Module 1: Introduction to Network Security & Cryptography

-by
Prof Rohini Sawant

BACKGROUND

Information Security requirements have changed in recent times

Traditionally provided by physical and administrative mechanisms

Computer use requires automated tools to protect files and other stored information

Use of networks and communications links requires measures to protect data during transmission

Aim of Course

Our focus is on Internet Security

Which consists of measures to deter, prevent, detect, and correct security violations that involve the transmission & storage of information

CIA TRIAD

Computer Security: The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications). This definition introduces three key objectives that are at the heart of computer security: •

Confidentiality: This term covers two related concepts:

Data confidentiality: Assures that private or confidential information is not made available or disclosed to unauthorized individuals.

Privacy: Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

CIA TRIAD

Integrity: This term covers two related concepts:

Data integrity: Assures that information and programs are changed only in a specified and authorized manner.

System integrity: Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

Availability: Assures that systems work promptly and service is not denied to authorized users

OSI Security Architecture

ITU-T X.800 “Security Architecture for OSI” defines a systematic way of defining and providing security requirements for us it provides a useful, if abstract, overview of concepts we will study in the due course.

OSI Security Architecture Encompasses three main concepts:

- Security Attacks
- Security Services
- Security Mechanisms

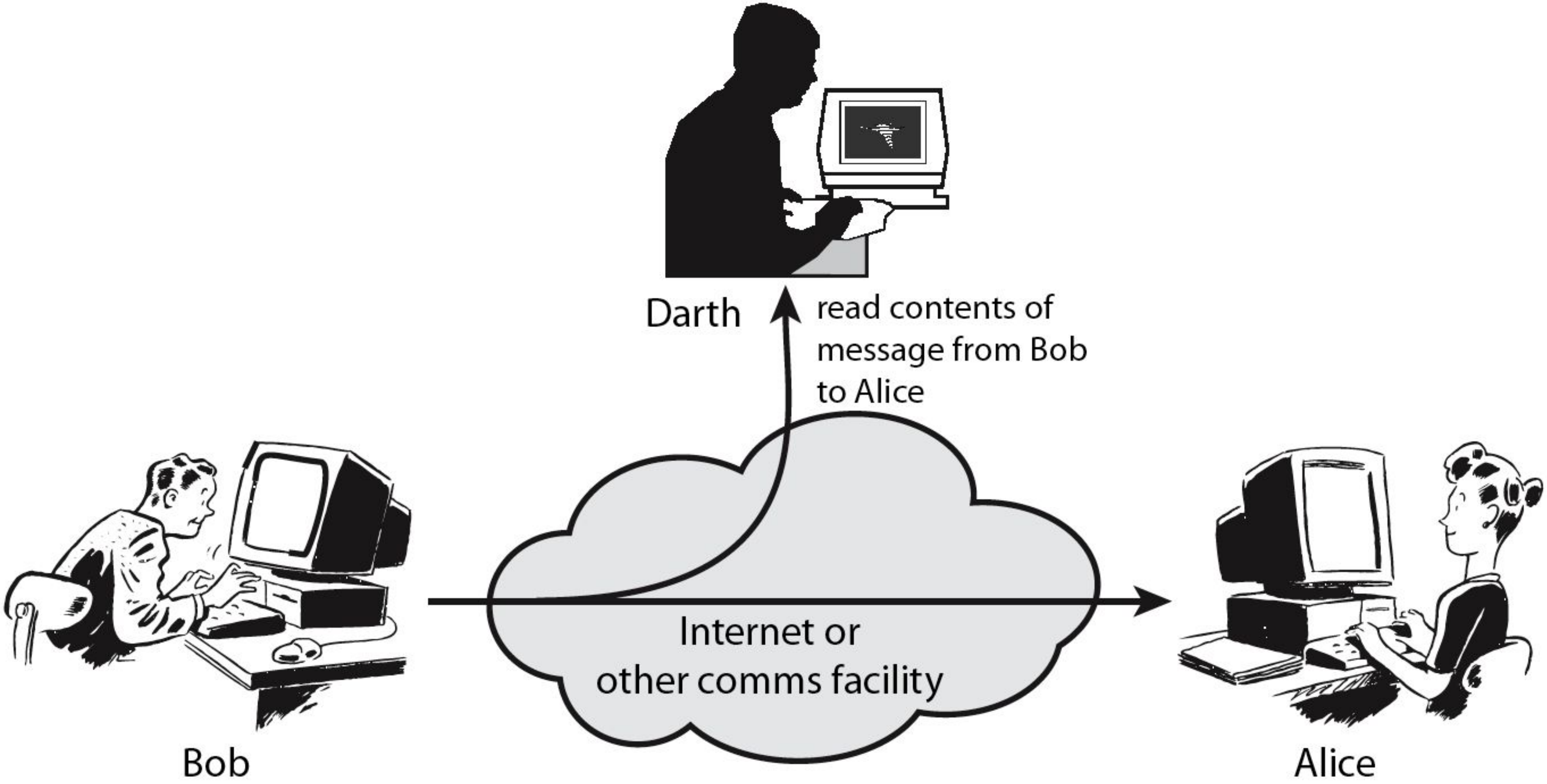
SECURITY ATTACK

ATTACK is any action that compromises the security of information owned by an organization

Information security is about how to prevent attacks, or failing that, to detect attacks on information-based systems.

Often threat & attack used to mean same thing. There is wide range of attacks & we can focus of generic types of attacks

- Passive Attacks
- Active Attacks


Darth
read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

PASSIVE ATTACKS

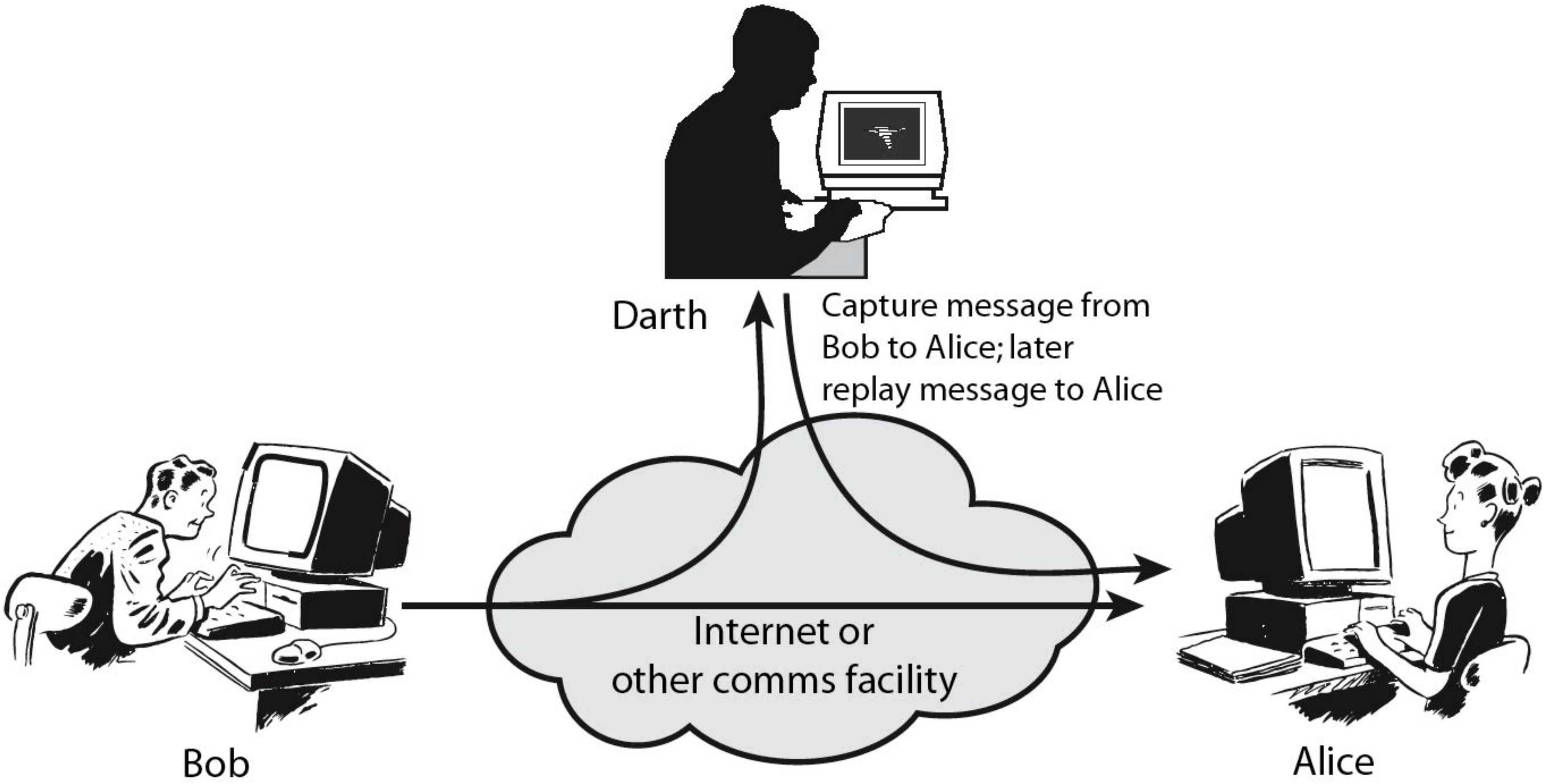
Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted.

Two types of passive attacks are the **release of message contents** and **traffic analysis.**

Passive attacks are very difficult to detect, because they do not involve any alteration of the data.

However, it is feasible to prevent the success of these attacks, usually by means of encryption.

Thus, the emphasis in dealing with passive attacks is on prevention rather than detection


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

ACTIVE ATTACKS

Active attack involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: masquerade, replay, modification of messages, and denial of service.

- A masquerade takes place when one entity pretends to be a different entity.
- Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.
- Modification of messages simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect
- The denial of service prevents or inhibits the normal use or management of communications facilities

ACTIVE ATTACKS

Active attacks present the opposite characteristics of passive attacks. Whereas passive attacks are difficult to detect, measures are available to prevent their success.

On the other hand, it is quite difficult to prevent active attacks absolutely because of the wide variety of potential physical, software, and network vulnerabilities. Instead, the goal is to detect active attacks and to recover from any disruption or delays caused by them.

SECURITY SERVICES

X.800:

“a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers”

RFC 2828:

“a processing or communication service provided by a system to give a specific kind of protection to system resources”

SECURITY SERVICES

Authentication - assurance that the communicating entity is the one claimed

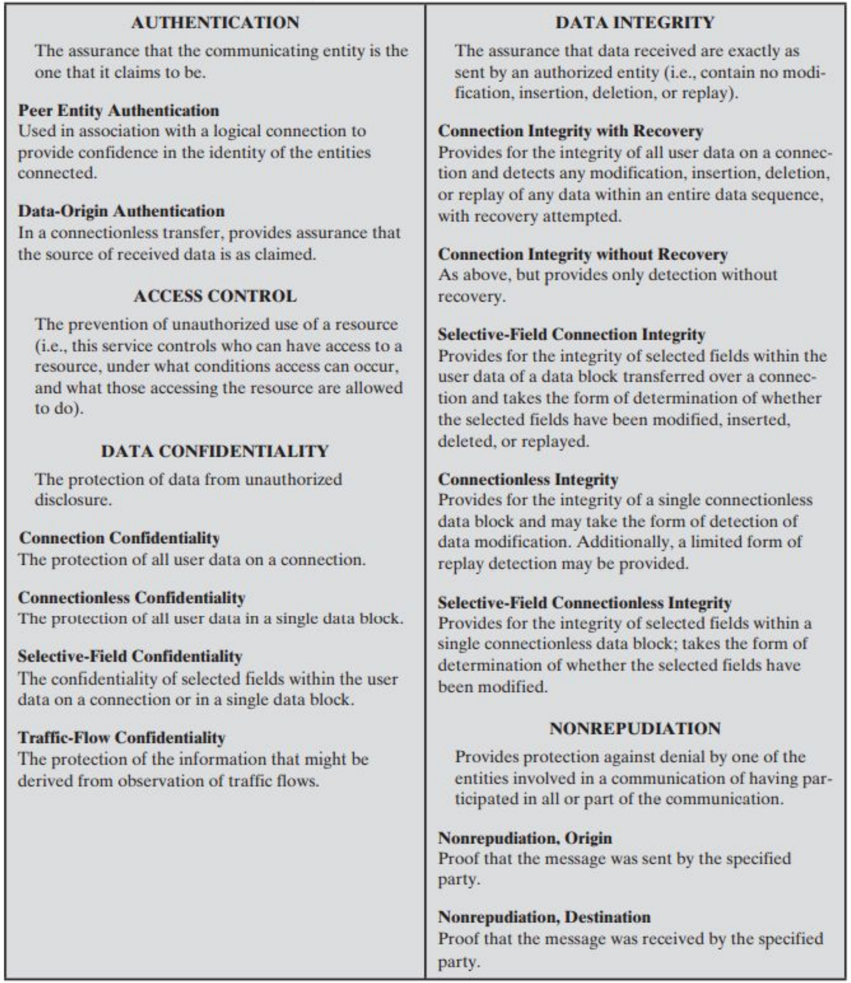
Access Control - prevention of the unauthorized use of a resource

Data Confidentiality –protection of data from unauthorized disclosure

Data Integrity - assurance that data received is as sent by an authorized entity

Non-Repudiation - protection against denial by one of the parties in a communication

Table 1.2 Security Services (X.800)



AUTHENTICATION

The assurance that the communicating entity is the one that it claims to be.

