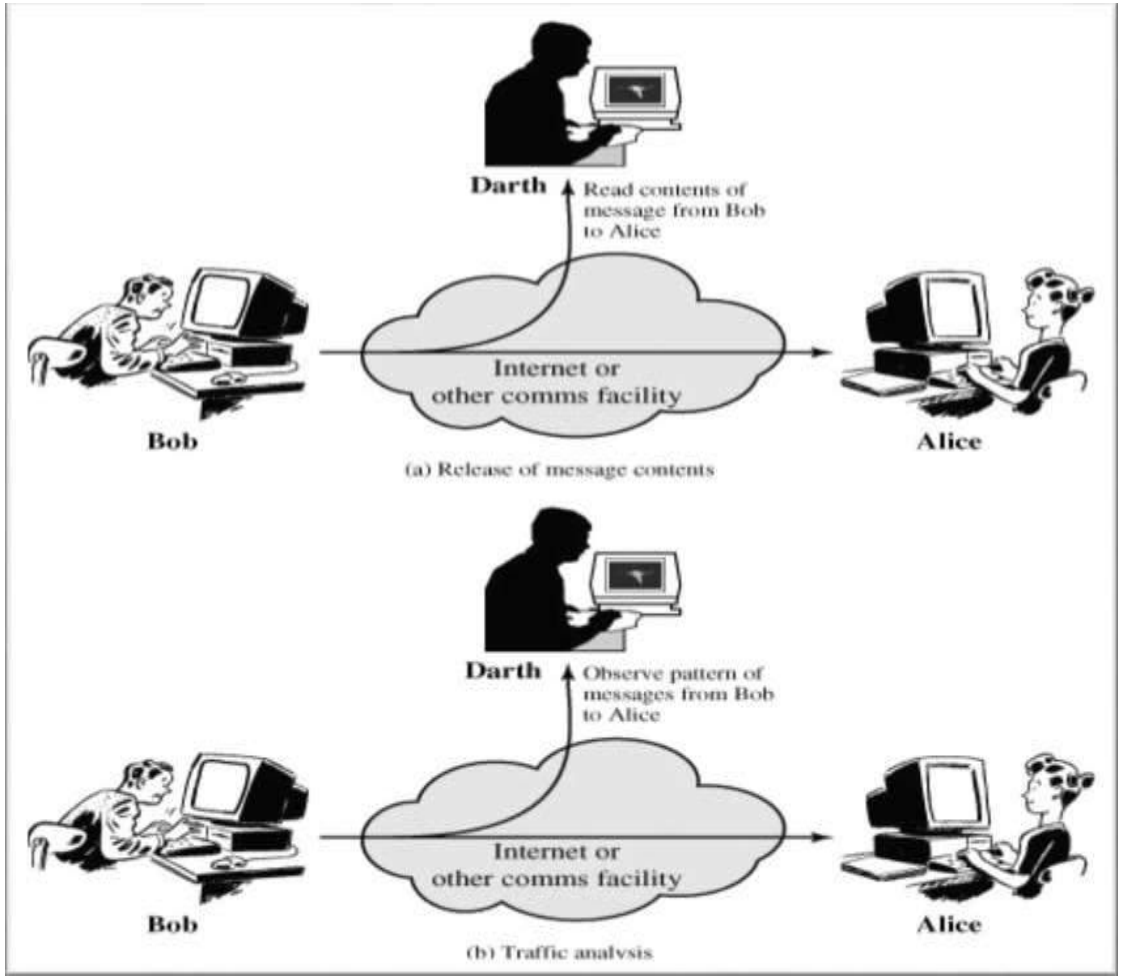
- Passive Attacks
- Active Attacks

Passive Attacks

Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted.

- Release of message contents
- Traffic analysis

Passive Attacks

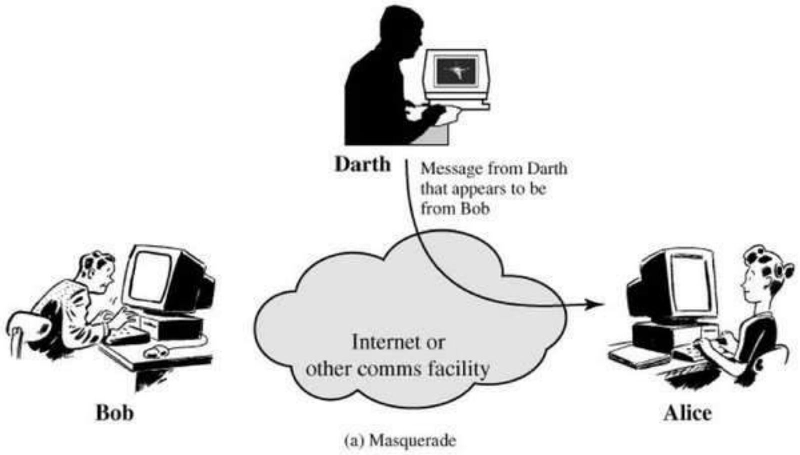

Darth
Read contents of message from Bob to Alice
Bob
Internet or other comms facility
Alice
(a) Release of message contents
Darth
Observe pattern of messages from Bob to Alice
Bob
Internet or other comms facility
Alice
(b) Traffic analysis

Active Attacks

Active attacks involve some modification of the data stream or the creation of a false stream

- **Masquerade**
- **Replay**
- **Modification of Message**
- **Denial of service** (DoS)

