Course Code : ECS401

Course Title : Cryptography and Network Security

Introduction

What is Cryptology, Cryptography & Cryptanalysis?

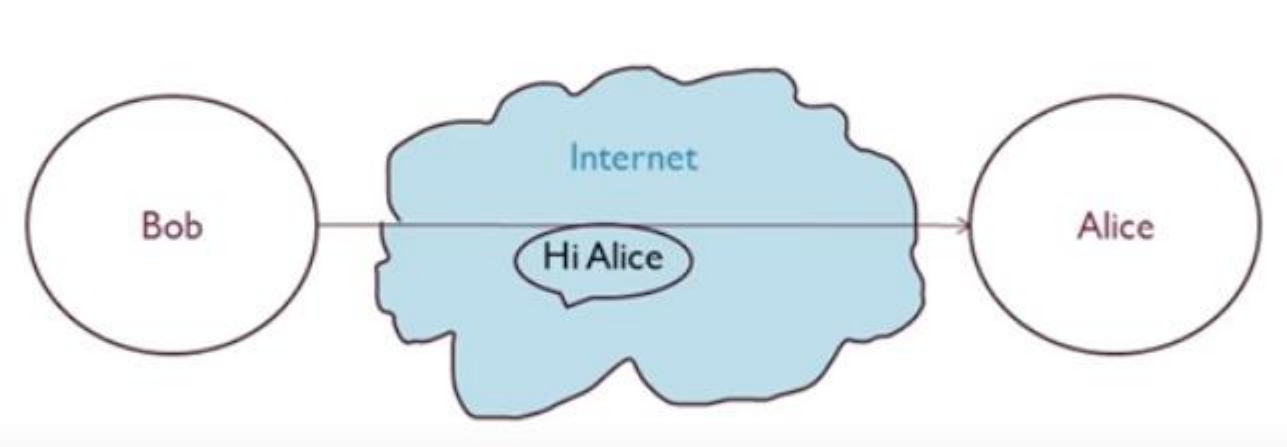
- **Greek word** : *kryptós* = "hidden" and *graphein* = "to write".
- **Cryptology** = "Study of codes, both hiding and solving them"
  = cryptography + cryptanalysis
- **Cryptography** = Art of creating codes
- **Cryptanalysis** = Analyzing or breaking the coded message

Why do we need Cryptography?

- Is Internet secure?

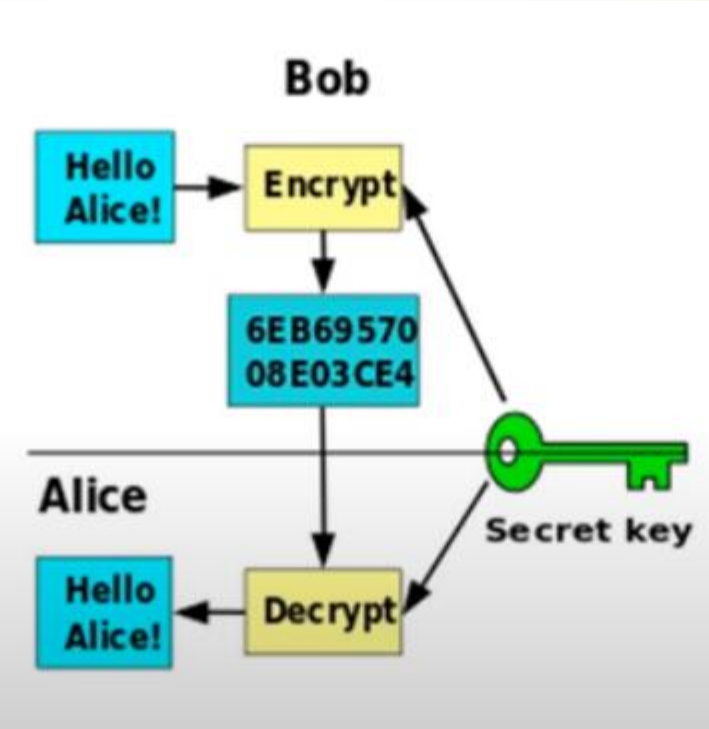
  Obviously NOT.

- Cryptography secures information and communications using a set of rules that allows only intended users to receive the information to access and process it.



What is Cryptography?

- **Cryptography** is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it.



Basic Terminologies

- **Plain Text**

  Is the original message

- **Cipher Text**

  Is the encrypted message

- **Encryption**

  transforming information from readable format into unreadable format

- **Decryption**

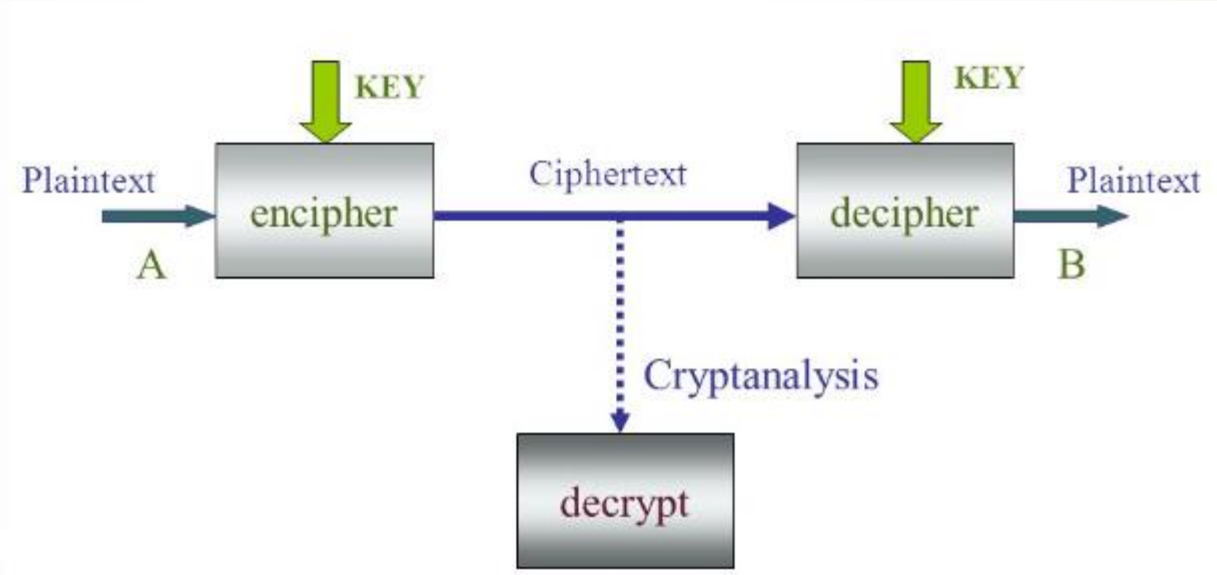
  transforming information from unreadable format to readable format

- **Key**

  a string of bits used by a cryptographic algorithm to transform plain text into cipher text or vice-versa.

What is Cryptanalysis?

- **Greek word :** *kryptós* = "hidden" and *analýein* = ""to loosen" or "untie"
- **Cryptanalysis** is used to breach cryptographic security systems and gain access to the contents of encrypted messages, even if the cryptographic key is unknown.