Peer Entity Authentication
Used in association with a logical connection to provide confidence in the identity of the entities connected.

Data-Origin Authentication
In a connectionless transfer, provides assurance that the source of received data is as claimed.

ACCESS CONTROL

The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).

DATA CONFIDENTIALITY

The protection of data from unauthorized disclosure.

Connection Confidentiality
The protection of all user data on a connection.

Connectionless Confidentiality
The protection of all user data in a single data block.

Selective-Field Confidentiality
The confidentiality of selected fields within the user data on a connection or in a single data block.

Traffic-Flow Confidentiality
The protection of the information that might be derived from observation of traffic flows.

DATA INTEGRITY

The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).

Connection Integrity with Recovery
Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.

Connection Integrity without Recovery
As above, but provides only detection without recovery.

Selective-Field Connection Integrity
Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.

Connectionless Integrity
Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.

Selective-Field Connectionless Integrity
Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.

NONREPUDIATION

Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

Nonrepudiation, Origin
Proof that the message was sent by the specified party.

Nonrepudiation, Destination
Proof that the message was received by the specified party.

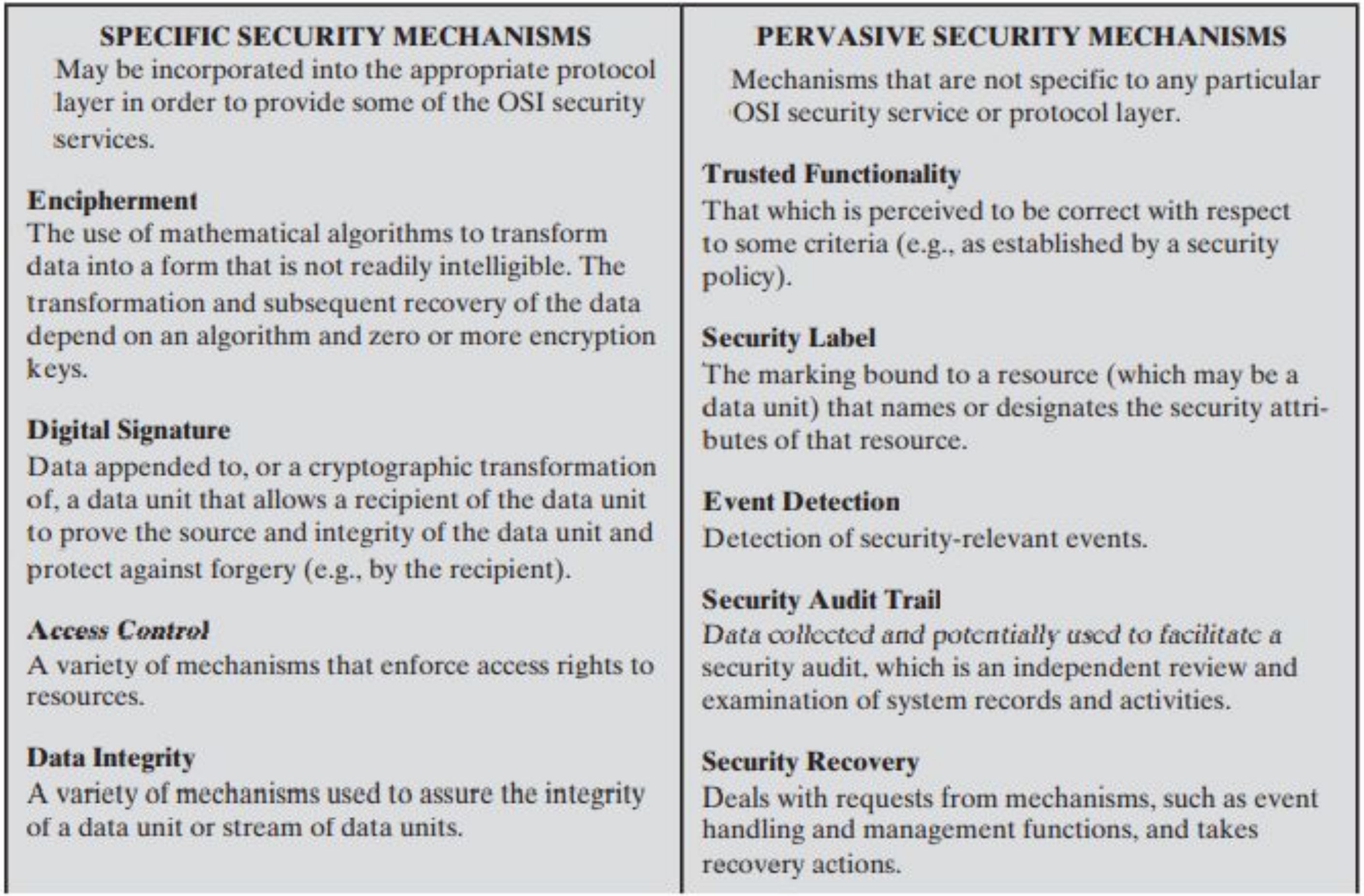
SECURITY MECHANISM

The mechanisms are divided into those that are implemented in a specific protocol layer, such as TCP or an application-layer protocol, and those that are not specific to any particular protocol layer or security service.

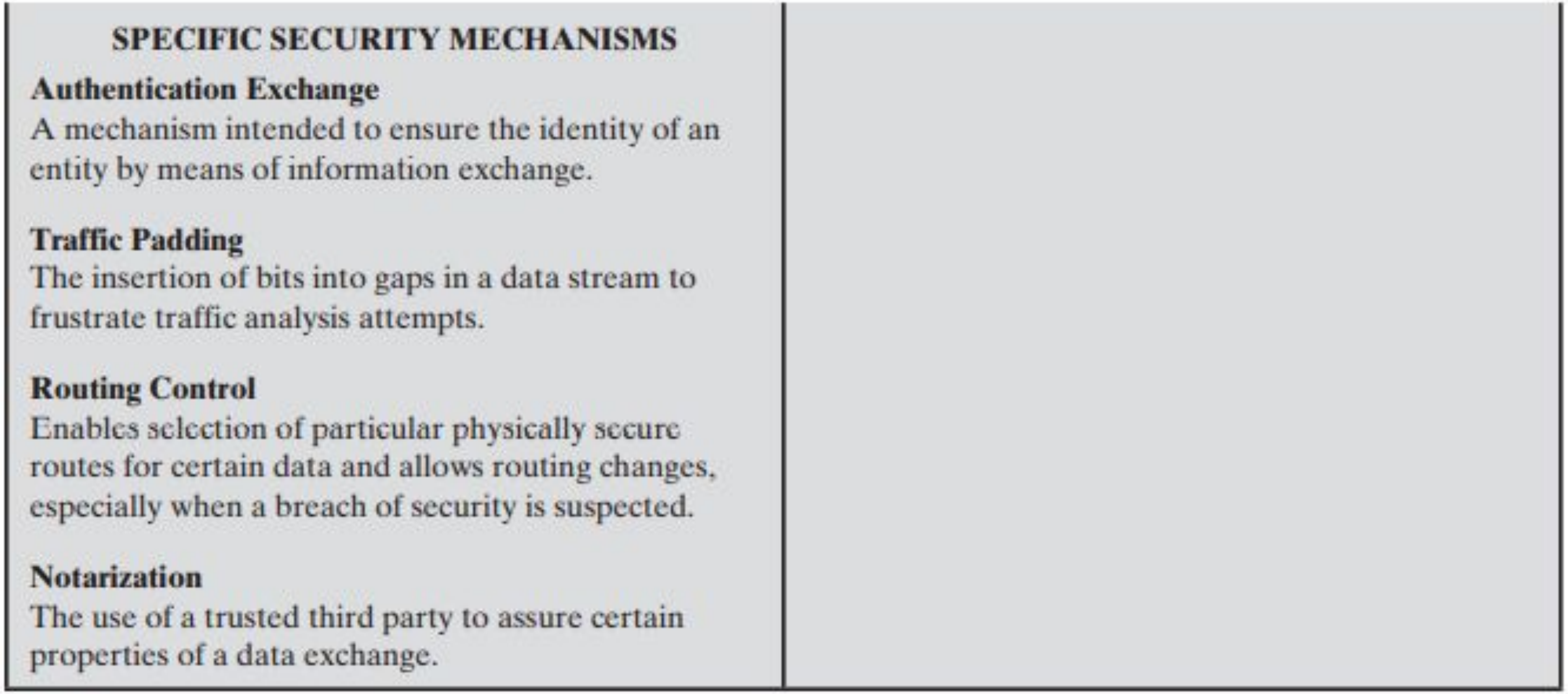
Specific security mechanisms: encipherment, digital signatures, access controls, data integrity, authentication exchange, traffic padding, routing control, notarization

Pervasive security mechanisms: trusted functionality, security labels, event detection, security audit trails, security recovery

Table 1.3 Security Mechanisms (X.800)



SPECIFIC SECURITY MECHANISMS	PERVASIVE SECURITY MECHANISMS
May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.	Mechanisms that are not specific to any particular OSI security service or protocol layer.
Encipherment The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.	**Trusted Functionality** That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).
Digital Signature Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery (e.g., by the recipient).	**Security Label** The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.
Access Control A variety of mechanisms that enforce access rights to resources.	**Event Detection** Detection of security-relevant events.
Data Integrity A variety of mechanisms used to assure the integrity of a data unit or stream of data units.	**Security Audit Trail** *Data collected and potentially used to facilitate a* security audit, which is an independent review and examination of system records and activities.
	Security Recovery Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.



SPECIFIC SECURITY MECHANISMS

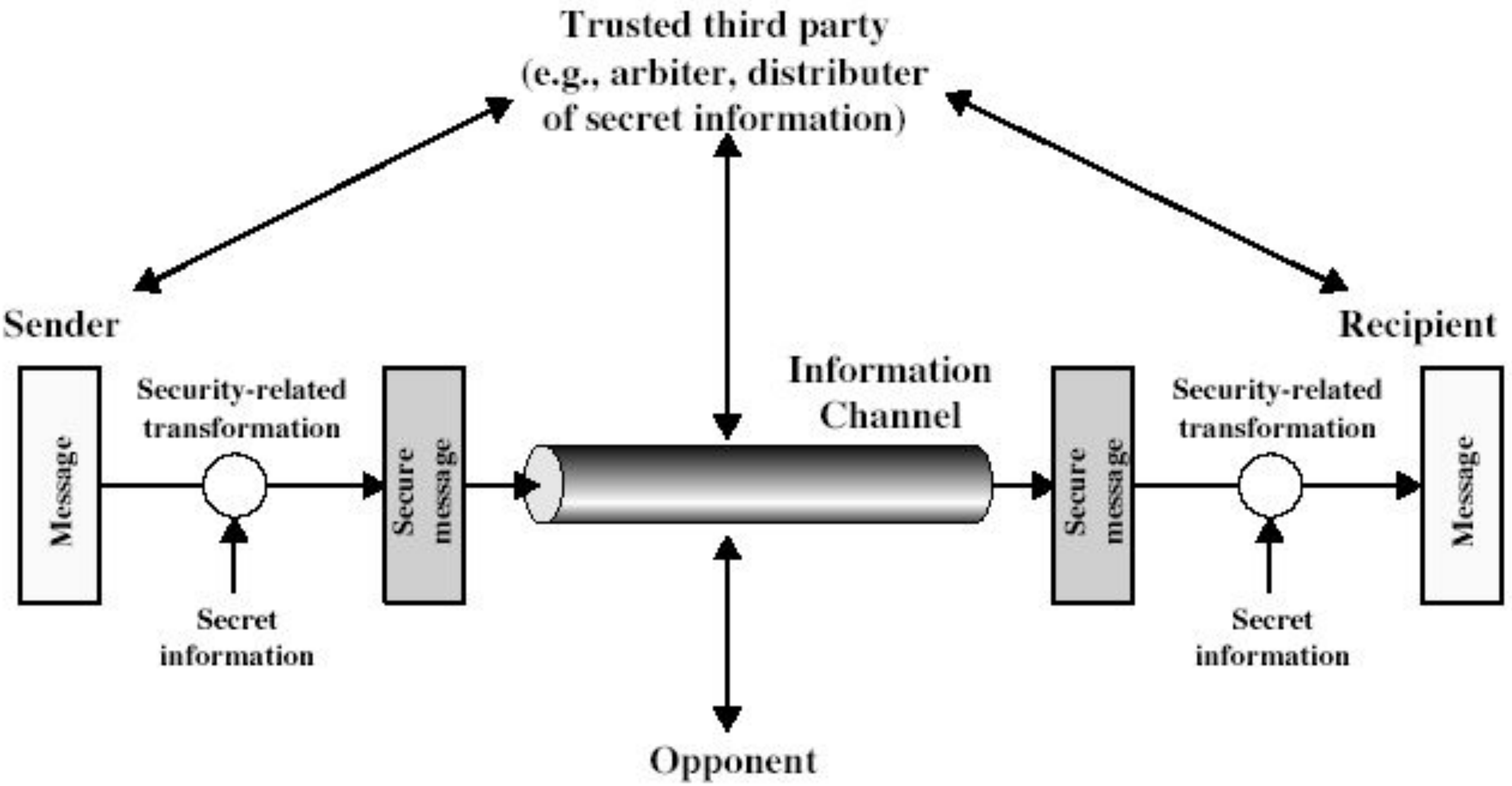
Authentication Exchange
A mechanism intended to ensure the identity of an entity by means of information exchange.