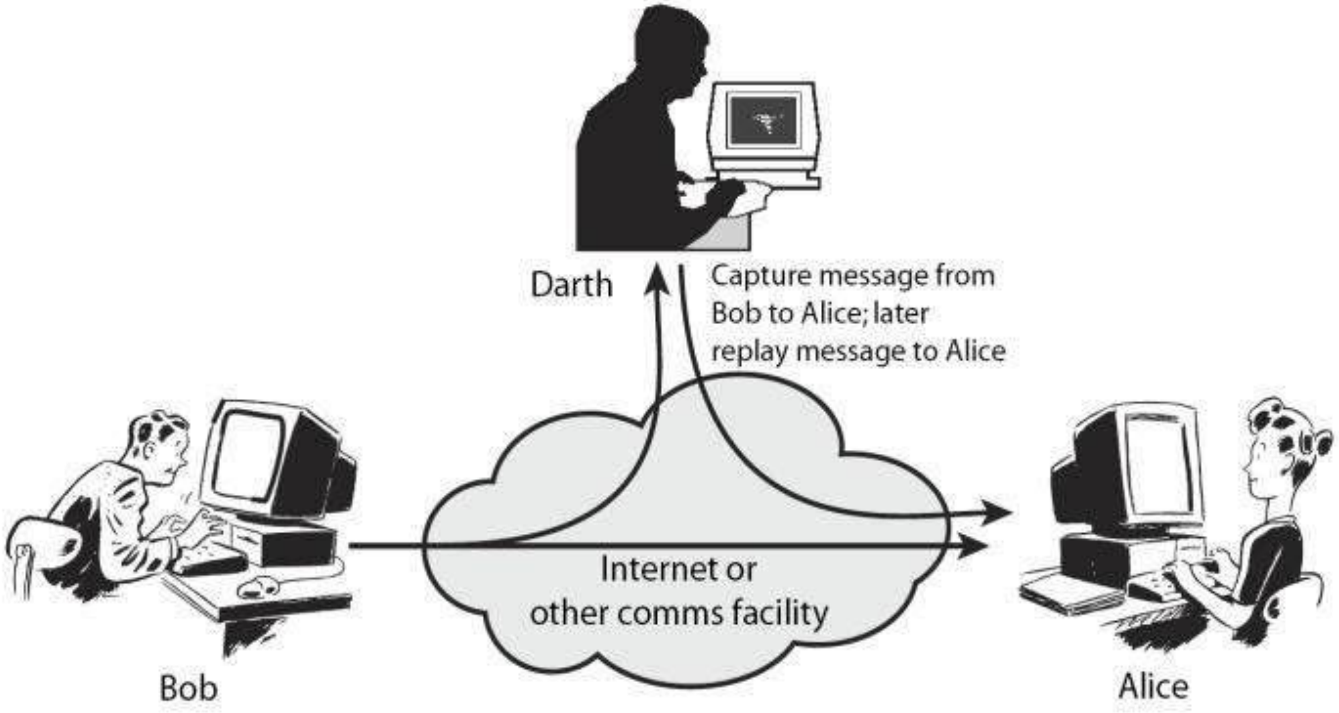
Masquerade


Darth
Message from Darth that appears to be from Bob
Internet or other comms facility
Bob
Alice

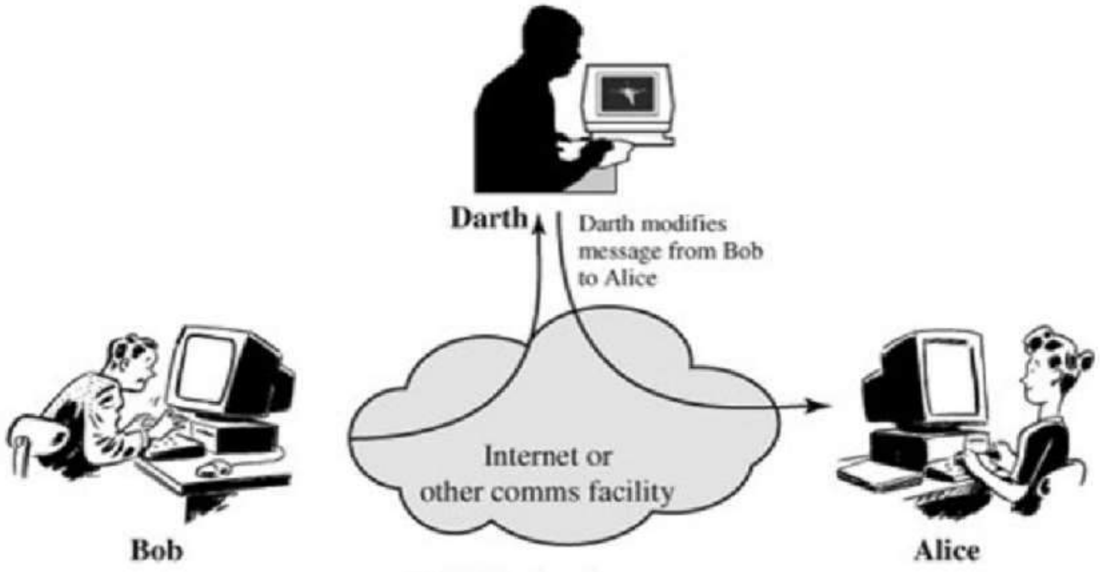
(a) Masquerade

Active Attack – Masquerade

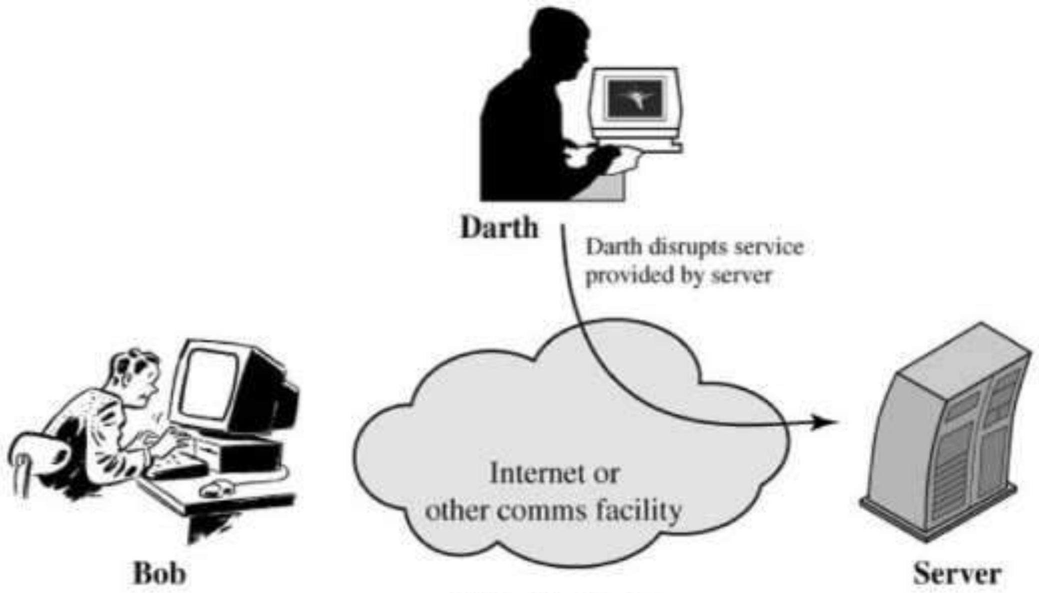
Replay


Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

Modification of message


Darth
Darth modifies message from Bob to Alice
Internet or other comms facility
Bob
Alice

Denial of Service(Dos)



Darth disrupts service provided by server

(d) Denial of service

Active Attack –Denial of Service (DoS)

Security Services

Security services refer to the different services available for maintaining the security and safety of an organization.