Security Attacks, Services and Mechanisms

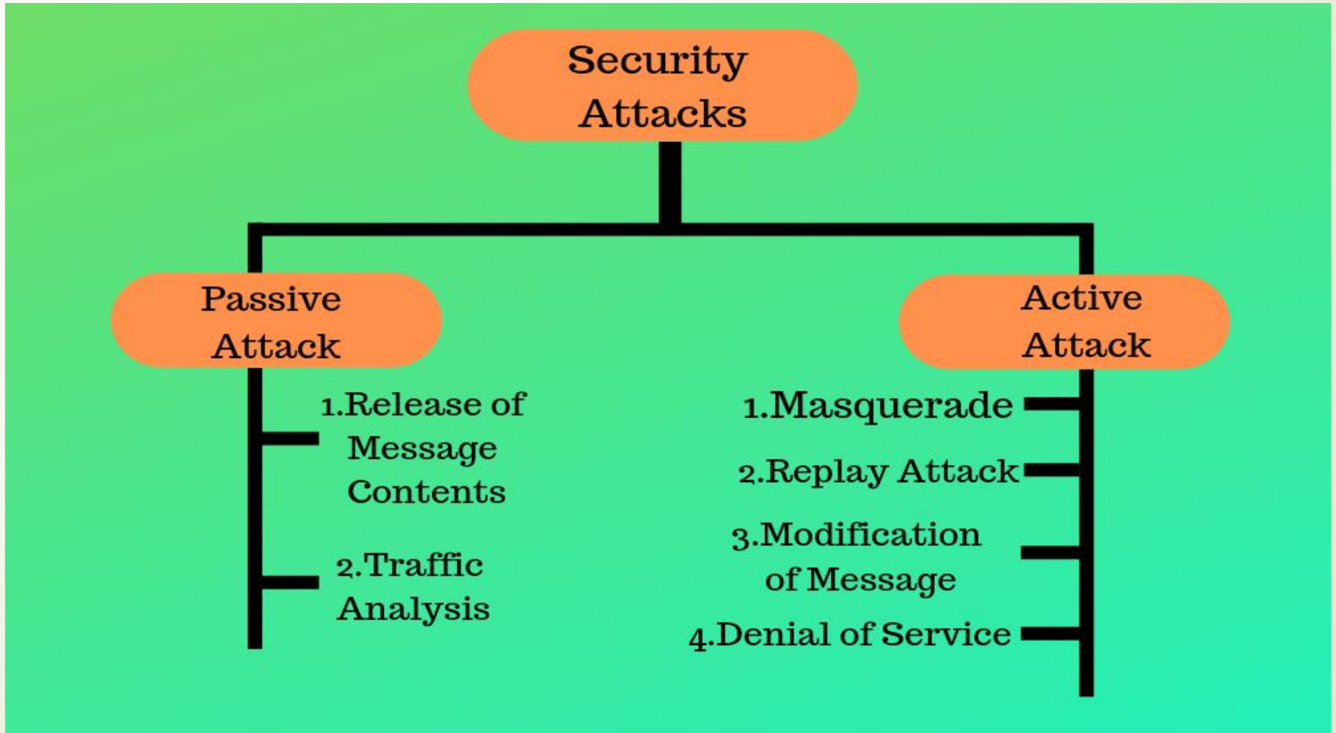
The OSI Security Architecture

- The OSI security architecture focuses on security attacks, mechanisms, and services as defined below:
- **Security Attack**: any action that compromises the security of information.
- **Security Mechanism:** a process that is designed to detect, prevent or recover from a security attack.
- **Security Service:** a processing or communication service that enhances the security of data processing system and information transfer of an organization.

SECURITY ATTACKS

- Two types of Security attacks:

1. **Passive**: A passive attack attempts to learn or make use of information from the system but does not affect system resources.
2. **Active:** An active attack attempts to alter system resources or affect their operation.