Traffic Padding
The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.

Routing Control
Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.

Notarization
The use of a trusted third party to assure certain properties of a data exchange.

NETWORK SECURITY MODEL



NETWORK SECURITY MODEL

A message is to be transferred from one party to another across some sort of Internet service.

The two parties, who are the principals in this transaction, must cooperate for the exchange to take place.

A logical information channel is established by defining a route through the Internet from source to destination and by the cooperative use of communication protocols (e.g., TCP/IP) by the two principals.

Security aspects come into play when it is necessary or desirable to protect the information transmission from an opponent who may present a threat to confidentiality, authenticity, and so on.

NETWORK SECURITY MODEL

All the techniques for providing security have two components:

- A security-related transformation on the information to be sent. Examples include the encryption of the message, which scrambles the message so that it is unreadable by the opponent, and the addition of a code based on the contents of the message, which can be used to verify the identity of the sender.
- Some secret information shared by the two principals and, it is hoped, unknown to the opponent. An example is an encryption key used in conjunction with the transformation to scramble the message before transmission and unscramble it on reception.

A trusted third party may be needed to achieve secure transmission. For example, a third party may be responsible for distributing the secret information to the two principals while keeping it from any opponent or for distribution of certificates.

NETWORK SECURITY MODEL

This general model shows that there are four basic tasks in designing a particular security service:

1. Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose.

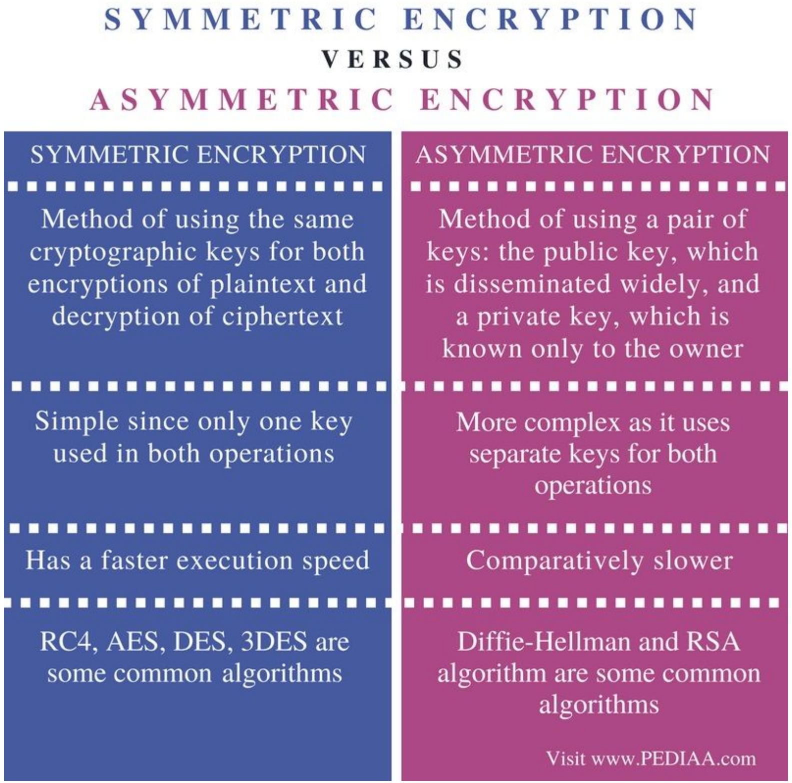
2. Generate the secret information to be used with the algorithm.

3. Develop methods for the distribution and sharing of the secret information.

4. Specify a protocol to be used by the two principals that makes use of the security algorithm and the secret information to achieve a particular security service.

SYMMETRIC & ASYMMETRIC KEY CRYPTOGRAPHY

- Symmetric key cryptography is any cryptographic algorithm that is based on a shared key that is used to encrypt or decrypt text/ciphertext, in contrast to asymmetric key cryptography, where the encryption and decryption keys are different.
- Symmetric encryption is generally more efficient than asymmetric encryption and therefore preferred when large amounts of data need to be exchanged.
- Establishing the shared key is difficult using only symmetric encryption algorithms, so in many cases, asymmetric encryption is used to establish the shared key between two parties.
- Examples of symmetric key cryptography include AES, DES, and 3DES.



SYMMETRIC ENCRYPTION
VERSUS
ASYMMETRIC ENCRYPTION

SYMMETRIC ENCRYPTION	ASYMMETRIC ENCRYPTION
Method of using the same cryptographic keys for both encryptions of plaintext and decryption of ciphertext	Method of using a pair of keys: the public key, which is disseminated widely, and a private key, which is known only to the owner
Simple since only one key used in both operations	More complex as it uses separate keys for both operations
Has a faster execution speed	Comparatively slower
RC4, AES, DES, 3DES are some common algorithms	Diffie-Hellman and RSA algorithm are some common algorithms

Visit www.PEDIAA.com

CLASSICAL ENCRYPTION TECHNIQUES

- Symmetric encryption, also referred to as conventional encryption or single-key encryption, was the only type of encryption in use prior to the development of publickey encryption in the 1970s.
- It remains by far the most widely used of the two types of encryption.
- An original message is known as the **plaintext**, while the coded message is called the **ciphertext.**
- The process of converting from plaintext to ciphertext is known as **enciphering or encryption;** restoring the plaintext from the ciphertext is **deciphering or decryption.**
- The many schemes used for encryption constitute the area of study known as **cryptography.**

CLASSICAL ENCRYPTION TECHNIQUES

- Such a scheme is known as a **cryptographic system or a cipher.**
- Techniques used for deciphering a message without any knowledge of the enciphering details fall into the area of **Cryptanalysis**.
- Cryptanalysis is what the layperson calls “breaking the code.”
- The areas of cryptography and cryptanalysis together are called **Cryptology.**
- There are two requirements for secure use of conventional encryption:

There are two requirements for secure use of conventional encryption:

1. We need a strong encryption algorithm. At a minimum, we would like the algorithm to be such that an opponent who knows the algorithm and has access to one or more ciphertexts would be unable to decipher the ciphertext or figure out the key.

2. Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure. If someone can discover the key and knows the algorithm, all communication using this key is readable.

CLASSICAL ENCRYPTION TECHNIQUES

The two basic building blocks of all encryption techniques are **Substitution** and **Transposition.**

- **A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols.**
- If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns.
- **A different kind of mapping is achieved by performing some sort of permutation on the plaintext letters. This technique is referred to as a transposition cipher.**

CAESAR CIPHER

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.
- So that the general Caesar algorithm is
- $C = E(k, p) = (p + k) \bmod 26$
- $p = D(k, C) = (C - k) \bmod 26$

CAESAR CIPHER

For example,

- plain: meet me after the toga party
- cipher: PHHW PH DIWHU WKH WRJD SDUWB

Three important characteristics of this problem enabled us to use a bruteforce cryptanalysis:

1. The encryption and decryption algorithms are known.

2. There are only 25 keys to try.

3. The language of the plaintext is known and easily recognizable

MONOALPHABETIC SUBSTITUTION CIPHER

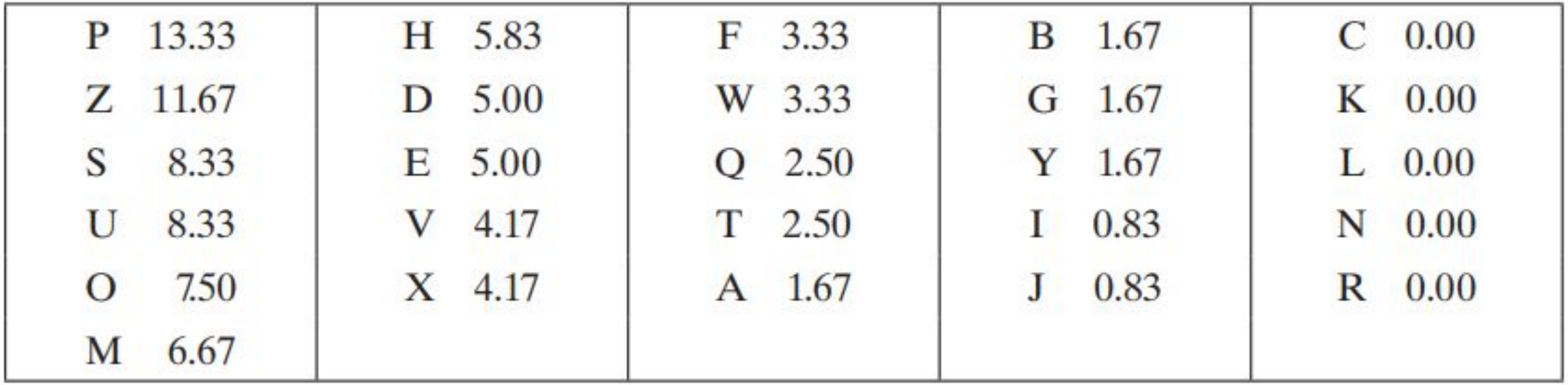
- A permutation of a finite set of elements S is an ordered sequence of all the elements of S, with each element appearing exactly once.
- For example, if S = {a, b, c}, there are six permutations of S

  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.
- If, instead, the “cipher” line can be any permutation of the 26 alphabetic characters, then there are 26! or greater than 4 * 1026 possible keys.
- 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

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ



P	13.33	H	5.83	F	3.33	B	1.67	C	0.00
Z	11.67	D	5.00	W	3.33	G	1.67	K	0.00
S	8.33	E	5.00	Q	2.50	Y	1.67	L	0.00
U	8.33	V	4.17	T	2.50	I	0.83	N	0.00
O	7.50	X	4.17	A	1.67	J	0.83	R	0.00
M	6.67								