- **Authentication** is the process of verifying the identity of a user or device in order to grant or deny access to a system or device.
- **Access control** involves the use of policies and procedures to determine who is allowed to access specific resources within a system.
- **Data Confidentiality** is responsible for the protection of information from being accessed or disclosed to unauthorized parties.

- **Data integrity** is a security mechanism that involves the use of techniques to ensure that data has not been tampered with or altered in any way during transmission or storage.
- **Non- repudiation** involves the use of techniques to create a verifiable record of the origin and transmission of a message, which can be used to prevent the sender from denying that they sent the message. protection against denial by one of the parties in a communication

Security Mechanisms

Encipherment (Encryption) The use of mathematical algorithms to transform data into a form that is not readily intelligible.

Digital signature is a security mechanism that involves the use of cryptographic techniques to create a unique, verifiable identifier for a digital document or message, which can be used to ensure the authenticity and integrity of the document or message.

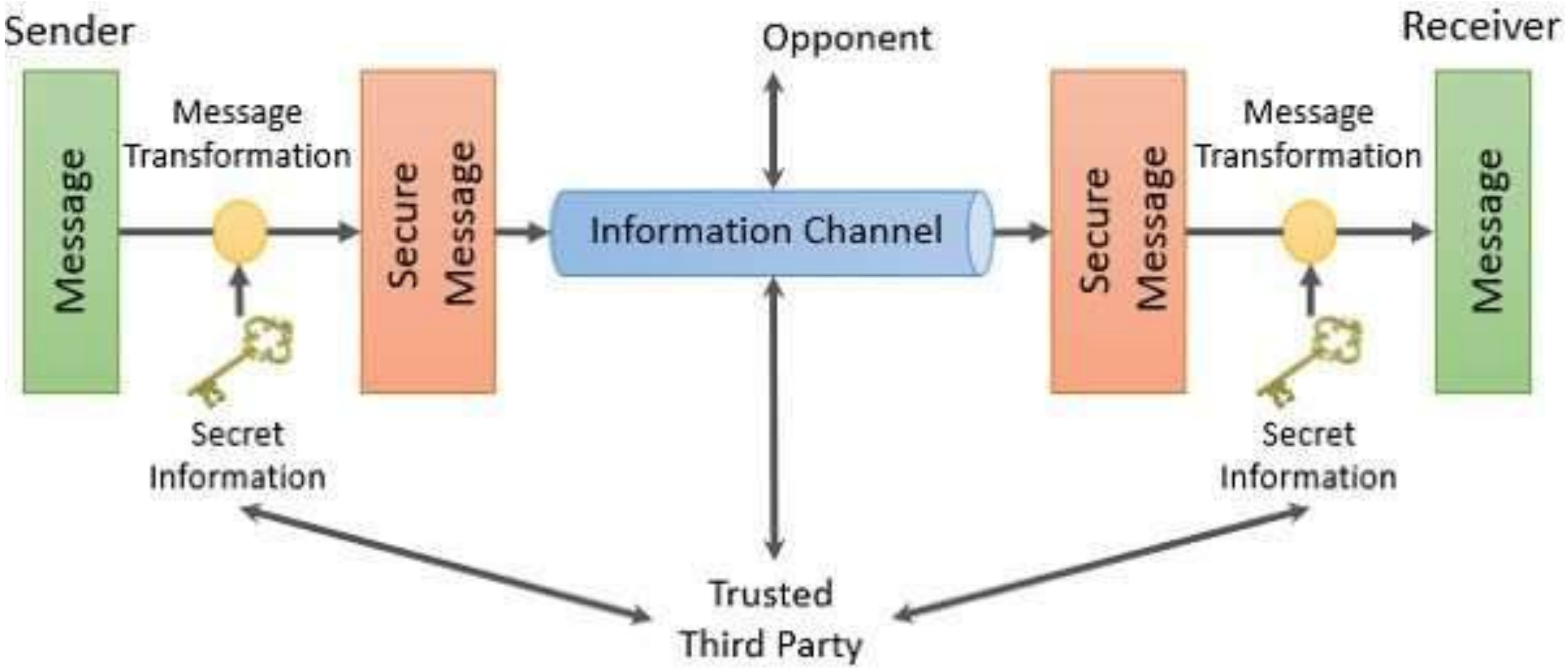
Traffic padding is a technique used to add extra data to a network traffic stream in an attempt to obscure the true content of the traffic and make it more difficult to analyze.

Routing control allows the selection of specific physically secure routes for specific data transmission and enables routing changes, particularly when a gap in security is suspected.