Security Attacks

Passive Attack

1.Release of Message Contents

2.Traffic Analysis

Active Attack

1.Masquerade

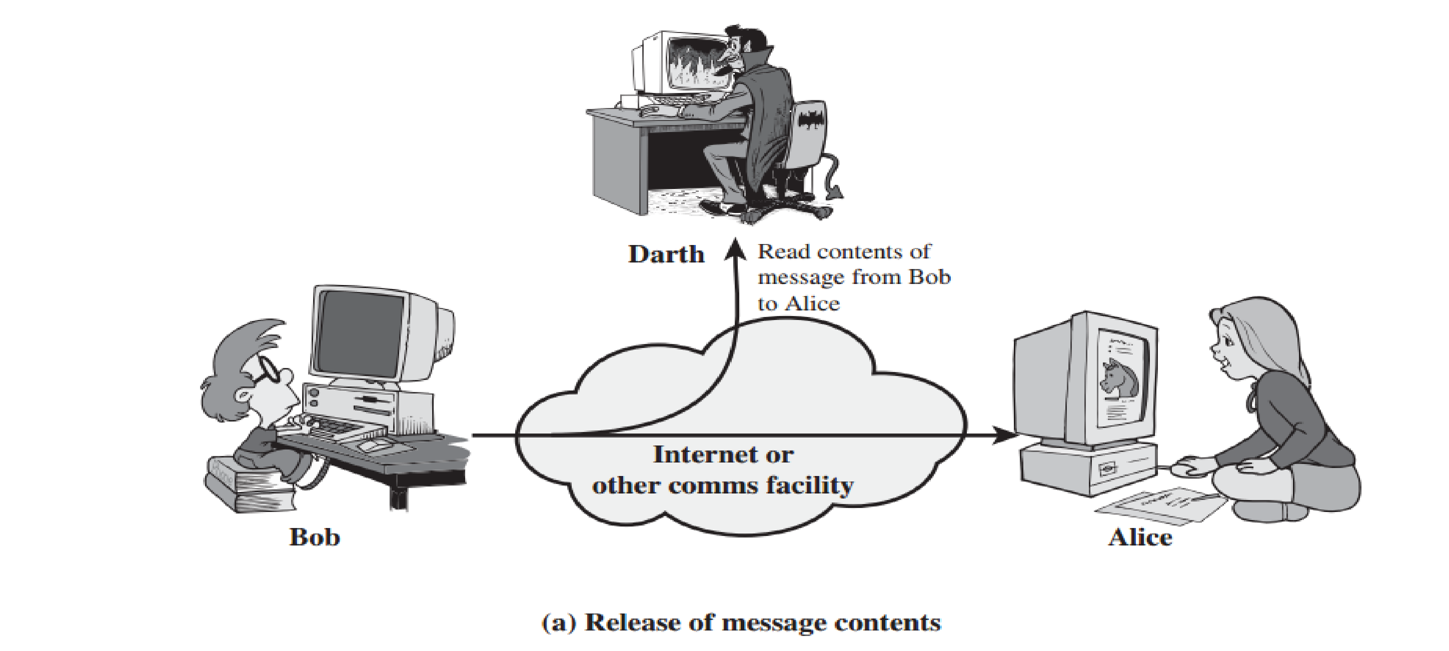
2.Replay Attack

3.Modification of Message

4.Denial of Service

Passive Attacks

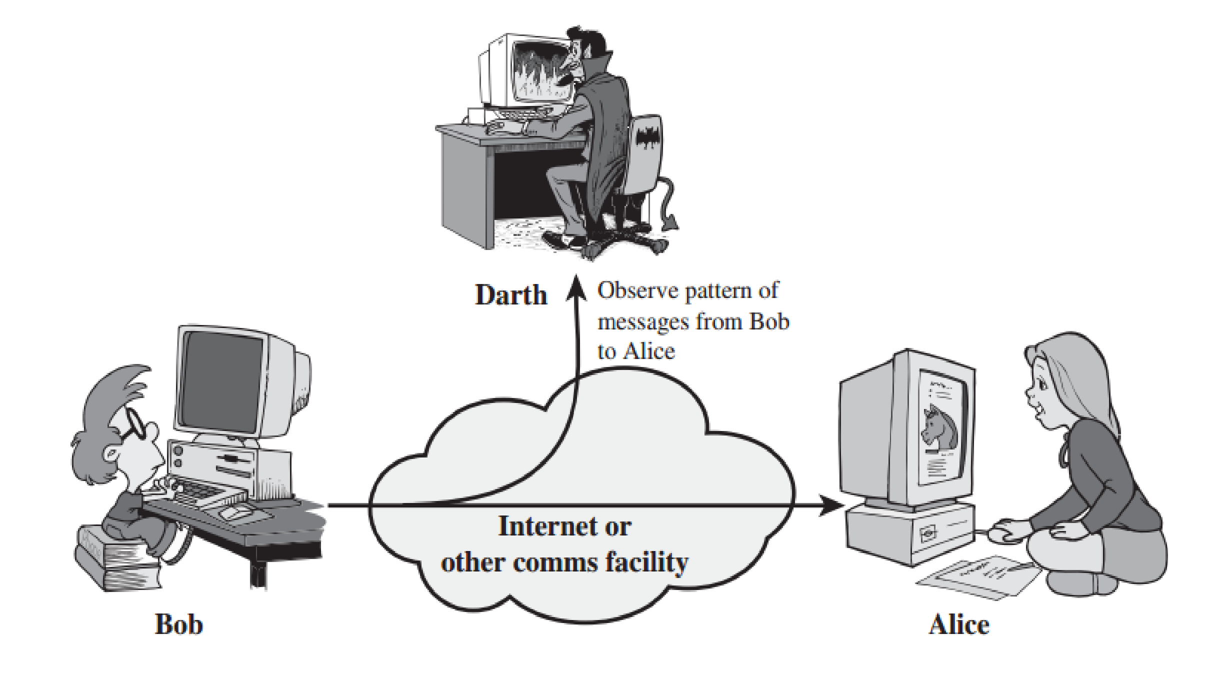
- **Goal:** The goal of the opponent is to obtain information that is being transmitted.
- **Release of message contents:** A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.


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

(a) Release of message contents

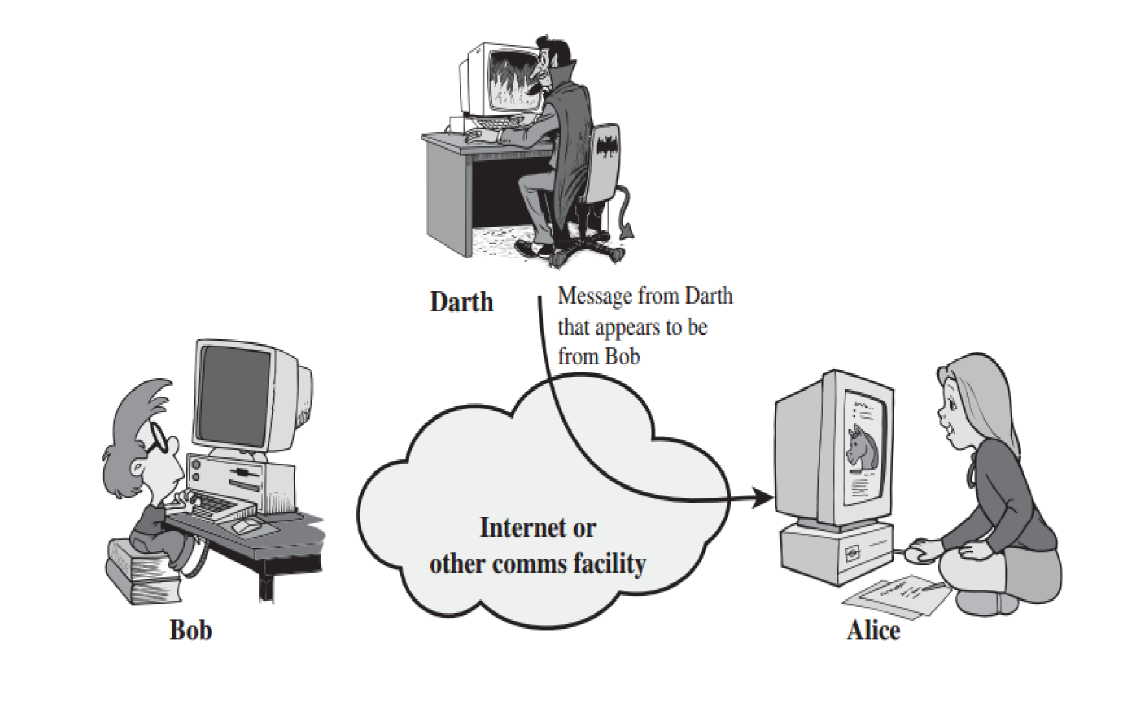
Passive Attacks

- **Traffic Analysis**: In this type, an attacker monitors communication channels to collect a range of information, including message pattern, human and machine identities, locations of these identities and types of encryption used, if applicable.


Darth
Observe pattern of messages from Bob to Alice
Internet or other comms facility
Bob
Alice