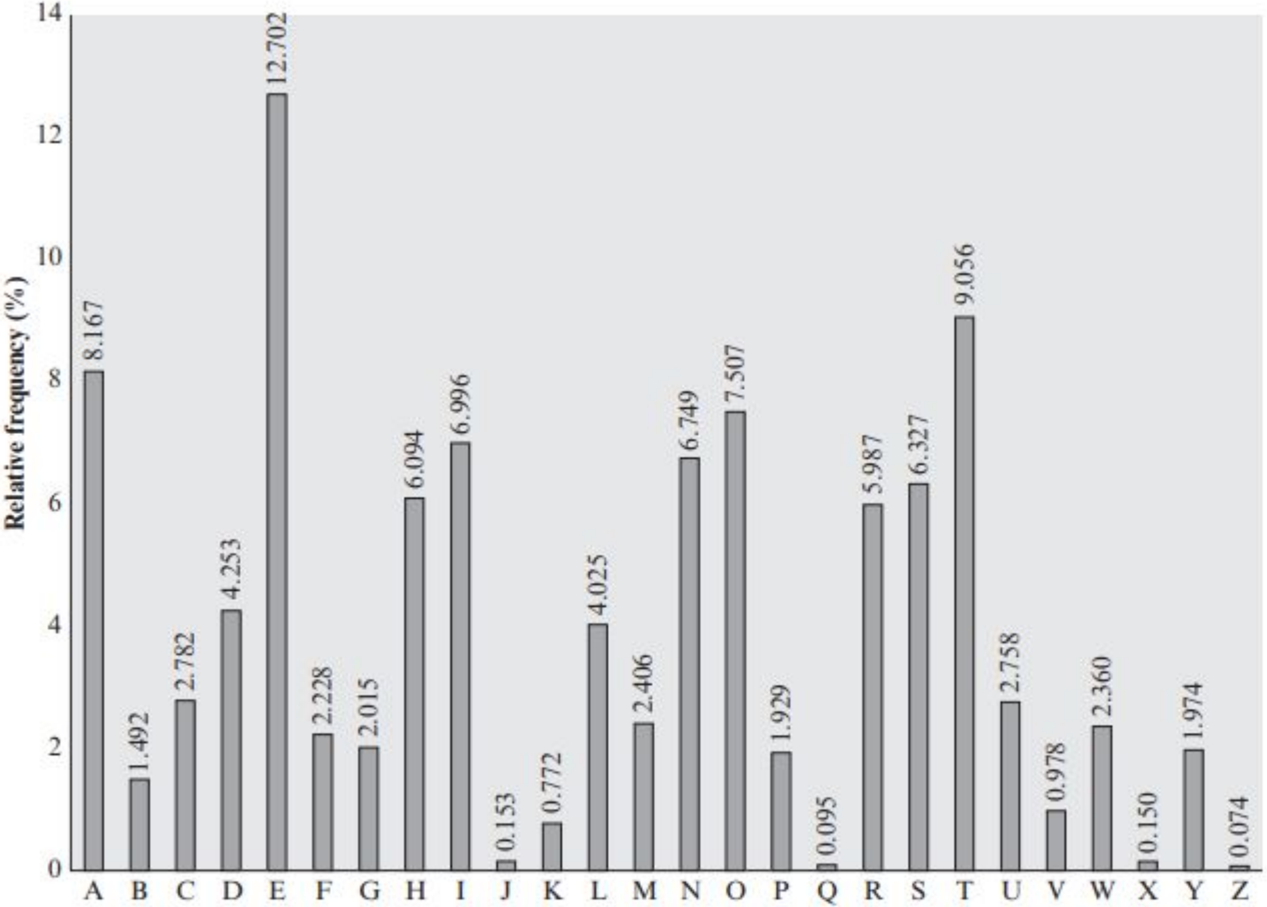


Figure 3.5 Relative Frequency of Letters in English Text

MONOALPHABETIC SUBSTITUTION CIPHER

- .A table similar to Figure 3.5 could be drawn up showing the relative frequency of diagrams.
- The most common such diagram is th.
- In our ciphertext, the most common diagram is ZW, which appears three times.
- So we make the correspondence of Z with t and W with h. Then, by our earlier hypothesis, we can equate P with e. Now notice that the sequence ZWP appears in the ciphertext, and we can translate that sequence as “the.”

MONOALPHABETIC SUBSTITUTION CIPHER

- Continued analysis of frequencies plus trial and error should easily yield a solution from this point.
- The complete plaintext, with spaces added between words, follows:

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

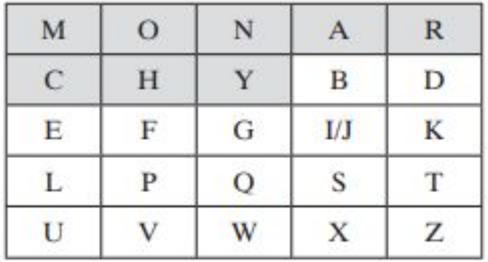
- Monoalphabetic ciphers are easy to break because they reflect the frequency data of the original alphabet.
- A countermeasure is to provide multiple substitutes, known as homophones, for a single letter.

PLAYFAIR CIPHER

- The best-known multiple-letter encryption cipher is the Playfair, which treats digrams in the plaintext as single units and translates these units into ciphertext digrams.
- The Playfair algorithm is based on the use of a 5 * 5 matrix of letters constructed using a keyword. Here is an example
- This cipher was actually invented by British scientist Sir Charles Wheatstone in 1854, but it bears the name of his friend Baron Playfair of St. Andrews, who championed the cipher at the British foreign office.

PLAYFAIR CIPHER

- In this case, the keyword is monarchy.
- The matrix is constructed by filling in the letters of the keyword (minus duplicates) 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 letters I and J count as one letter.



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

Plaintext is encrypted two letters at a time, according to the following rules:

- Repeating plaintext letters that are in the same pair are separated with a filler letter, such as x, so that balloon would be treated as ba lx lo on.
- Two plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row circularly following the last.
- For example, ar is encrypted as RM.
- Two plaintext letters that fall in the same column are each replaced by the letter beneath, with the top element of the column circularly following the last. For example, mu is encrypted as CM.
- Otherwise, each plaintext letter in a pair is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter.
- Thus, hs becomes BP and ea becomes IM (or JM, as the encipherer wishes)

PLAYFAIR CIPHER

PLAINTEXT: greet

KEYWORD: moon mission = m,o,n,i,s

Digrams: gr ee t = gr ex et

Cipher Text: HQ CZ DU

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

G	H
Q	R

gr= HQ

C	D	E
H	K	L
R	T	U
X	Y	Z

ex = CZ

D	E
H	L
T	U

et = DU

PLAYFAIR CIPHER

Q. Encrypt “this is the final exam” with Playfair Cipher using key “Guidance”. Explain the steps involved (MU_May19, 10 Marks)

VIGENERE CIPHER

- The best known, and one of the simplest, polyalphabetic ciphers is the Vigenère cipher.
- In this scheme, the set of related monoalphabetic substitution rules consists of the 26 Caesar ciphers with shifts of 0 through 25.
- Each cipher is denoted by a key letter, which is the ciphertext letter that substitutes for the plaintext letter.
- We can express the Vigenère cipher in the following manner. Assume a sequence of plaintext letters P = p0, p1, p2, c , pn-1 and a key consisting of the sequence of letters K = k0, k1, k2, c , km-1, where typically m 6 n. The sequence of ciphertext letters C = C0, C1, C2, c , Cn-1 is calculated as follows:
- C = C0, C1, C2, c , Cn-1 = E(K, P) = E[(k0, k1, k2, c , km-1), (p0, p1, p2, c , pn-1)] = (p0 + k0) mod 26, (p1 + k1) mod 26, c ,(pm-1 + km-1) mod 26, (pm + k0) mod 26, (pm+1 + k1) mod 26, c , (p2m-1 + km-1) mod 26, c

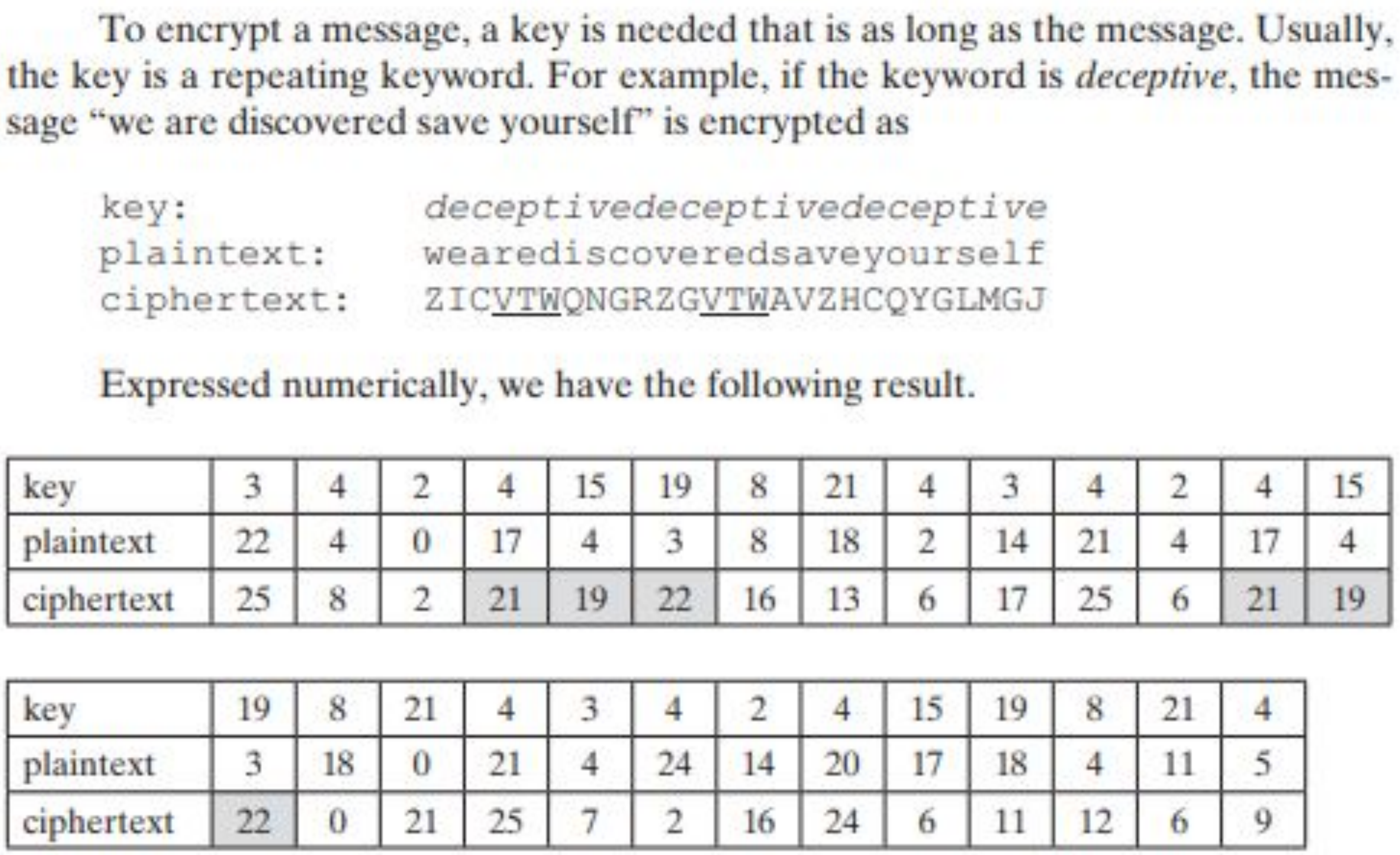
VIGENERE CIPHER

- Thus, 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.
- A general equation of the encryption process is

  $C_i = (p_i + k_{i \bmod m}) \bmod 26$

- Similarly, decryption is a generalization of above Equation

  $p_i = (C_i - k_{i \bmod m}) \bmod 26$



To encrypt a message, a key is needed that is as long as the message. Usually, the key is a repeating keyword. For example, if the keyword is *deceptive*, the message "we are discovered save yourself" is encrypted as

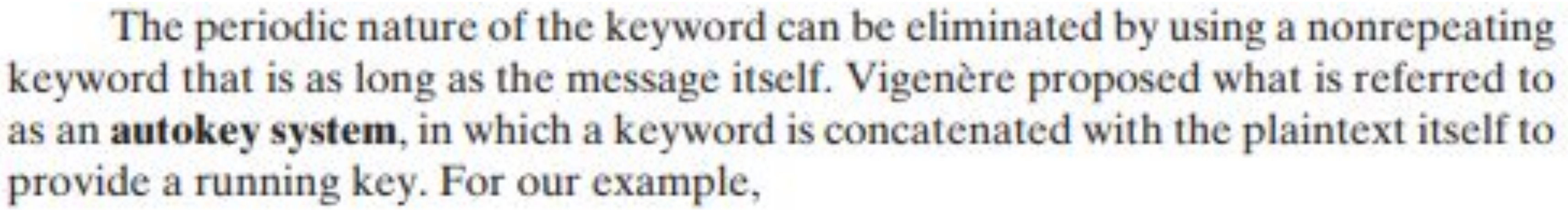
```
key:          deceptivedeceptivedeceptive
plaintext:    wearediscoveredsaveyourself
ciphertext:   ZICVTWQNGRZGVTWAVZHCQYGLMGJ
```

Expressed numerically, we have the following result.