Basic Concepts

- ***Plaintext*** The original intelligible message
- **Ciphertext -** the coded message
- **Cipher -** algorithm for transforming plaintext to ciphertext
- **Key -** info used in cipher known only to sender/receiver
- **Encipher (encrypt) -** converting plaintext to ciphertext
- **Decipher (decrypt) -** recovering ciphertext from plaintext

Network Security model



Network Security Model

Symmetric Cipher Model

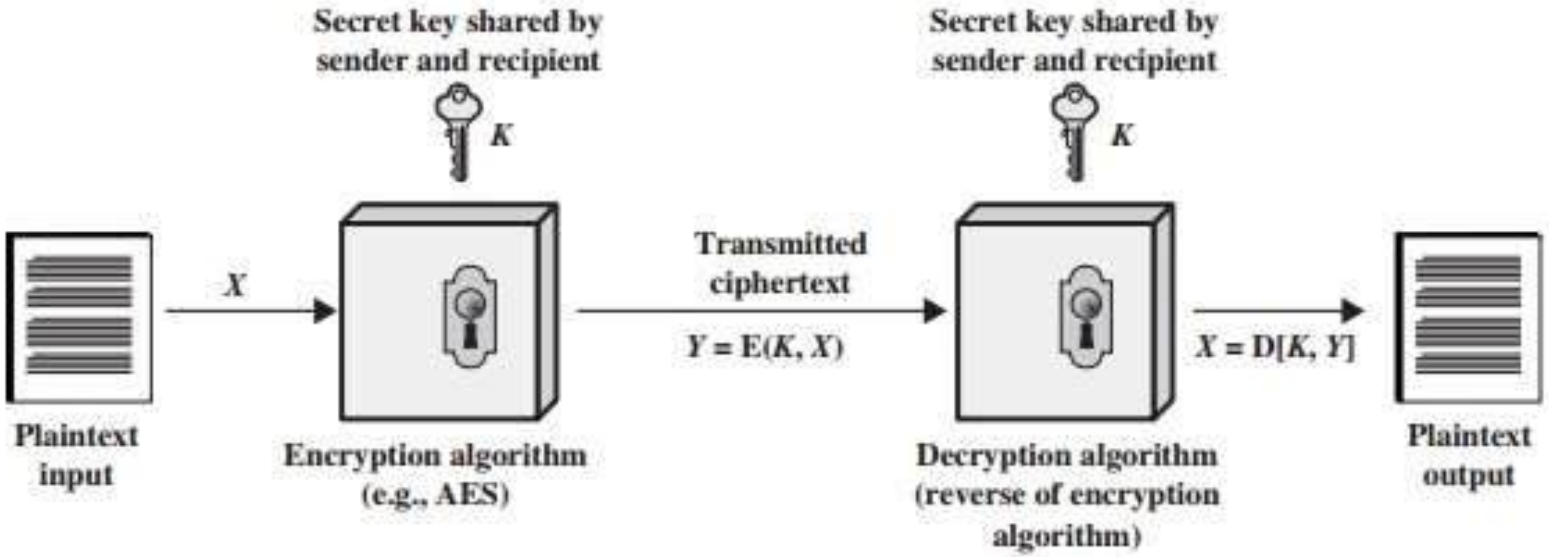

Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
Y = E(K, X)
X = D[K, Y]
Plaintext input
Encryption algorithm (e.g., AES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Figure 2.1 Simplified Model of Symmetric Encryption

Cryptography

Cryptographic systems are characterized along three independent dimensions:

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.

***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 encryp-tion. If the sender and receiver use different keys, the system is referred to as **asymmetric**, 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.

Types of Attacks

Cryptanalysis:

- This type of attack exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used.

Brute-force attack:

The attacker tries every possible key on a piece of cipher-text until an intelligible translation into plaintext is obtained

SUBSTITUTION TECHNIQUES

- A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols.

Caesar Cipher

- The earliest known, and the simplest, use of a substitution cipher was by Julius Caesar. The Caesar cipher involves replacing each letter of the alphabet with the letter standing **three places** further down the alphabet.