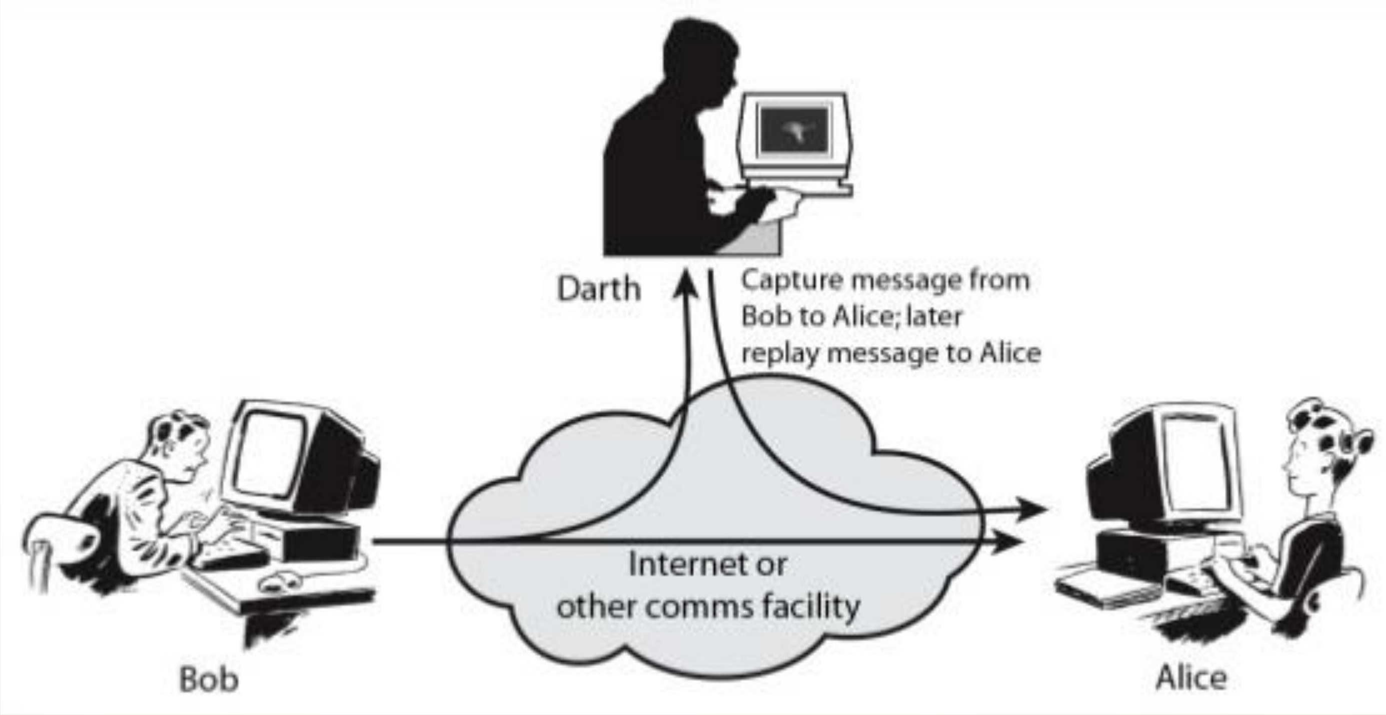
Active Attacks

- **Goal:** is the modification of the data stream or the creation of a false stream.
- **Masquerade:** takes place when one entity pretends to be a different entity.


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

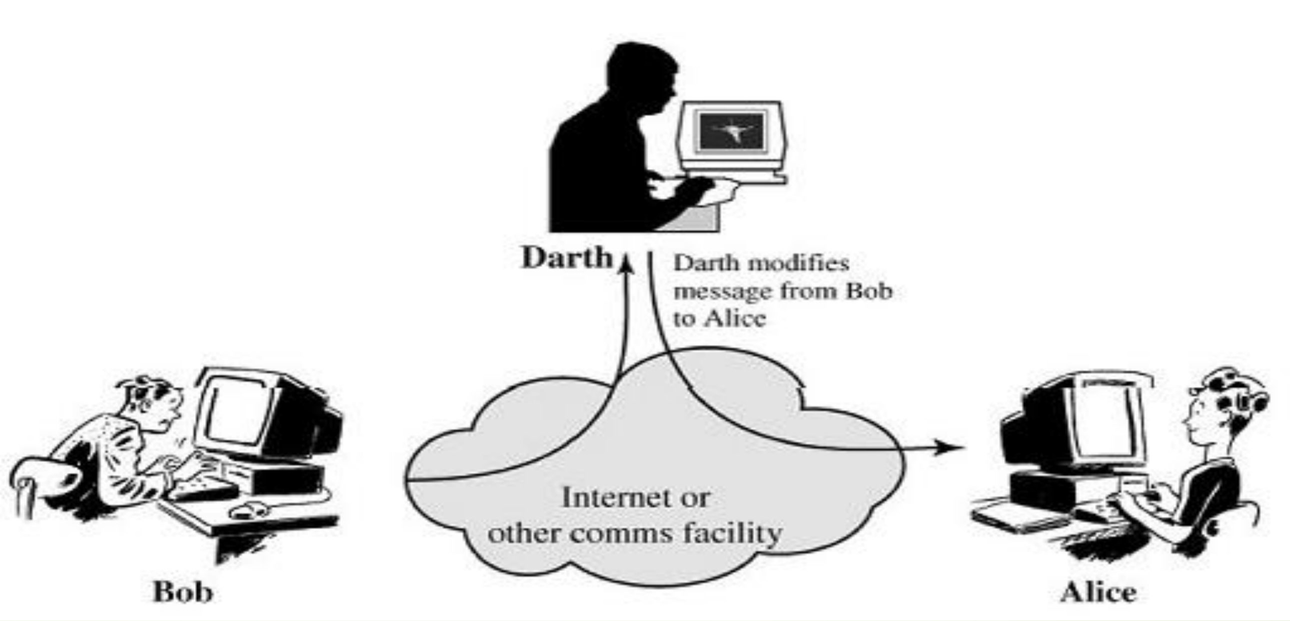
Active Attacks

- **Replay :** involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.


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

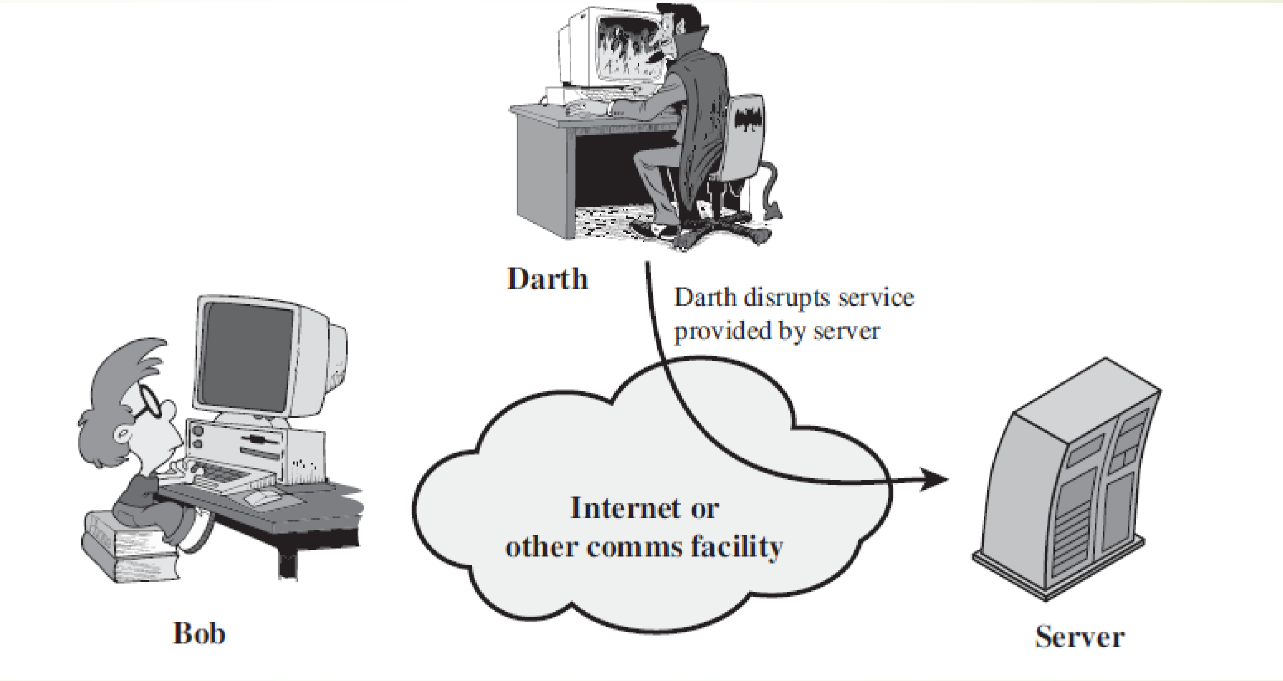
Active Attacks

- **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.