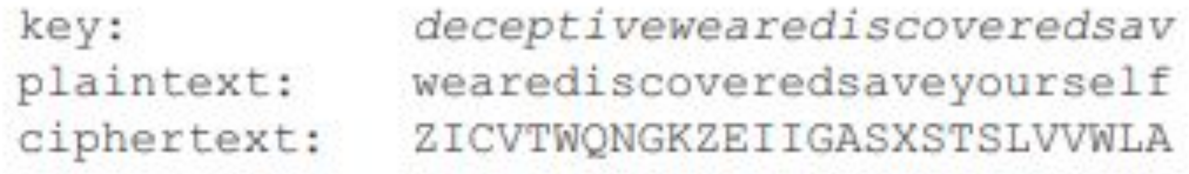
key	3	4	2	4	15	19	8	21	4	3	4	2	4	15
plaintext	22	4	0	17	4	3	8	18	2	14	21	4	17	4
ciphertext	25	8	2	21	19	22	16	13	6	17	25	6	21	19

key	19	8	21	4	3	4	2	4	15	19	8	21	4
plaintext	3	18	0	21	4	24	14	20	17	18	4	11	5
ciphertext	22	0	21	25	7	2	16	24	6	11	12	6	9

VIGENERE CIPHER



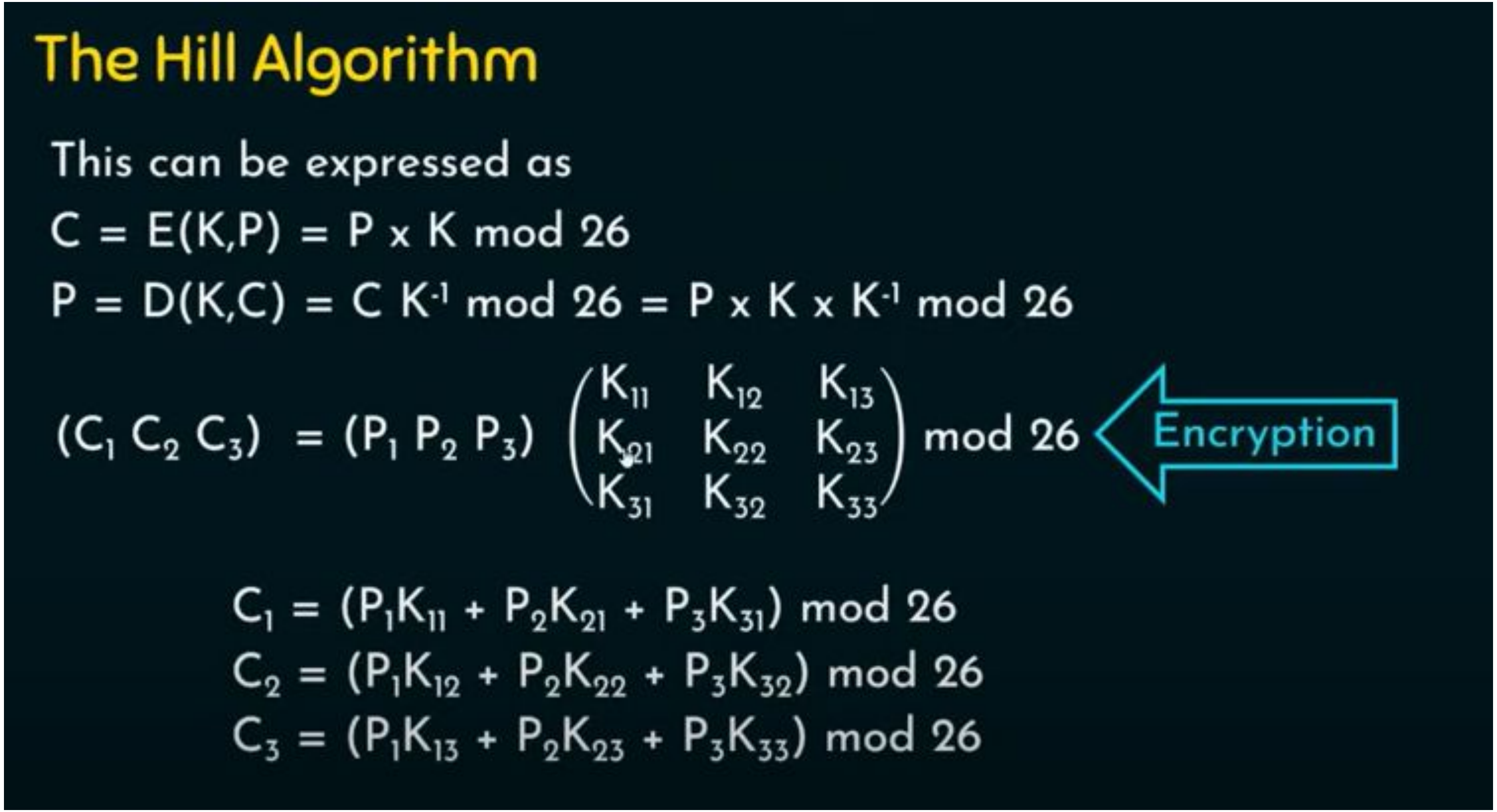
The periodic nature of the keyword can be eliminated by using a nonrepeating keyword that is as long as the message itself. Vigenère proposed what is referred to as an **autokey system**, in which a keyword is concatenated with the plaintext itself to provide a running key. For our example,



```
key:          deceptivewearediscoveredsav
plaintext:    wearediscoveredsaveyourself
ciphertext:   ZICVTWQNGKZEIIGASXSTSLVVWLA
```

HILL CIPHER

- Another interesting multiletter cipher is the Hill cipher, developed by the mathematician Lester Hill in 1929.
- M This encryption algorithm takes m successive plaintext letters and substitutes for them m ciphertext letters. The substitution is determined by m linear equations in which each character is assigned a numerical value (a = 0, b = 1, c , z = 25). For m = 3, the system can be described as



The Hill Algorithm

This can be expressed as

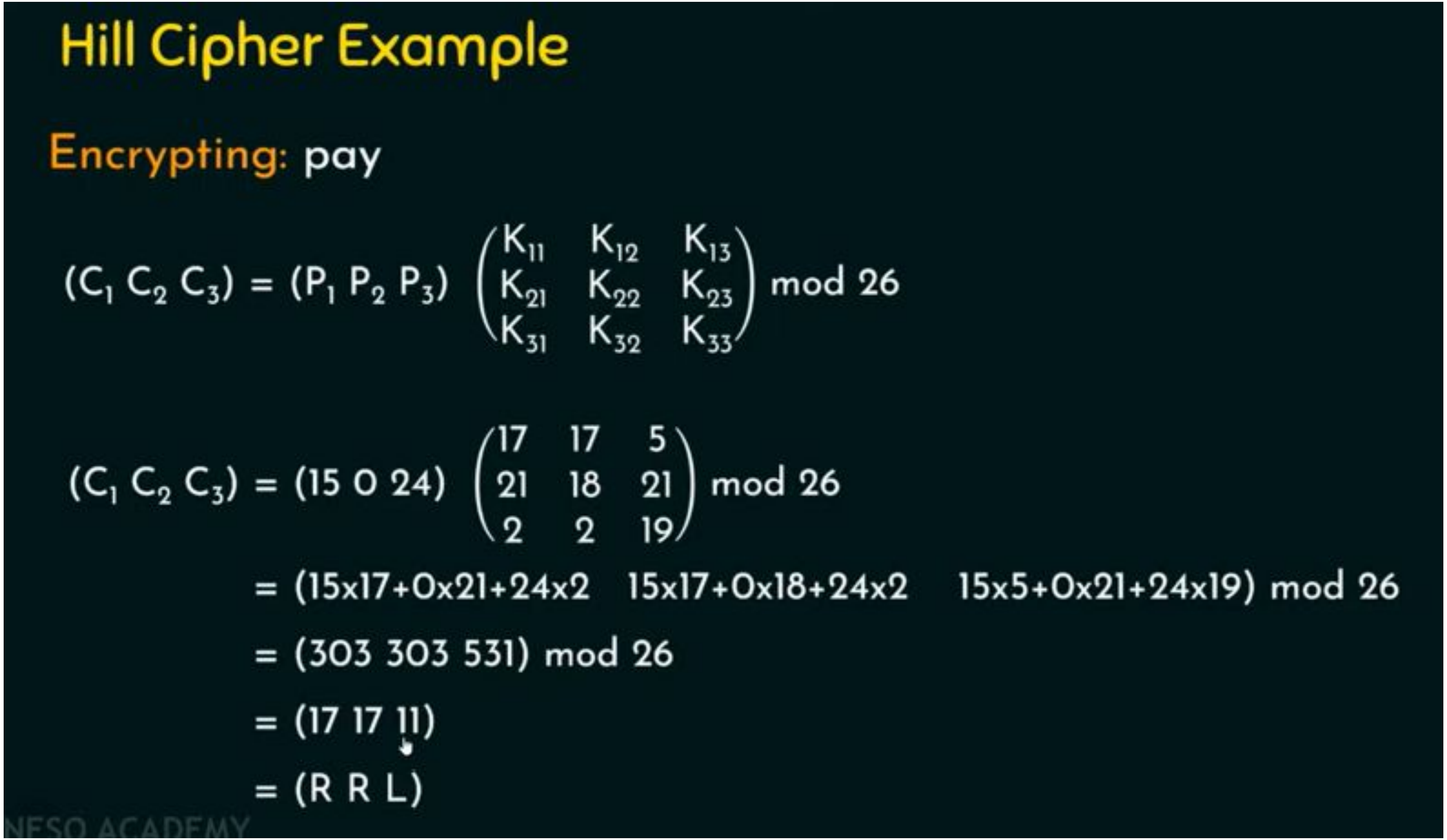
$C = E(K,P) = P \times K \bmod 26$

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

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

Encryption

$$C_1 = (P_1K_{11} + P_2K_{21} + P_3K_{31}) \bmod 26$$
$$C_2 = (P_1K_{12} + P_2K_{22} + P_3K_{32}) \bmod 26$$
$$C_3 = (P_1K_{13} + P_2K_{23} + P_3K_{33}) \bmod 26$$



Hill Cipher Example

Encrypting: pay

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

$$(C_1\ C_2\ C_3) = (15\ 0\ 24)\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \bmod 26$$

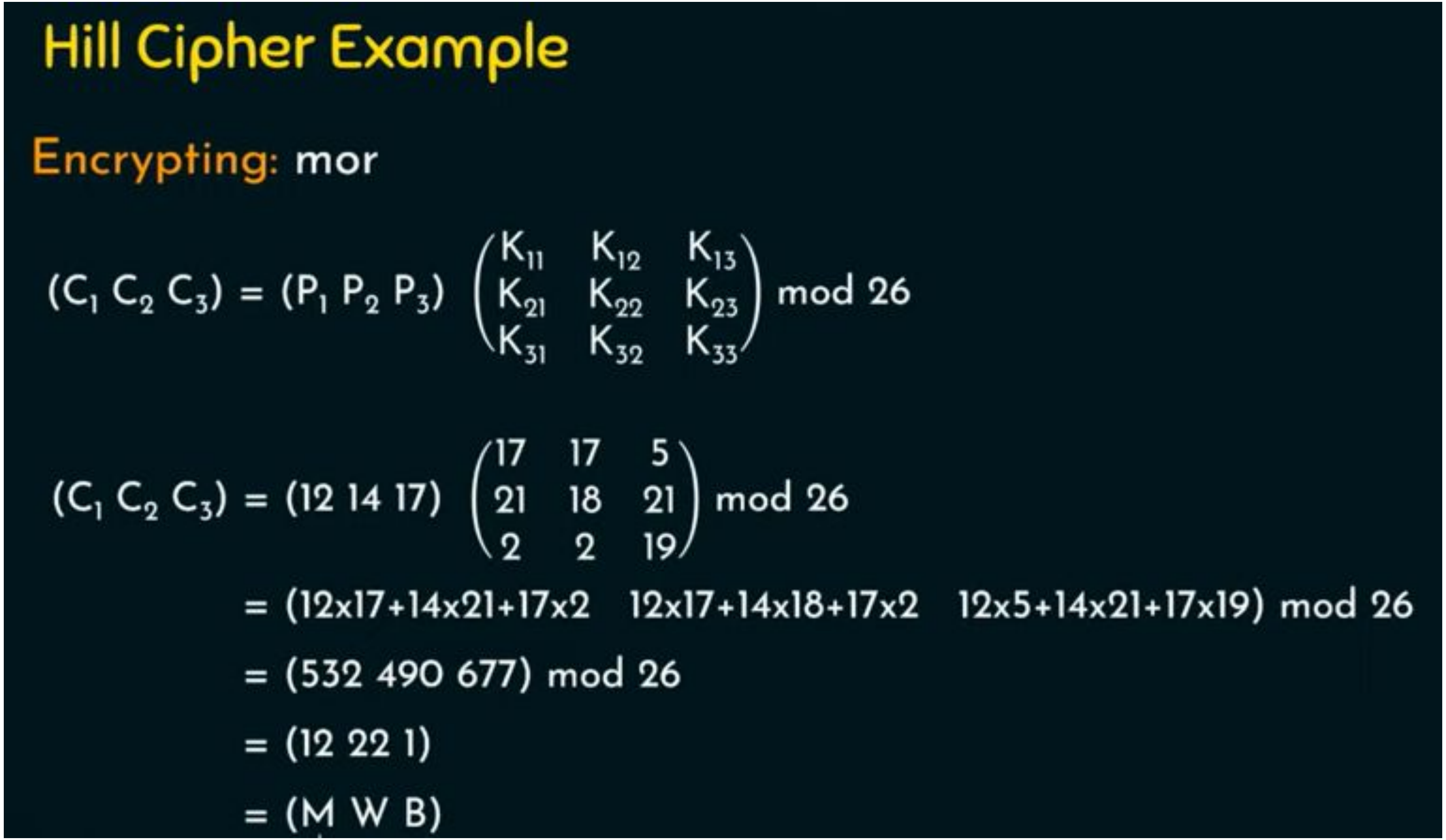
$$= (15x17+0x21+24x2 \quad 15x17+0x18+24x2 \quad 15x5+0x21+24x19) \bmod 26$$