e.g.,

plain text *: pay more money*

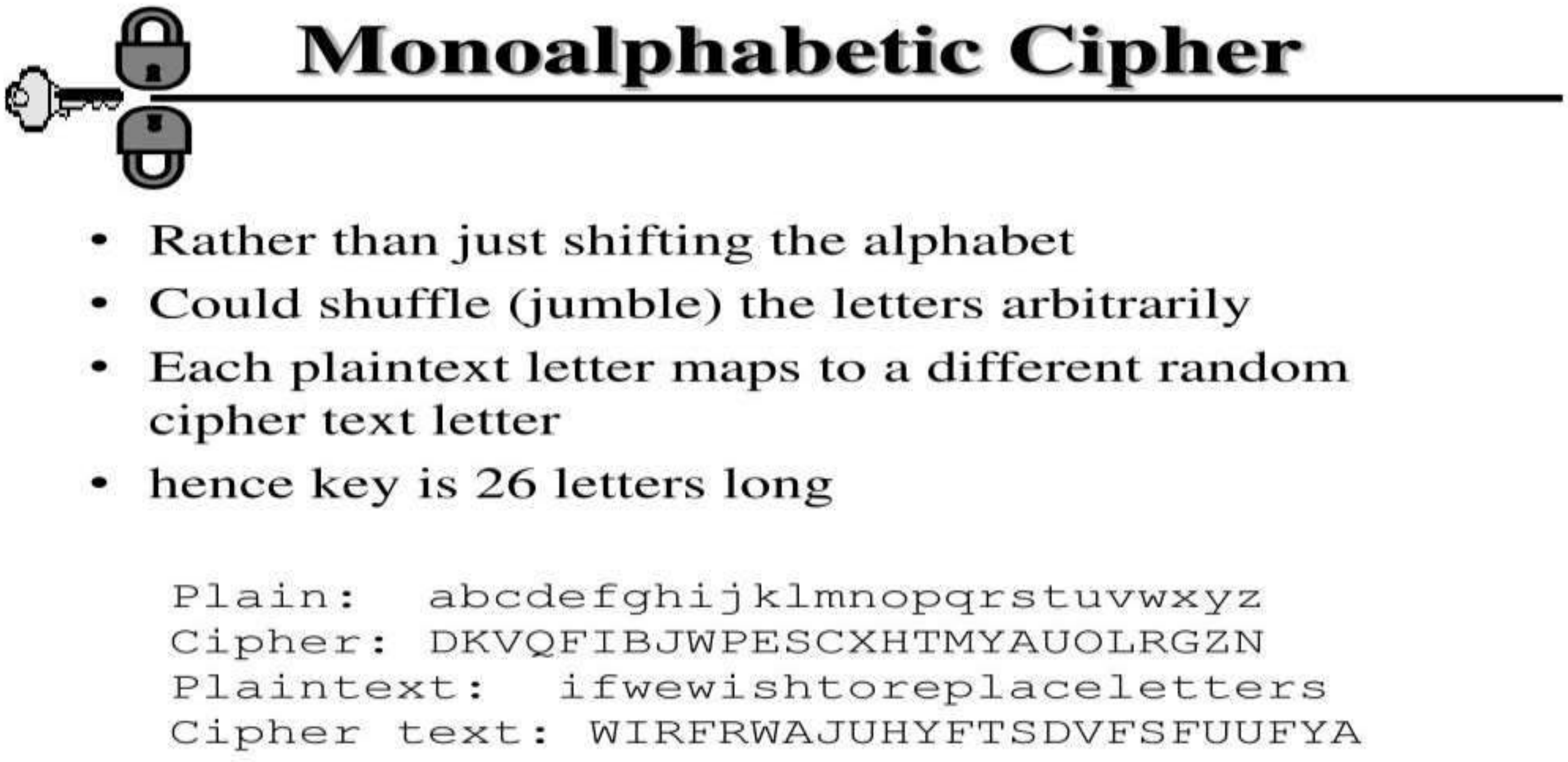
Cipher text: *SDB PRUH PRQHB*

Note that the alphabet is wrapped around, so that the letter following Z is A.

- *Plain: 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*
- *cipher: 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*

- *For each plaintext letter* ***p****, substitute the cipher text letter* ***c*** *such that*
- ***C = E(p) = (p+3) mod 26***
- *A shift may be any amount, so that general Caesar algorithm is*
- ***C = E (p) = (p+k) mod 26***
- *Where k takes on a value in the range 1 to 25. The decryption algorithm is simply*
- ***P = D(C) = (C-k) mod 26***

Monoalphabetic Cipher



Monoalphabetic Cipher

- Rather than just shifting the alphabet
- Could shuffle (jumble) the letters arbitrarily
- Each plaintext letter maps to a different random cipher text letter
- hence key is 26 letters long

```
Plain:   abcdefghijklmnopqrstuvwxyz
Cipher:  DKVQFIBJWPESCXHTMYAUOLRGZN
Plaintext:   ifwewishtoreplaceletters
Cipher text:  WIRFRWAJUHYFTSDVFSFUUFYA
```

Playfair Cipher

- The playfair algorithm is based on the use of 5x5 matrix of letters constructed using a keyword. Let the keyword be **"monarchy".**
- The matrix is constructed by filling in the letters of the keyword from left to right and from top to bottom, and then filling in the remainder of the matrix with the remaining letters in alphabetical order.
- The letter **"i" and "j"** count as one letter. Plaintext is encrypted two letters at a time According to the following rules:
- Repeating plaintext letters that would fall in the same pair are separated with a Filler letter such as "x".

Rules

1.Splitting 2 letters as a unit

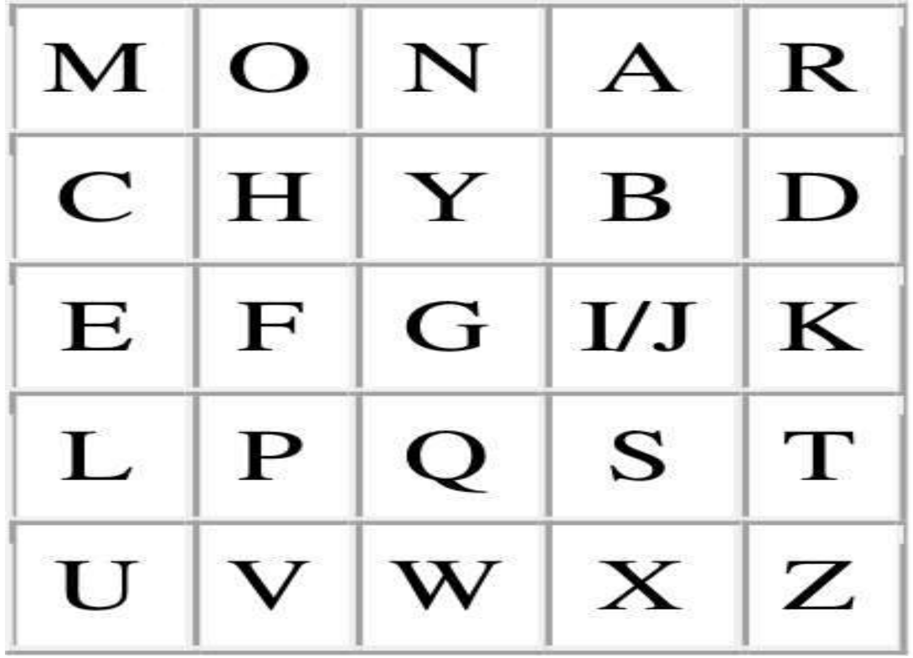
2.Repeating letter-Filler letter(Eg:balloon- ba lx lo on)

3.Same row|→| Wrap around

4.Same Column|↓| wrap around

5.Rectangle|⇄| Swap

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

Example

Plain Text: me(Same column)

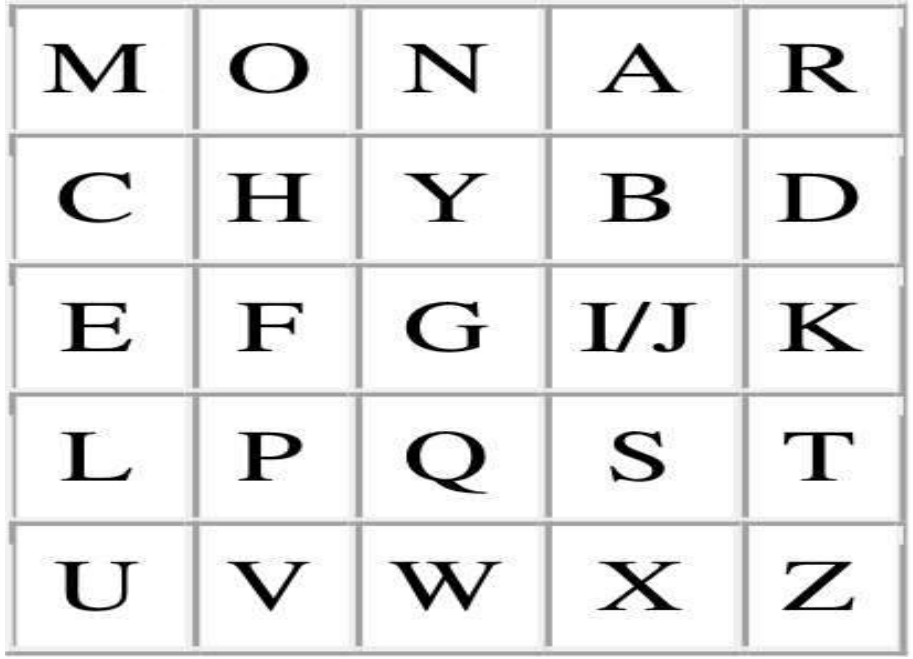
Cipher Text: CL

Plain Text: st (Same Row)