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

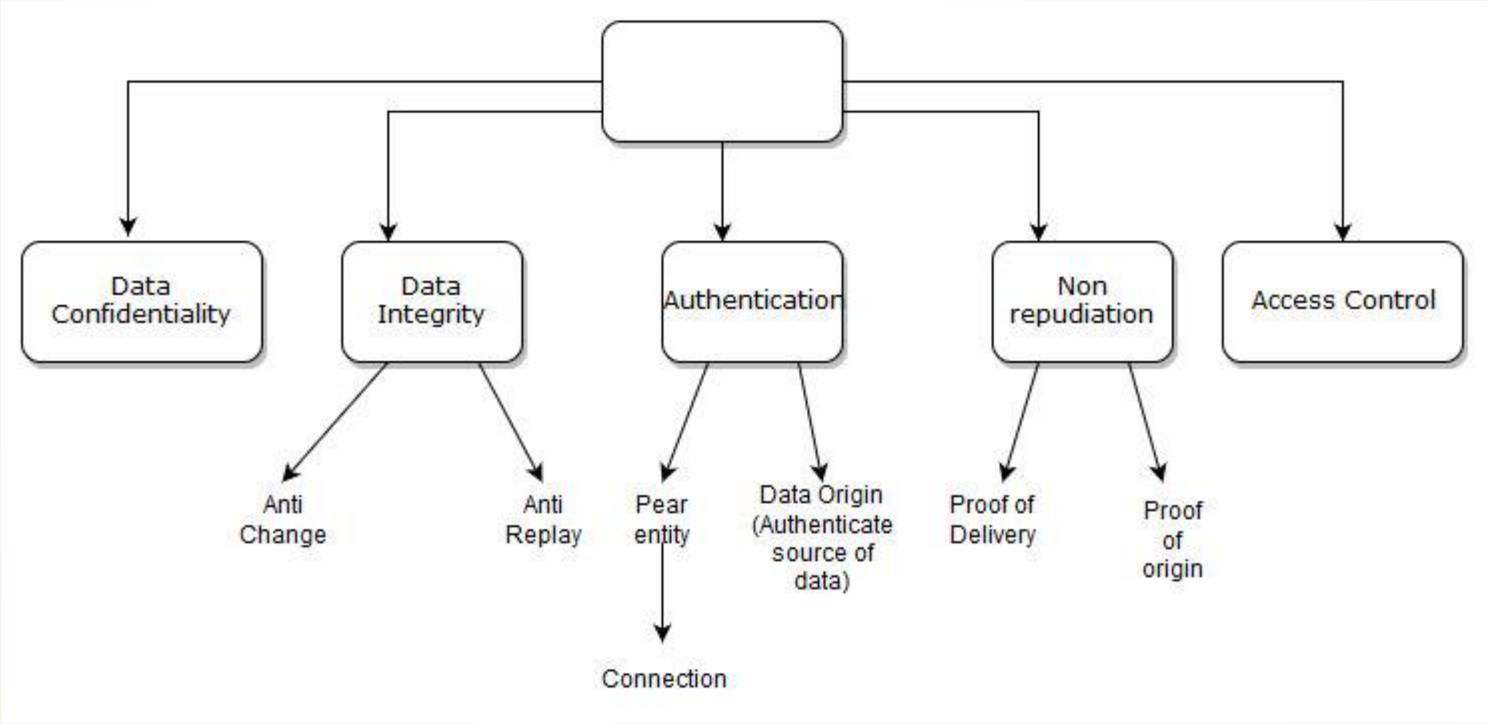
Active Attacks

- **Denial of service:** it prevents or inhibits the normal use or management of communications facilities.


Darth
Darth disrupts service provided by server
Bob
Internet or other comms facility
Server

SECURITY SERVICES

- X.800 security model divides the security services into five categories.



Authentication

- The assurance that the communicating entity is the one that it claims to be.
- Two specific authentication services:
  - **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.
- 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

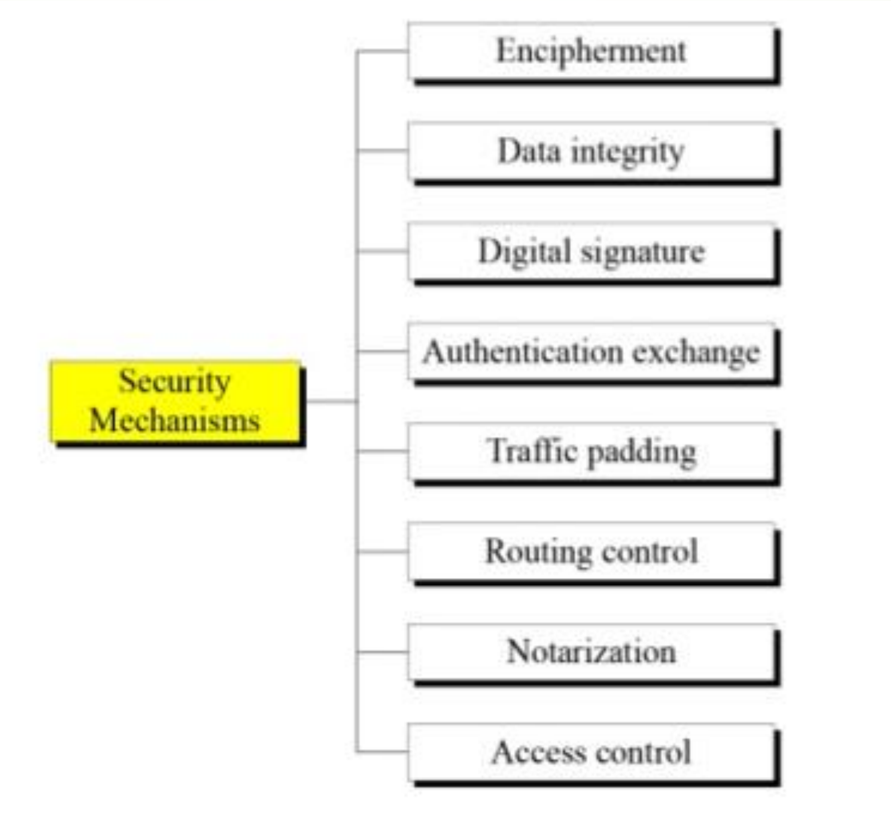
- The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).
- **Connection Integrity with Recovery:** Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data with recovery attempted.
- **Connection Integrity without Recovery:** same 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.
- **Connectionless Integrity:** Provides for the integrity of a single connectionless data block and may take the form of detection of data modification.
- **Selective-Field Connectionless Integrity:** Provides for the integrity of selected fields within a single connectionless data block.

Non-Repudiation

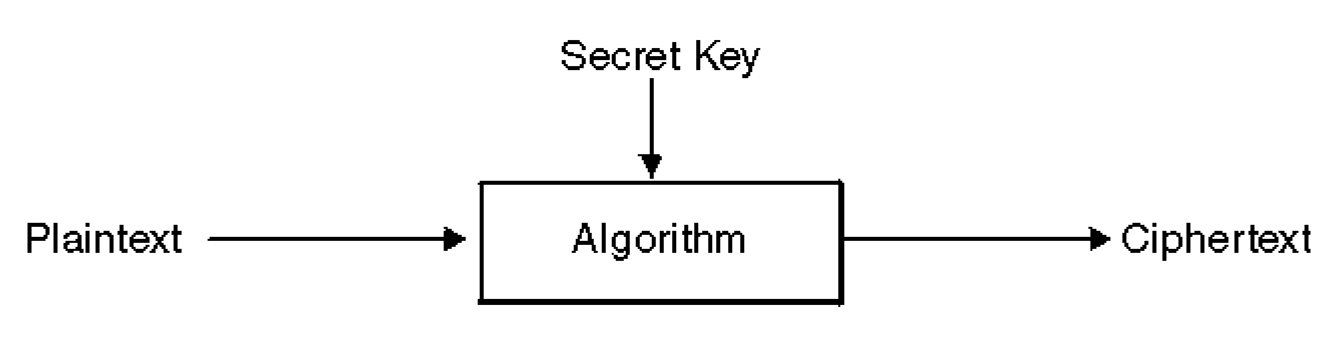
- Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.
- **Nonrepudiation, Origin:** Proof that the message was sent by the specified party.
- **Nonrepudiation, Destination:** Proof that the message was received by the specified party.