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

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

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

NESO ACADEMY



Hill Cipher Example

Encrypting: mor

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

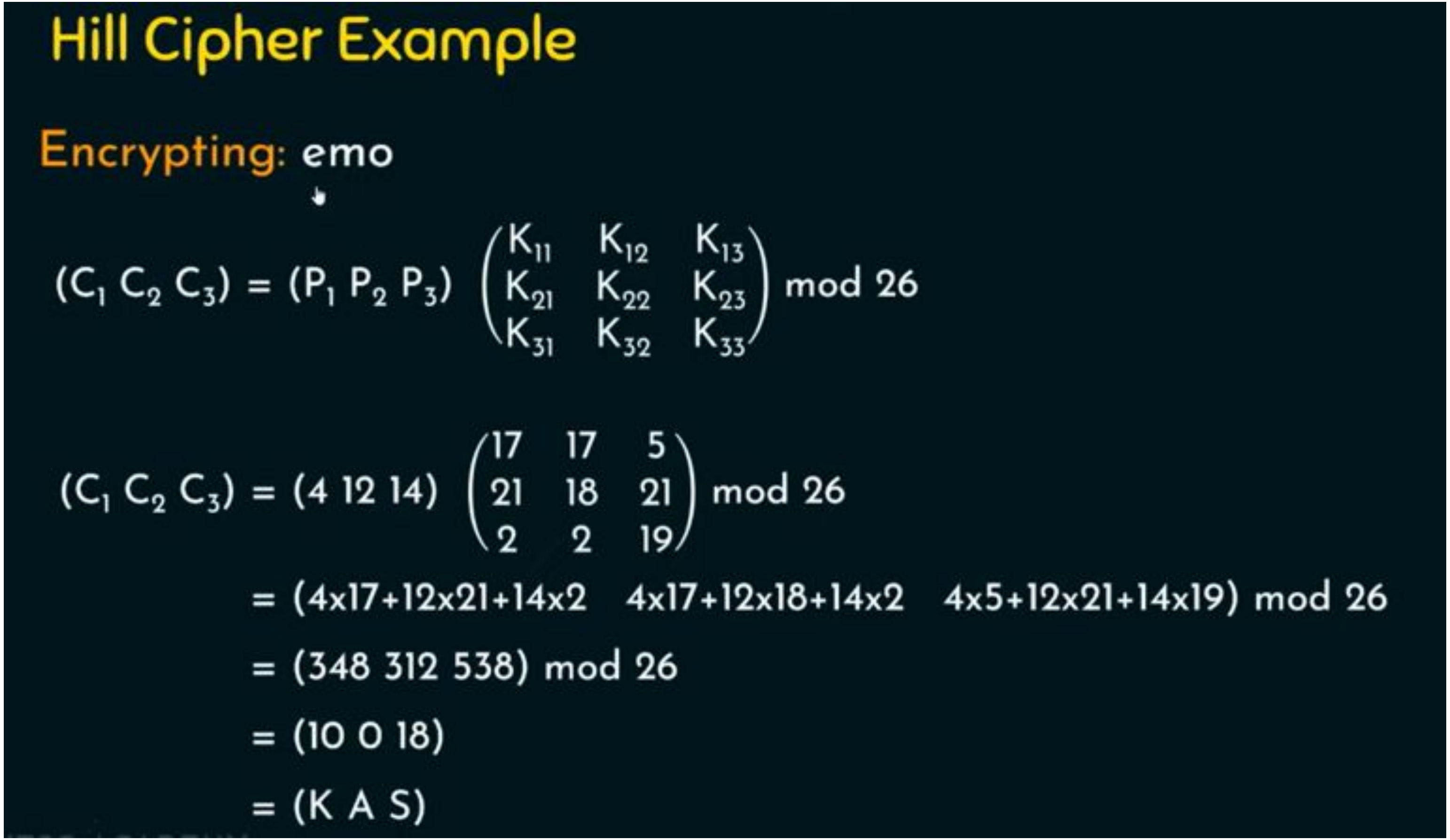
$$(C_1\ C_2\ C_3) = (12\ 14\ 17) \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \text{mod } 26$$

$$= (12\text{x}17+14\text{x}21+17\text{x}2 \quad 12\text{x}17+14\text{x}18+17\text{x}2 \quad 12\text{x}5+14\text{x}21+17\text{x}19) \text{ mod } 26$$

$$= (532\ 490\ 677) \text{ mod } 26$$

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

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



Hill Cipher Example

Encrypting: emo

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

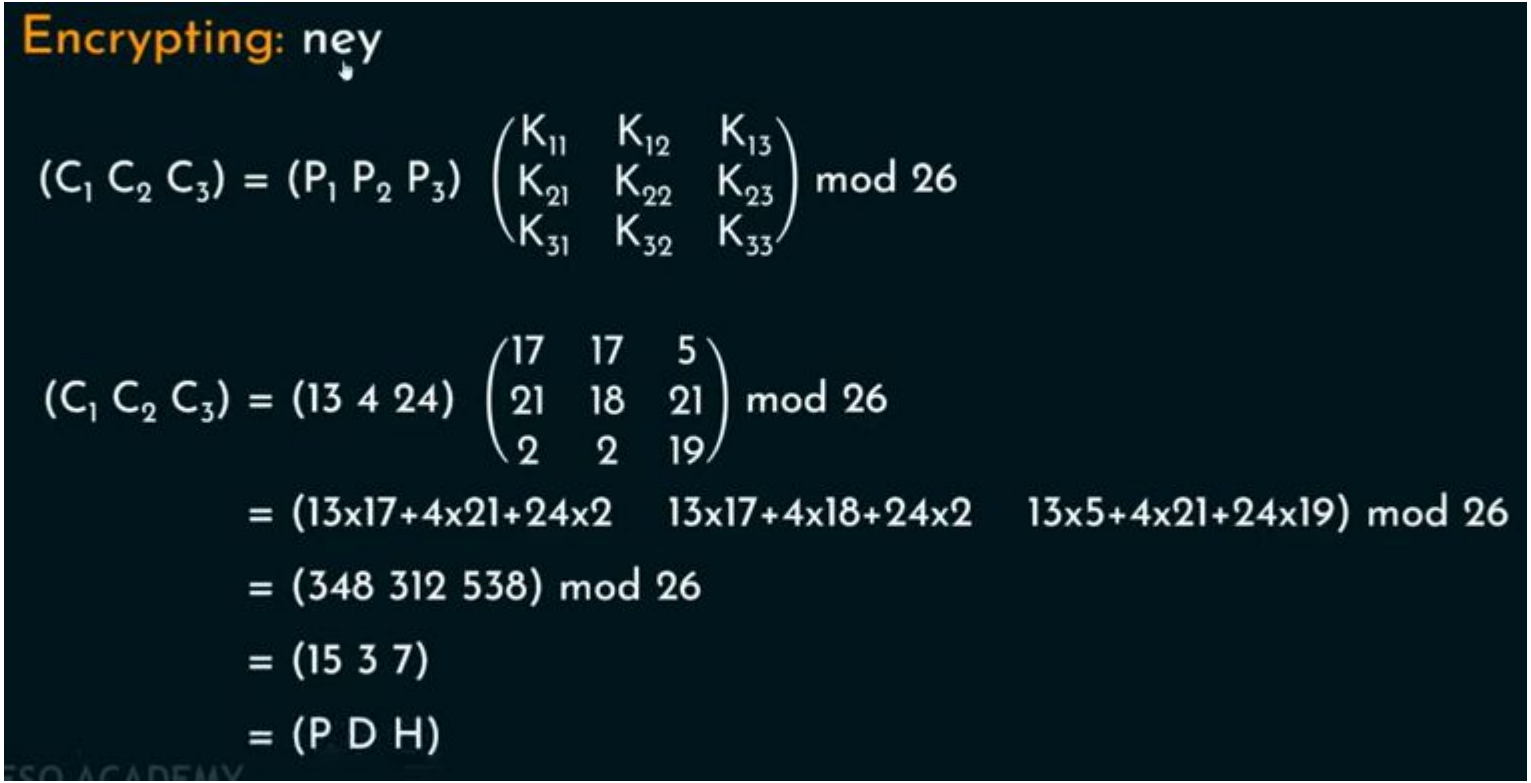
$$(C_1\ C_2\ C_3) = (4\ 12\ 14)\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \bmod 26$$

$$= (4\text{x}17+12\text{x}21+14\text{x}2 \quad 4\text{x}17+12\text{x}18+14\text{x}2 \quad 4\text{x}5+12\text{x}21+14\text{x}19) \bmod 26$$

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

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

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



Encrypting: ney

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

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

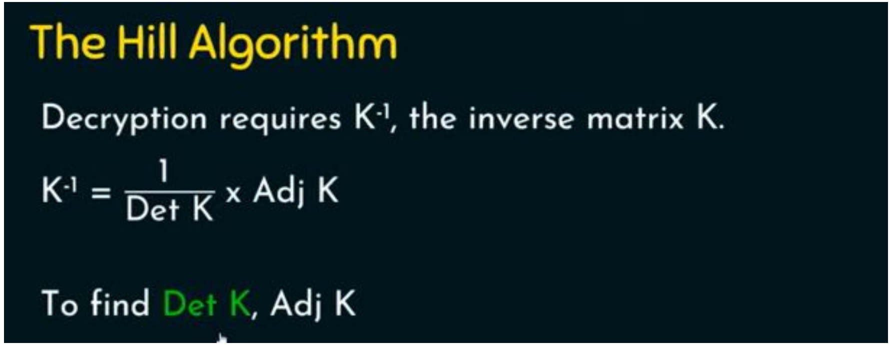
$$= (13\text{x}17+4\text{x}21+24\text{x}2 \quad 13\text{x}17+4\text{x}18+24\text{x}2 \quad 13\text{x}5+4\text{x}21+24\text{x}19) \bmod 26$$

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

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

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

ESO ACADEMY

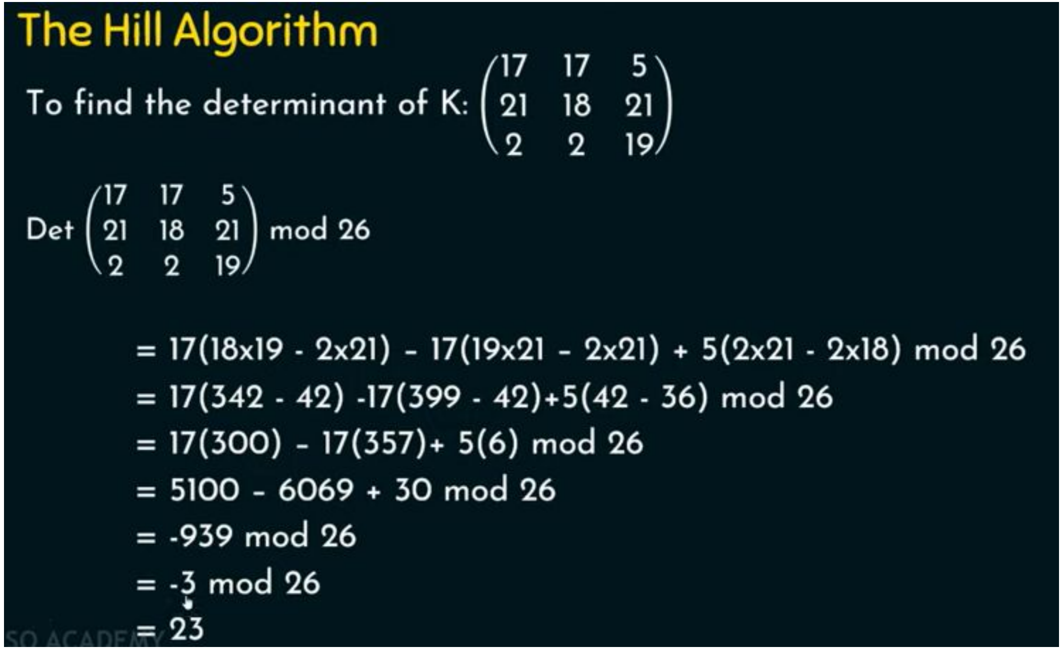


The Hill Algorithm

Decryption requires K^{-1}, the inverse matrix K.