Cipher Text: TL

Plain Text: nt(Rectangle)

Cipher Text:RQ



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

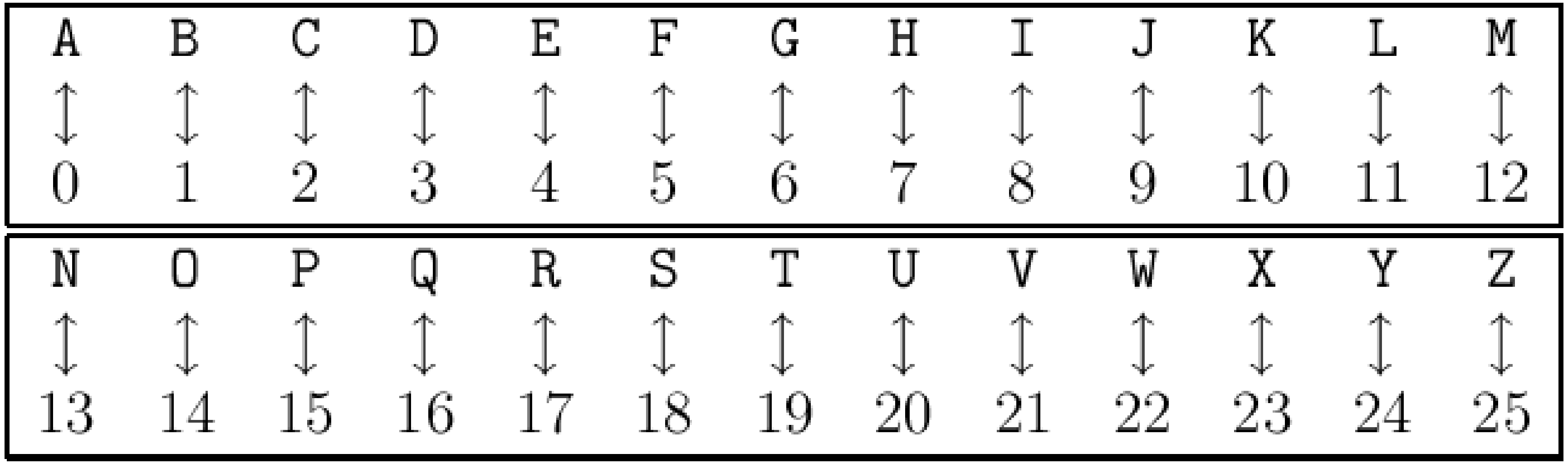
Plain Text:meet me at the school house

Splitting two letters as a unit => me et me at th es ch o x ol ho us ex

Corresponding cipher text => CL KL CL RS PD IL HY AV MP HF XL IU

Hill Cipher

- Another interesting multiletter cipher is the Hill cipher, developed by the mathe-matician Lester Hill in 1929.
- The Hill cipher makes use of modulo arithmetic, matrix multiplication, and matrix inverses; hence, it is a more mathematical cipher than others.



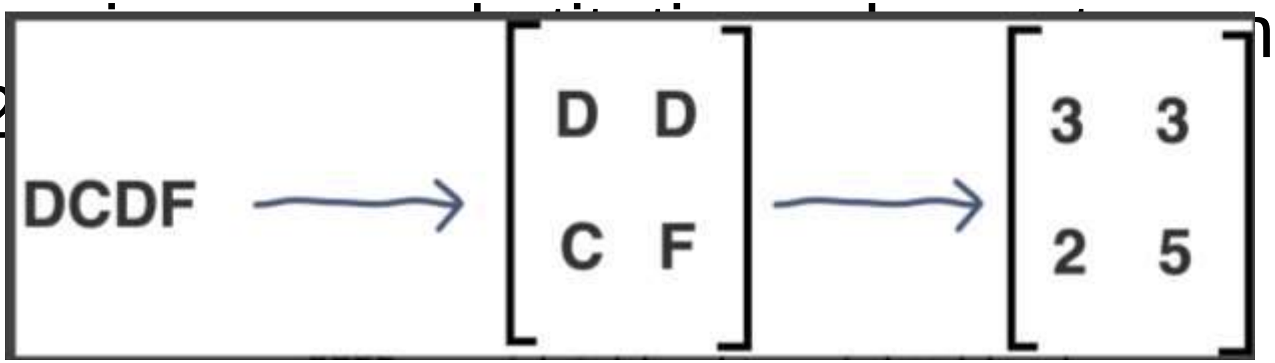
A	B	C	D	E	F	G	H	I	J	K	L	M
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
13	14	15	16	17	18	19	20	21	22	23	24	25

Encryption

E(K, P) = (K*P) mod 26

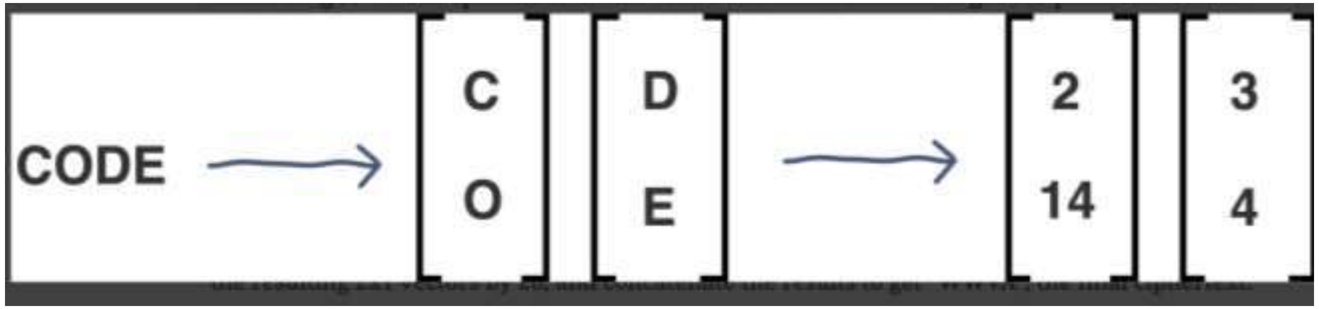
Where K is our key matrix and P is the plaintext in vector form. Matrix multiplying these two terms produces the encrypted ciphertext.