SECURITY MECHANISMS

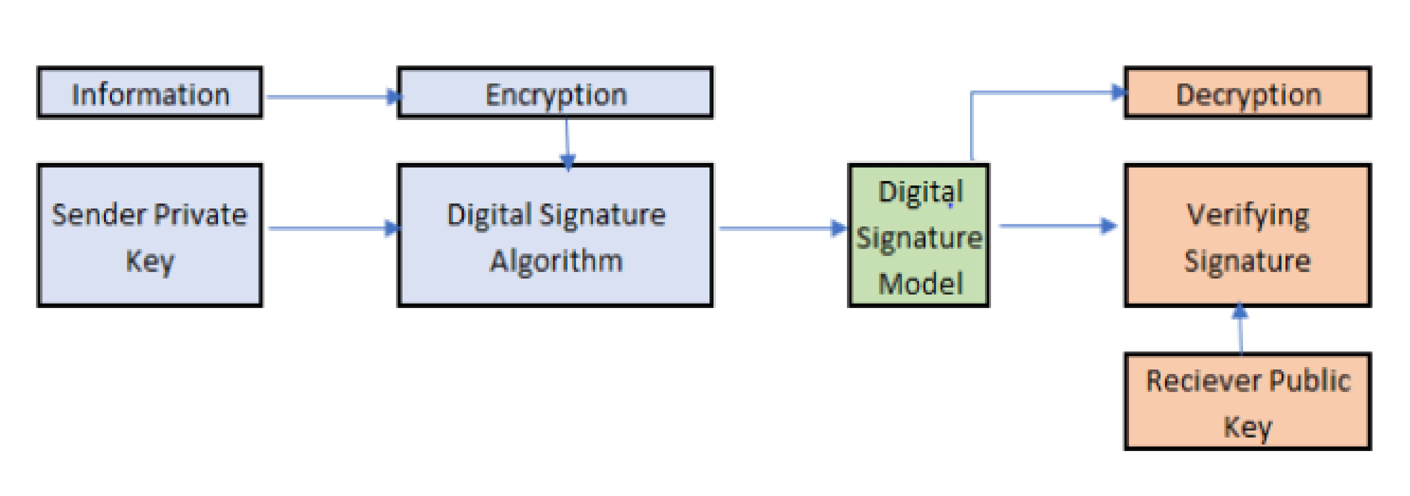
- **Specific Security Mechanisms:** these are incorporated into the appropriate protocol layer in order to provide some of the OSI security services.



- **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.



- **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).



- **Access Control**
- A variety of mechanisms that enforce access rights to resources.

- **Data Integrity**
- A variety of mechanisms used to assure the integrity of a data unit or stream of data units.

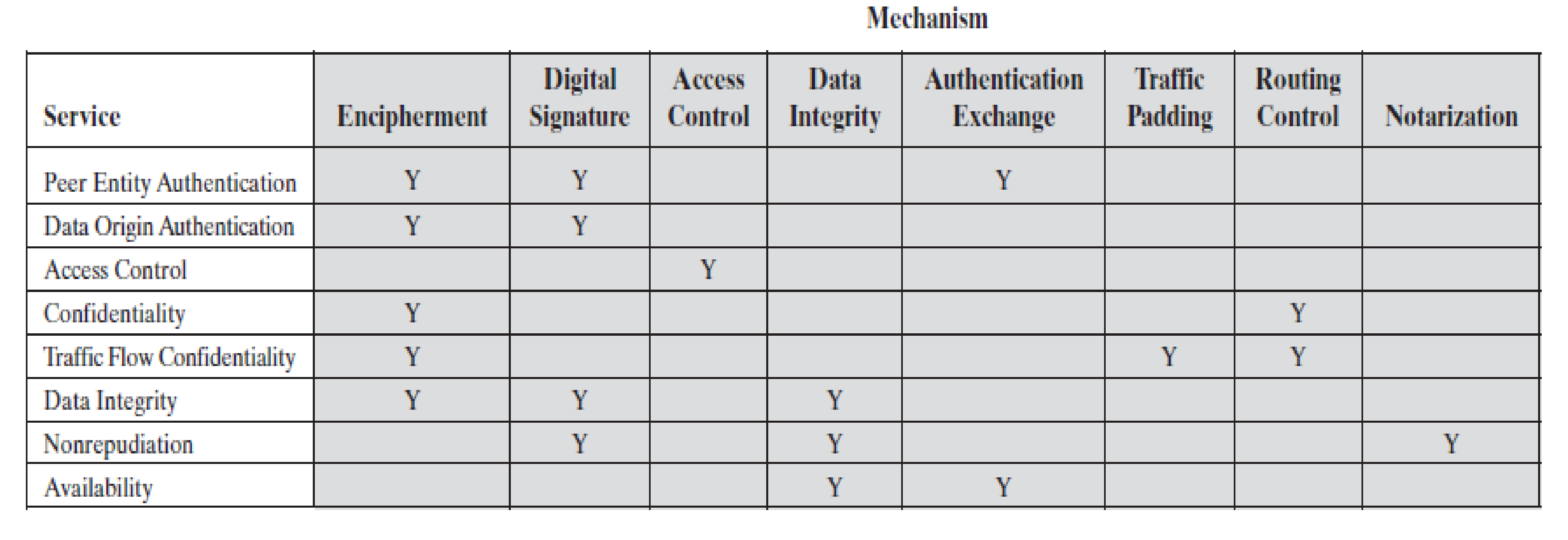
- **Authentication Exchange**
- A mechanism intended to ensure the identity of an entity by means of information exchange.

- **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.