$$K^{-1} = \frac{1}{\text{Det } K} \times \text{Adj } K$$

To find Det K, Adj K



The Hill Algorithm

To find the determinant of K: $\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$

$$\text{Det} \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \bmod 26$$

$$= 17(18\text{x}19 - 2\text{x}21) - 17(19\text{x}21 - 2\text{x}21) + 5(2\text{x}21 - 2\text{x}18) \bmod 26$$

$$= 17(342 - 42) -17(399 - 42)+5(42 - 36) \bmod 26$$

$$= 17(300) - 17(357)+ 5(6) \bmod 26$$

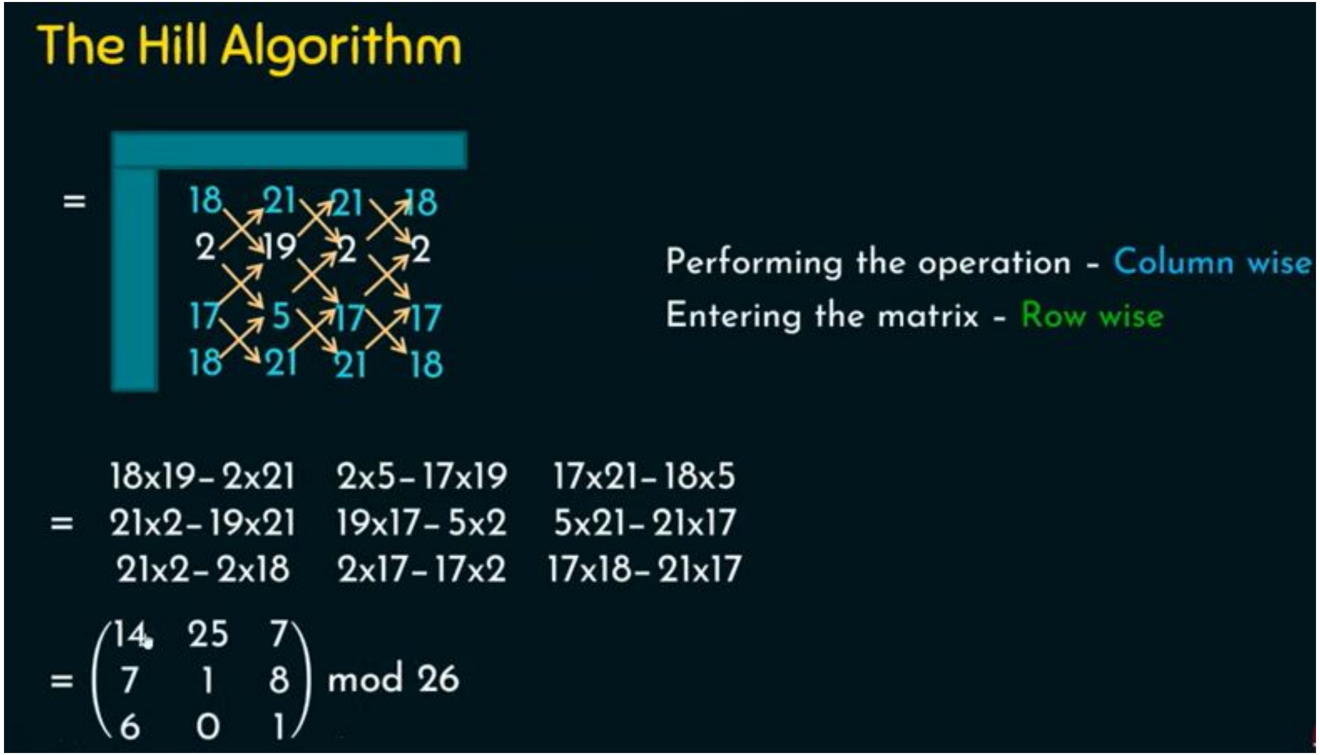
$$= 5100 - 6069 + 30 \bmod 26$$

$$= -939 \bmod 26$$

$$= -3 \bmod 26$$

$$= 23$$

SO ACADEMY



The Hill Algorithm

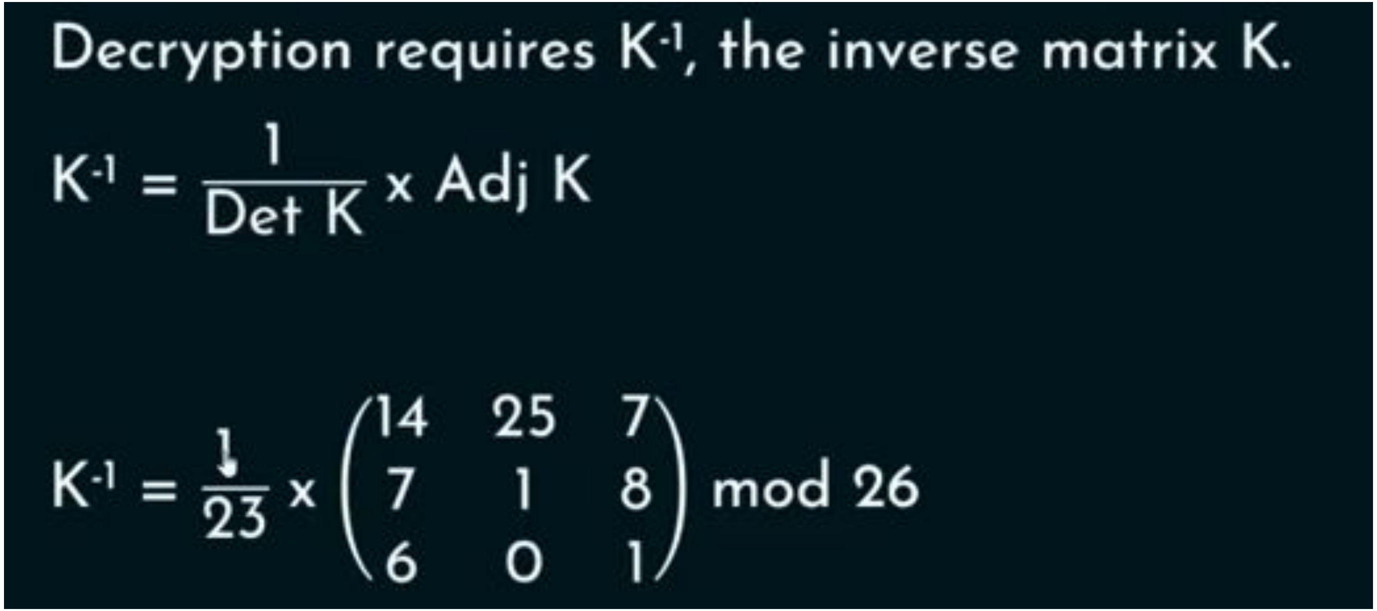
$$= \begin{array}{cccc} 18 & 21 & 21 & 18 \\ 2 & 19 & 2 & 2 \\ 17 & 5 & 17 & 17 \\ 18 & 21 & 21 & 18 \end{array}$$

Performing the operation - Column wise

Entering the matrix - Row wise

$$= \begin{array}{ccc} 18\text{x}19-2\text{x}21 & 2\text{x}5-17\text{x}19 & 17\text{x}21-18\text{x}5 \\ 21\text{x}2-19\text{x}21 & 19\text{x}17-5\text{x}2 & 5\text{x}21-21\text{x}17 \\ 21\text{x}2-2\text{x}18 & 2\text{x}17-17\text{x}2 & 17\text{x}18-21\text{x}17 \end{array}$$

$$= \begin{pmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{pmatrix} \text{mod } 26$$



Decryption requires K^{-1}, the inverse matrix K.

$$K^{-1} = \frac{1}{\text{Det } K} \times \text{Adj } K$$

$$K^{-1} = \frac{1}{23} \times \begin{pmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{pmatrix} \bmod 26$$

VERNAM CIPHER

The ultimate defense against such a cryptanalysis is to choose a keyword that is as long as the plaintext and has no statistical relationship to it. Such a system was introduced by an AT&T engineer named Gilbert Vernam in 1918.

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

$$ci = pi \oplus ki$$

where pi = ith binary digit of plaintext

ki = ith binary digit of key ci = ith binary digit of ciphertext

$\oplus$ = exclusive@or (XOR) operation

$$pi = ci \oplus ki$$

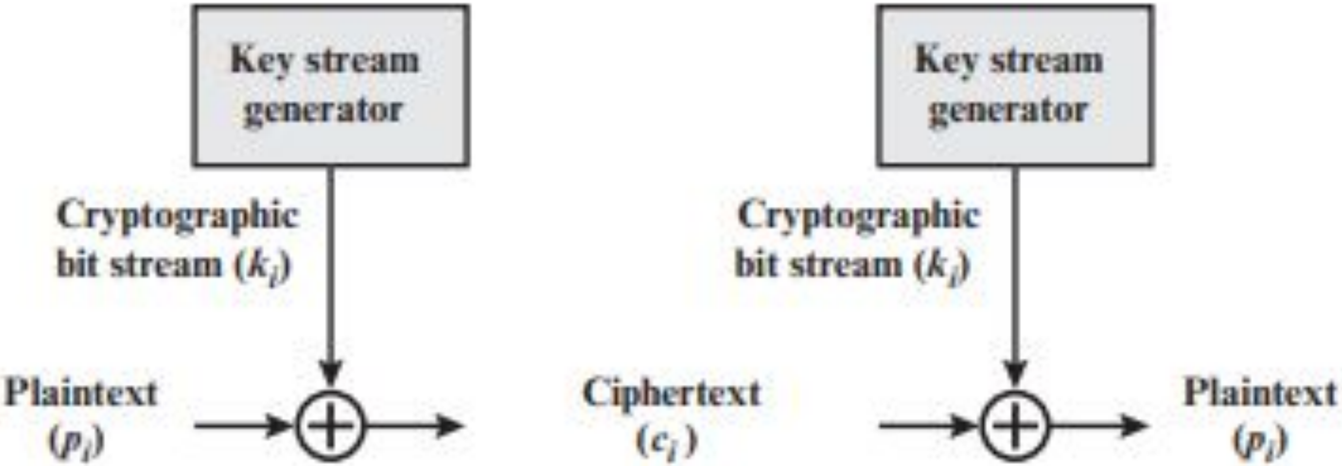
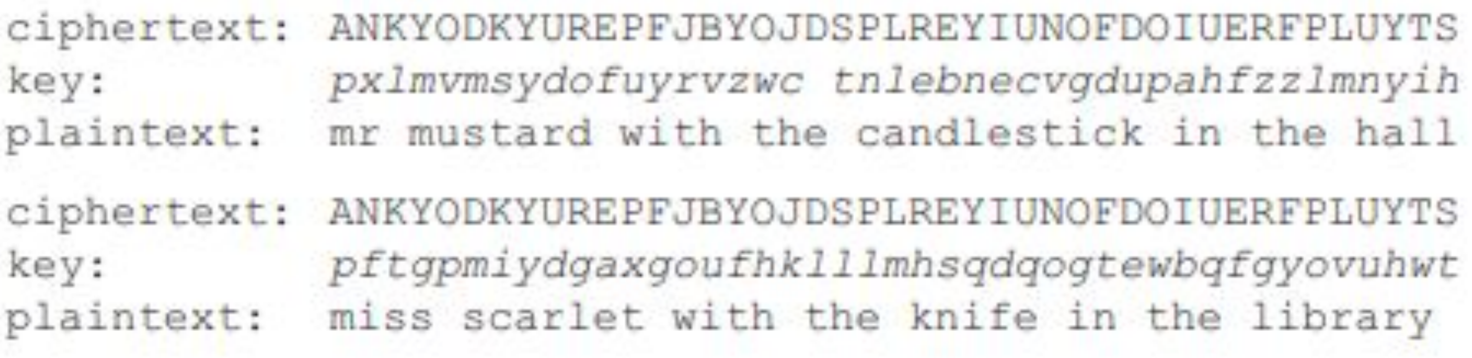


Figure 3.7 Vernam Cipher

ONE TIME PAD

- An Army Signal Corp officer, Joseph Mauborgne, proposed an improvement to the Vernam cipher that yields the ultimate in security.
- Mauborgne suggested using a random key that is as long as the message, so that the key need not be repeated.
- In addition, the key is to be used to encrypt and decrypt a single message, and then is discarded.
- Each new message requires a new key of the same length as the new message.
- Such a scheme, known as a one-time pad, is unbreakable. It

ONE TIME PAD

- It produces random output that bears no statistical relationship to the plaintext.
- Because the ciphertext contains no information whatsoever about the plaintext, there is simply no way to break the code.
- 

```
ciphertext: ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS
key:        pxlmvmsydofuyrvzwc tnlebnecvgdupahfzzlmnyih
plaintext:  mr mustard with the candlestick in the hall

ciphertext: ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS
key:        pftgpmiydgaxgoufhklllmhsqdqogtewbqfgyovuhwt
plaintext:  miss scarlet with the knife in the library
```

ONE TIME PAD

The one-time pad offers complete security but, in practice, has two fundamental difficulties:

- There is the practical problem of making large quantities of random keys. Any heavily used system might require millions of random characters on a regular basis. Supplying truly random characters in this volume is a significant task.
- Even more daunting is the problem of key distribution and protection. For every message to be sent, a key of equal length is needed by both sender and receiver. Thus, a mammoth key distribution problem exists.