1. Pick a keyword to encrypt your plaintext message. Let’s work with the random keyword “DCDF”. Convert this keyword to matrix form vert it to a numerical 2



$$\text{DCDF} \longrightarrow \begin{bmatrix} D & D \\ C & F \end{bmatrix} \longrightarrow \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$$

2. we will convert our plaintext message to vector form. Since our key matrix is 2x2, the vector needs to be 2x1 for matrix multiplication to be possible. In our case, our message is four letters long so we can split it into blocks of two and then substitute to get our plaintext vectors.



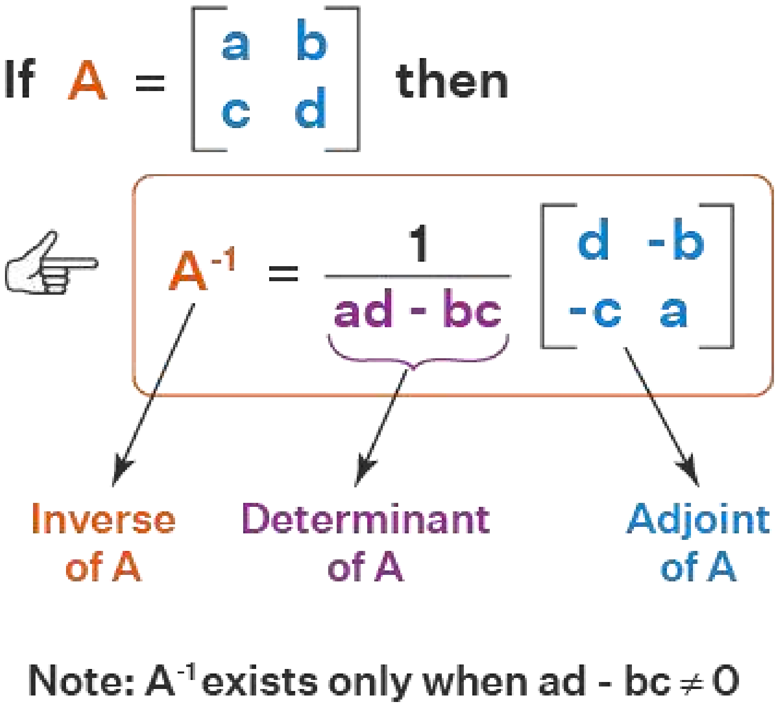
$$\text{CODE} \longrightarrow \begin{bmatrix} C \\ O \end{bmatrix} \begin{bmatrix} D \\ E \end{bmatrix} \longrightarrow \begin{bmatrix} 2 \\ 14 \end{bmatrix} \begin{bmatrix} 3 \\ 4 \end{bmatrix}$$

$$\left.\begin{aligned}
&\begin{bmatrix} D & D \\ C & F \end{bmatrix} \times \begin{bmatrix} C \\ O \end{bmatrix} \longrightarrow \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \times \begin{bmatrix} 2 \\ 14 \end{bmatrix} = \begin{bmatrix} 48 \\ 74 \end{bmatrix} \% \, 26 = \begin{bmatrix} 22 \\ 22 \end{bmatrix} \longrightarrow \begin{bmatrix} W \\ W \end{bmatrix} \\[2em]
&\begin{bmatrix} D & D \\ C & F \end{bmatrix} \times \begin{bmatrix} D \\ E \end{bmatrix} \longrightarrow \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \times \begin{bmatrix} 3 \\ 4 \end{bmatrix} = \begin{bmatrix} 21 \\ 26 \end{bmatrix} \% \, 26 = \begin{bmatrix} 21 \\ 0 \end{bmatrix} \longrightarrow \begin{bmatrix} V \\ A \end{bmatrix}
\end{aligned}\right\} \text{WWVA}$$

Decryption

- **D(K, C) = (K^{-1} *C) mod 26**

Inverse of a Matrix



If $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ then

$$\underset{\text{Inverse of A}}{A^{-1}} = \frac{1}{\underbrace{ad - bc}_{\text{Determinant of A}}} \underset{\text{Adjoint of A}}{\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}}$$