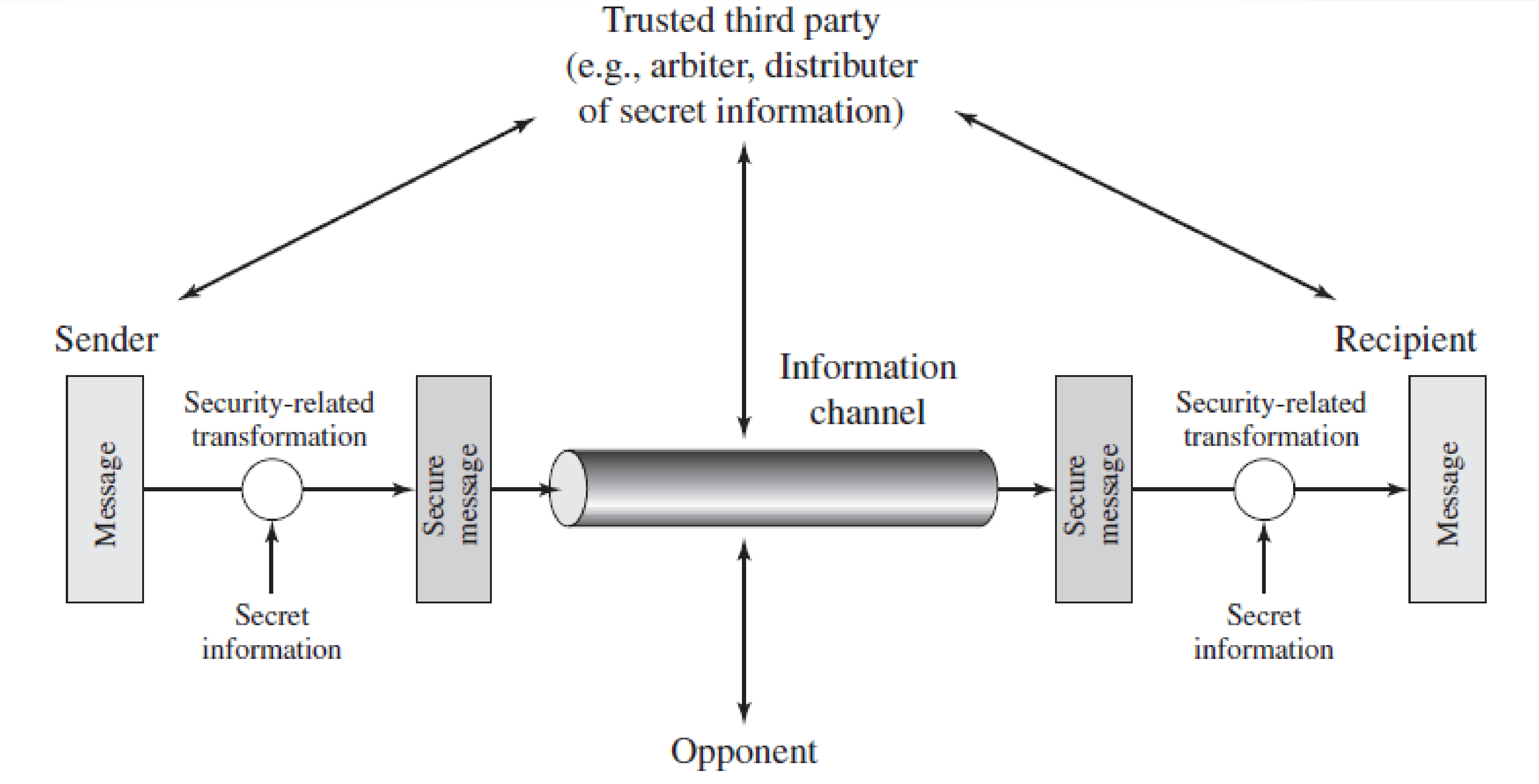
Relationship Between Security Services and Mechanisms



Mechanism

Service	Encipherment	Digital Signature	Access Control	Data Integrity	Authentication Exchange	Traffic Padding	Routing Control	Notarization
Peer Entity Authentication	Y	Y			Y			
Data Origin Authentication	Y	Y						
Access Control			Y					
Confidentiality	Y						Y	
Traffic Flow Confidentiality	Y					Y	Y	
Data Integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

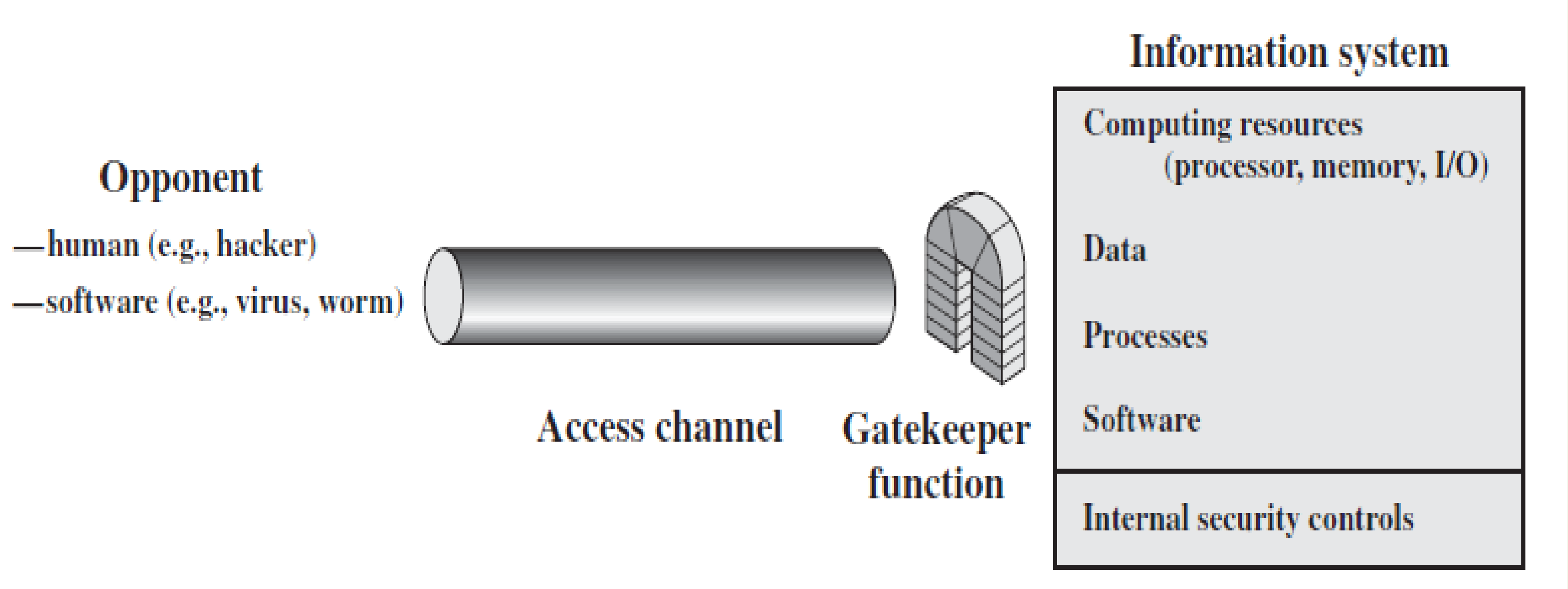
A Model For Network Security



- **Description:**
- A message is to be transferred from one party to another across some sort of Internet service.
- A logical information channel is established by defining a route through the Internet from source to destination.
- Security aspects come into play when it is necessary to protect the information transmission from an opponent.
- The techniques for providing security have two components:
  - A security-related transformation on the information to be sent.
  - Some secret information shared by the two principals and, it is hoped, unknown to the opponent.
- 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.

Network Access Security Model

- Used for protecting an information system from unwanted access.



- The security mechanisms needed to cope with unwanted access fall into two broad categories:
- The first category is termed a **gatekeeper function.** It includes password-based login procedures that are designed to deny access to all but authorized users.
- the second line of defense consists of a variety of internal controls that monitor activity and analyze stored information in an attempt to detect the presence of unwanted intruders.

Thank You

CLASSICAL ENCRYPTION TECHNIQUES

Introduction

- **Symmetric encryption** is a form of cryptosystem in which encryption and decryption are performed using the same key. It is also known as **conventional encryption**.
- Symmetric encryption transforms **plaintext into ciphertext** using a secret key and an encryption algorithm. Using the same key and a decryption algorithm, the **plaintext is recovered from the ciphertext**.