Because of these difficulties, the one-time pad is of limited utility and is useful primarily for low-bandwidth channels requiring very high security.

The one-time pad is the only cryptosystem that exhibits what is referred to as **perfect secrecy**.

TRANSPOSITION CIPHER

- So far, all the ciphers we’ve discussed are substitution ciphers, in which plaintext letters are replaced by ciphertext letters.
- Changing the positions of plaintext letters is another enciphering technique. It’s called **transposition**, as in transferring position.
- \Many newspapers have transposition puzzles called “jumbles.”
- A simple transposition of FIVE AM moves each letter one position to the left. FIVE AM is encrypted to IVEA MF.
- Although the letters have been moved around, all the ciphertext letters are the same as the plaintext letters. There’s no replacement or substitution of letters.

RAIL FENCE CIPHER

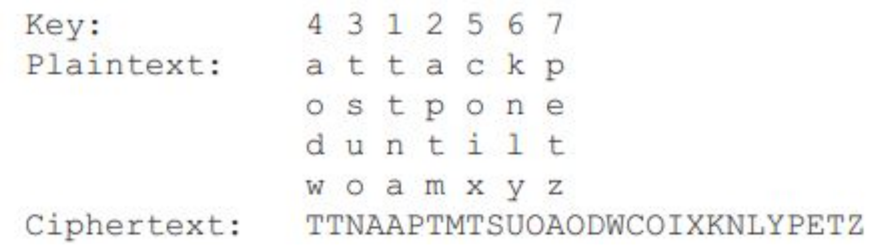
- The simplest such cipher is the Rail Fence technique, in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.
- It is also known as Keyless Transposition Cipher
- For example, to encipher the message “meet me after the toga party” with a rail fence of depth 2, we write the following:

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

- The encrypted message is MEMATRHTGPRYETEFETEOAAT

COLUMNAR 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.
- This is called Keyed Transposition Cipher. The order of the columns then becomes the key to the algorithm. For example,

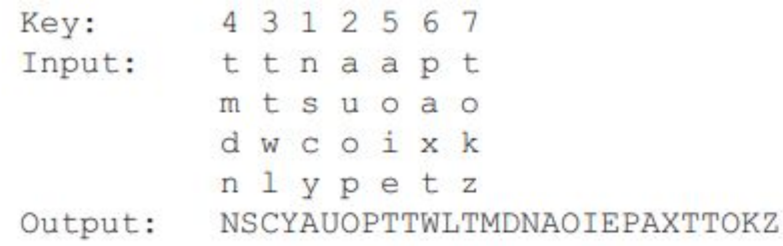


```
Key:           4 3 1 2 5 6 7
Plaintext:     a t t a c k p
               o s t p o n e
               d u n t i l t
               w o a m x y z
Ciphertext:    TTNAAPTMTSUOAODWCOIXKNLYPETZ
```

- Thus, in this example, the key is 4312567. To encrypt, start with the column that is labeled 1, in this case column 3. Write down all the letters in that column. Proceed to column 4, which is labeled 2, then column 2, then column 1, then columns 5, 6, and 7

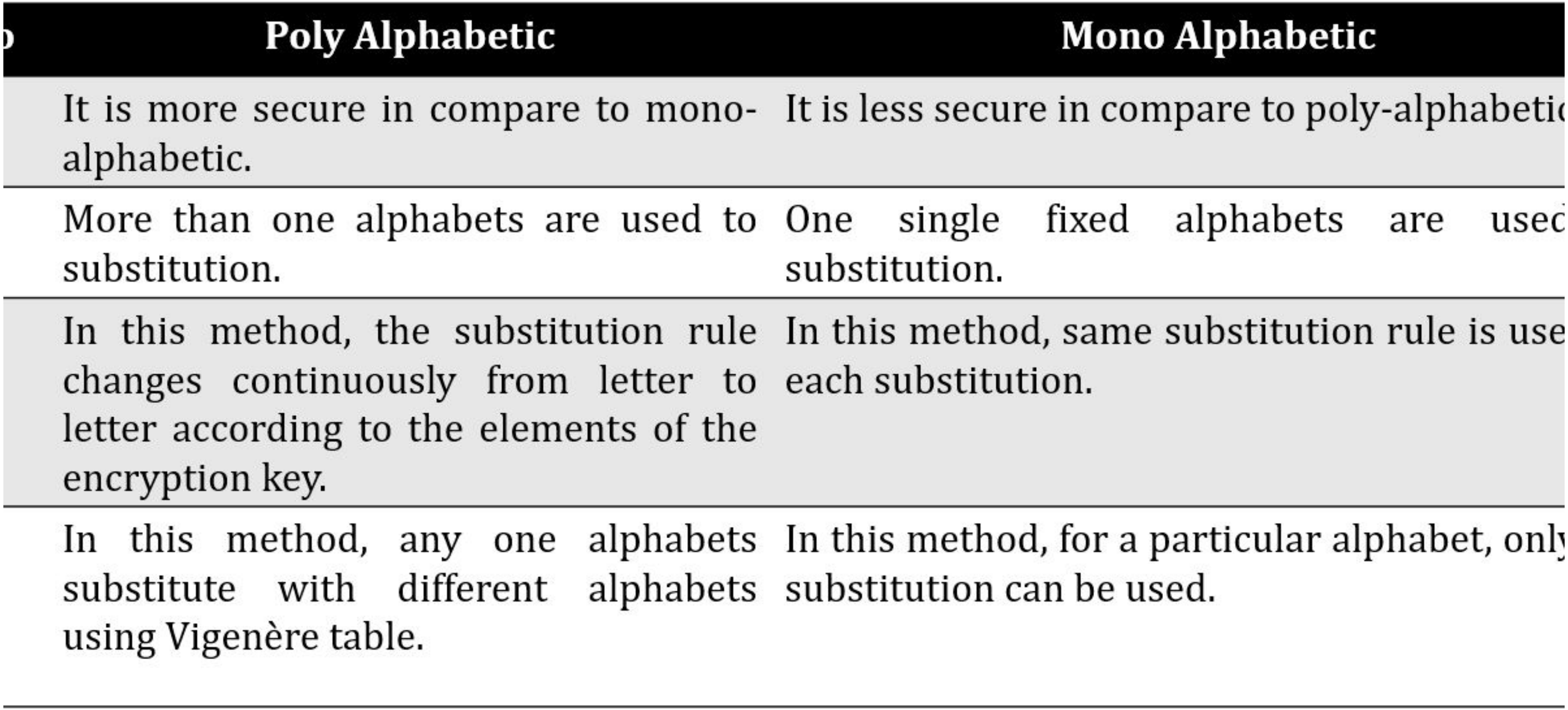
COLUMNAR TRANSPOSITION CIPHER

- The transposition cipher can be made significantly more secure by performing more than one stage of transposition.
- The result is a more complex permutation that is not easily reconstructed. Thus, if the foregoing message is re-encrypted using the same algorithm then the output is



```
Key:       4 3 1 2 5 6 7
Input:     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
Output:    NSCYAUOPTTWLTMDNAOIEPAXTTOKZ
```

DIFFERENCE IN MONO-ALPHABETIC & POLYALPHABETIC CIPHER



o	Poly Alphabetic	Mono Alphabetic
	It is more secure in compare to mono-alphabetic.	It is less secure in compare to poly-alphabetic
	More than one alphabets are used to substitution.	One single fixed alphabets are used substitution.
	In this method, the substitution rule changes continuously from letter to letter according to the elements of the encryption key.	In this method, same substitution rule is use each substitution.
	In this method, any one alphabets substitute with different alphabets using Vigenère table.	In this method, for a particular alphabet, only substitution can be used.

STEGANOGRAPHY

- A plaintext message may be hidden in one of two ways. The methods of steganography conceal the existence of the message, whereas the methods of cryptography render the message unintelligible to outsiders by various transformations of the text.
- A simple form of steganography, but one that is time-consuming to construct, is one in which an arrangement of words or letters within an apparently innocuous text spells out the real message.
- Various other techniques have been used historically; some examples are the following:

■ Character marking: Selected letters of printed or typewritten text are overwritten 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 visible unless the paper is held up in front of a light.

STEGANOGRAPHY

Steganography has a number of drawbacks when compared to encryption:

- It requires a lot of overhead to hide a relatively few bits of information.
- Also, once the system is discovered, it becomes virtually worthless.

- **Alternatively, a message can be first encrypted and then hidden using steganography.**

CRYPTANALYSIS

- **Cryptology** has two parts namely, **Cryptography** which focuses on creating secret codes and **Cryptanalysis** which is the study of the cryptographic algorithm and the breaking of those secret codes.
- The person practicing Cryptanalysis is called a **Cryptanalyst**. It helps us to better understand the cryptosystems and also helps us improve the system by finding any weak point and thus work on the algorithm to create a more secure secret code.
- To determine the weak points of a cryptographic system, it is important to attack the system. This attacks are called **Cryptanalytic attacks.**
- The attacks rely on nature of the algorithm and also knowledge of the general characteristics of the plaintext, i.e., plaintext can be a regular document written in English or it can be a code written in Java.
- Therefore, nature of the plaintext should be known before trying to use the attacks.

Type of Attack	**Known to Cryptanalyst**
Cipher text only	• Encryption algorithm • Cipher text to be decoded
Known plain text	• Encryption algorithm • Cipher text to be decoded • One or more plain text-cipher text pairs formed with the secret key
Chosen plain text	• Encryption algorithm • Cipher text to be decoded • Plain text message chosen by cryptanalyst, together with its corresponding cipher text generated with the secret key
Chosen cipher text	• Encryption algorithm • Cipher text to be decoded • The purported cipher text chosen by cryptanalyst, together with its corresponding decrypted plain text generated with the secret key
Chosen text	• Encryption algorithm • Cipher text to be decoded • Plain text message chosen by cryptanalyst, together with its corresponding cipher text generated with the secret key • The purported cipher text chosen by cryptanalyst, together with its corresponding decrypted plain text generated with the secret key

CRYPTANALYSIS

- **Ciphertext only:** In this type of attack, only some cipher-text is known and the attacker tries to find the corresponding encryption key and plaintext. Its the hardest to implement but is the most probable attack as only ciphertext is required. It is the most difficult attack for cryptanalyst and most eastiest for us to defend.
- **Known-Plaintext Analysis (KPA) :** In this type of attack, some plaintext-ciphertext pairs are already known. Attacker maps them in order to find the encryption key. This attack is easier to use as a lot of information is already available.
- **Chosen-Plaintext Analysis (CPA) :** In this type of attack, the attacker chooses random plaintexts and obtains the corresponding ciphertexts and tries to find the encryption key. Its very simple to implement like KPA but the success rate is quite low.

CRYPTANALYSIS

- **Chosen-Ciphertext Analysis (CPA)**During the chosen-ciphertext attack, a cryptanalyst can analyse any chosen ciphertexts together with their corresponding plaintexts. His goal is to acquire a secret key or to get as many information about the attacked system as possible.The attacker has capability to make the victim (who obviously knows the secret key) decrypt any ciphertext and send him back the result. By analysing the chosen ciphertext and the corresponding received plaintext, the intruder tries to guess the secret key which has been used by the victim.
- **Chosen Text Analysis:** It is a combination of Chosen Plaintext and Chosen Cipher Text attack