Note: A^{-1} exists only when $ad - bc \neq 0$

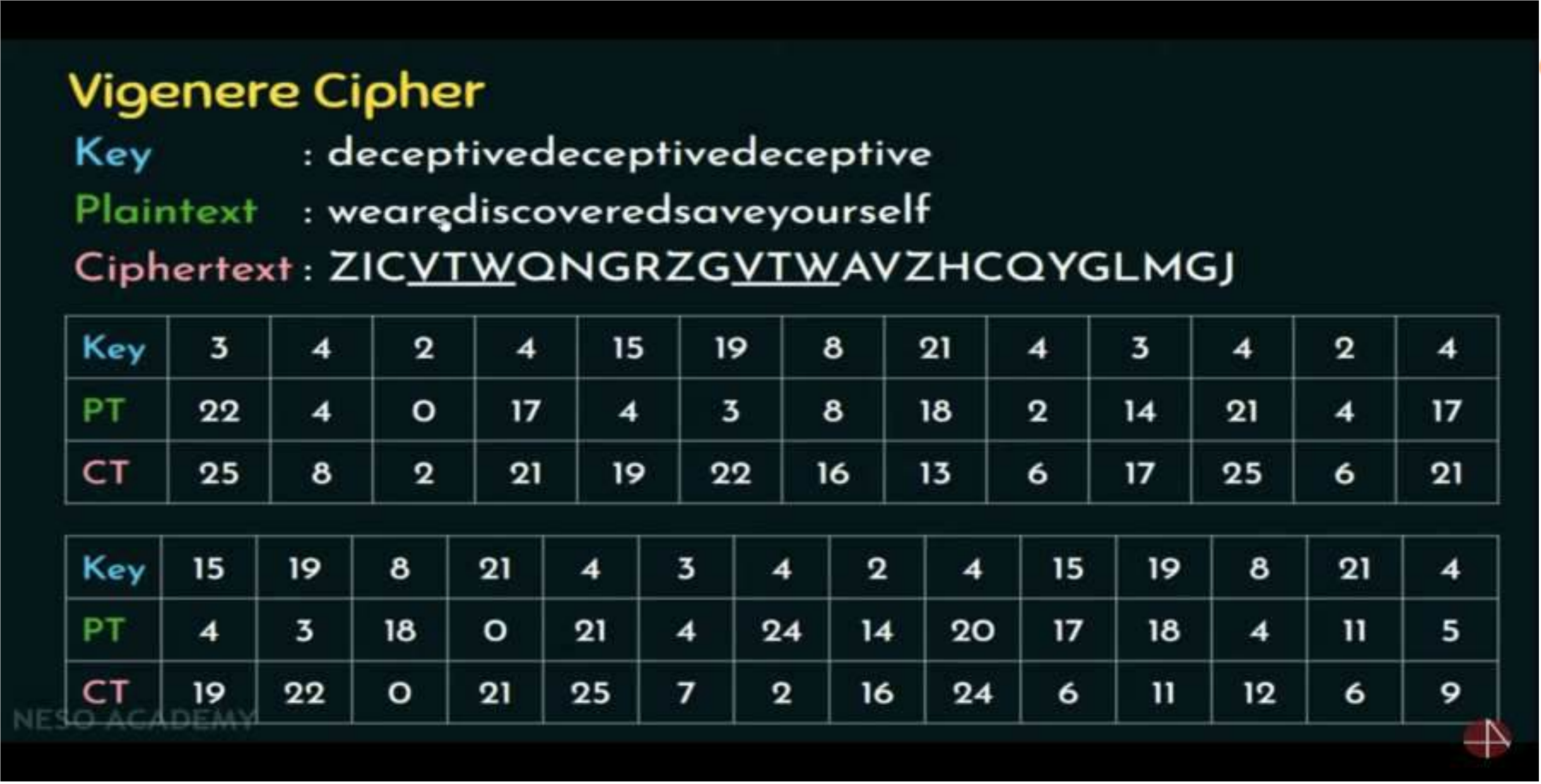
Polyalphabetic Cipher

Vigenere Cipher

$C_i = (p_i + k_i) \bmod 26$ **(Encryption)**

$p_i = (C_i - k_i) \bmod 26$ **(Decryption)**

- The first letter of the key is added to the first letter of the plaintext, mod 26
- The second letters are added, and so on through the first *m* letters of the plaintext.
- For the next *m* letters of the plaintext, the key letters are **repeated**. This process continues until all of the plaintext sequence is encrypted.



Vigenere Cipher

Key : deceptivedeceptivedeceptive

Plaintext : wearediscoveredsaveyourself

Ciphertext : ZICVTWQNGRZGVTWAVZHCQYGLMGJ

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

Key	15	19	8	21	4	3	4	2	4	15	19	8	21	4
PT	4	3	18	0	21	4	24	14	20	17	18	4	11	5
CT	19	22	0	21	25	7	2	16	24	6	11	12	6	9

25 mod 26=25
8 mod 26=8
39 mod 26=13

Vernam Cipher

- Introduced by Gilbert Vernam in 1918. His system works on binary data (bits) rather than letters.
- Vernam proposed 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.

$E\ (P_i\ ,\ K_i) = P_i\ (XOR)\ K_i$

$D\ (C_i\ ,\ K_i) = C_i\ (XOR)\ K_i$

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 00 = 28

Since the resulting number is greater than 26, subtract 26 from it.

28 - 26 = 2 ==> C

CIPHER-TEXT: C

One time pad

One Time Pad algorithm is the improvement of the Vernam Cipher

- The key should be **randomly generated as long as the size of the message**.
- The key is to be used to encrypt and decrypt **a single message**, and **then it is discarded**.
- So encrypting every new message requires a new key of the same length as the new message in one-time pad.

One-Time Pad is the only algorithm that is truly unbreakable and can be used for low-bandwidth channels requiring very high security**(ex. for military uses).**

Transposition Techniques

Rail Fence Technique

- Rail fence is simplest of such cipher, in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.

Plaintext = meet at the school house

- To encipher this message with a rail fence of depth 2,
- **m e a t e c o l o s**
- **e t t h s h o h u e**
- *The encrypted message is*

Cipher Text=MEATECOLOSETTHSHOHUE

Row-Transposition Cipher

- A more complex scheme is to write the message in a rectangle, row by row, and read the message off, **column by column**, but permute the order of the columns. The order of columns then becomes the key of the algorithm.

plaintext = meet at the school house

Key = 4 3 1 2 5 6 7

4	3	1	2	5	6	7
M	E	E	T	A	T	T
H	E	S	C	H	O	O
L	H	O	U	S	E	X

Cipher Text:ESOTCUEEHMHLAHSTOETOX

Stegnography

Steganography is the practice of concealing information within another message or physical object to avoid detection.

Example: Simply encrypt correct reading exactly twice.

- **Character marking:** Selected letters of printed or typewritten text are over-written in pencil. The marks are ordinarily not visible unless the paper is held at an angle to bright light.
- **Invisible ink:** A number of substances can be used for writing but leave no visible trace until heat or some chemical is applied to the paper.
- **Pin punctures:** Small pin punctures on selected letters are ordinarily not visi-ble unless the paper is held up in front of a light.
- **Typewriter correction ribbon:** Used between lines typed with a black ribbon, the results of typing with the correction tape are visible only under a strong light.