Symmetric Cipher Model

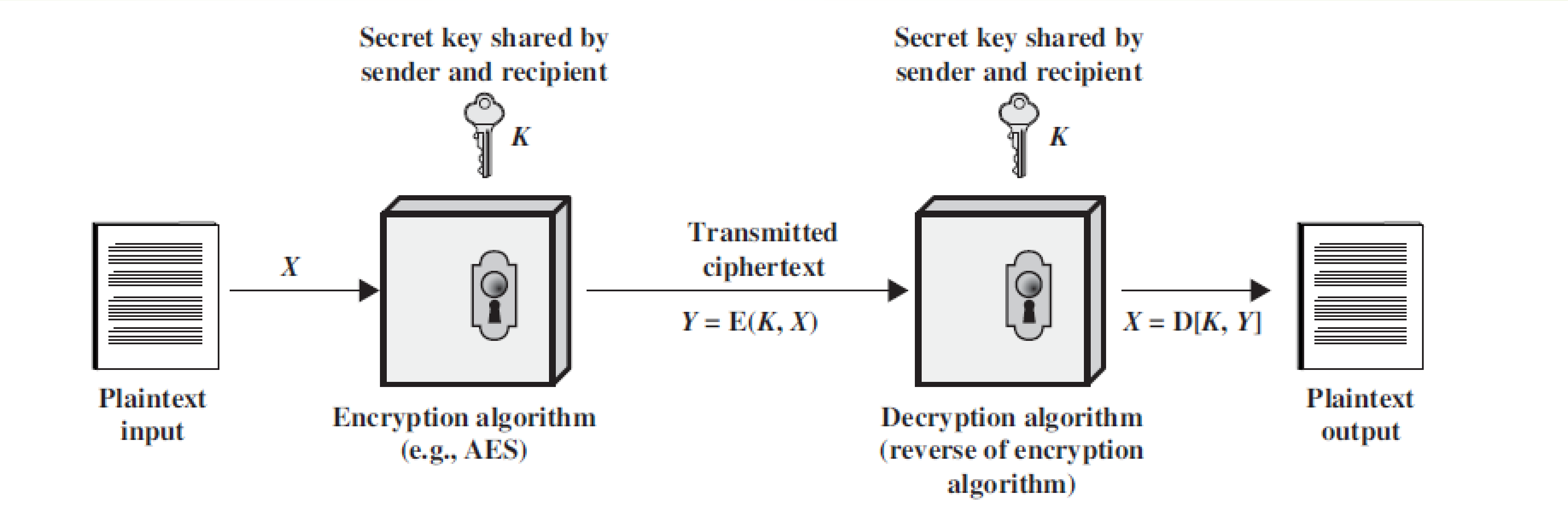
- **A Symmetric encryption scheme has five ingredients :-**

1. **Plaintext:** 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.
4. **Ciphertext:** This is the scrambled message produced as output. It depends on the plaintext and the secret key.
5. **Decryption algorithm:** This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

Symmetric Cipher Model

- There are two requirements for secure use of conventional encryption:

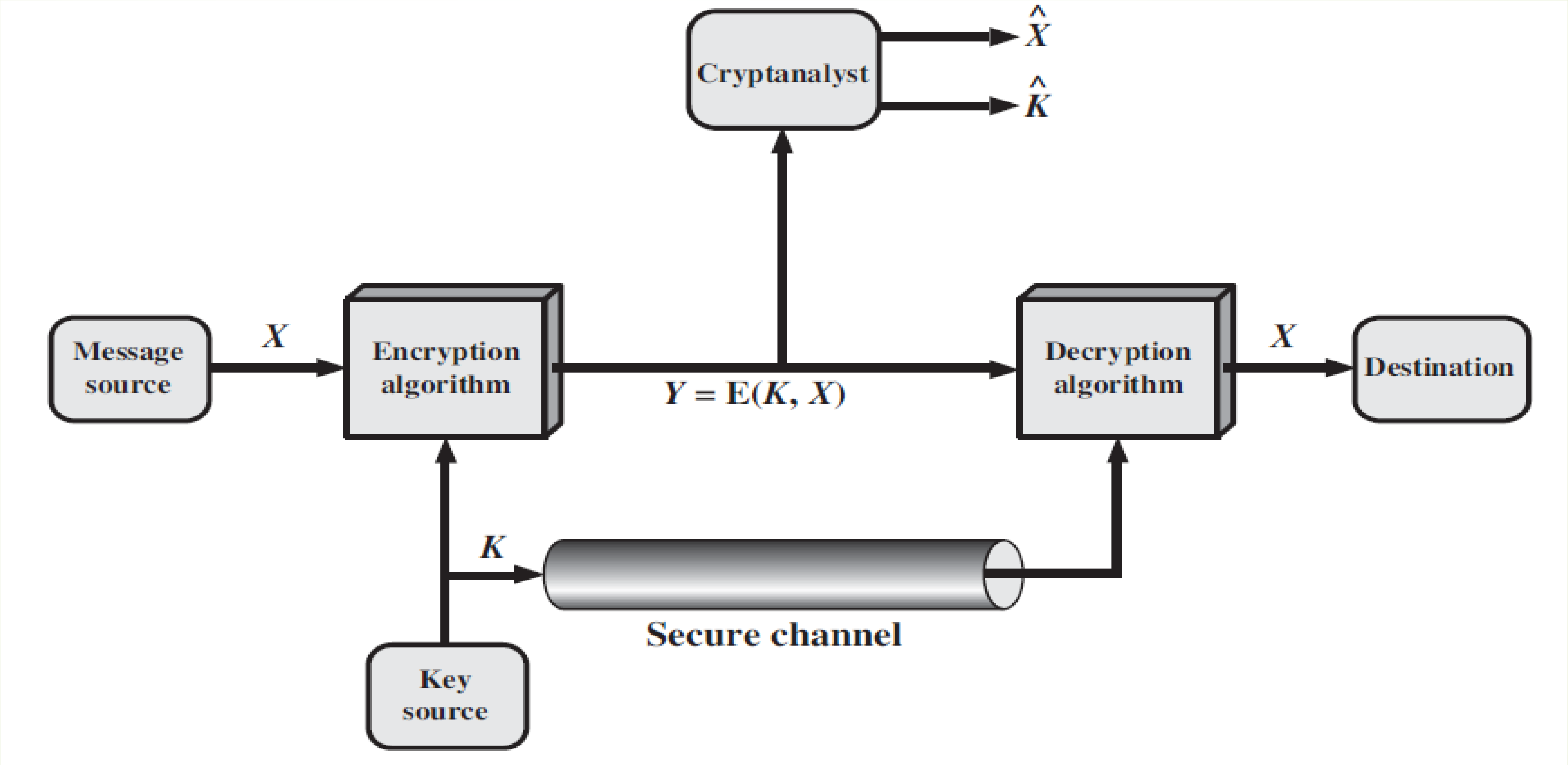
1. We need a strong encryption algorithm.
2. Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure.



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

Model of Symmetric Cryptosystem

- A closer look at the essential elements of a symmetric encryption scheme.



Model of Symmetric Cryptosystem

- A source produces a message in plaintext, X.
- For encryption, a key of the form K is generated.
- With the message X and the encryption key K as input, the encryption algorithm forms the ciphertext Y as:

$$Y = E(K,X)$$

- The intended receiver, in possession of the key, is able to invert the transformation as:

$$X = D(K,Y)$$

- An opponent, observing Y but not having access to K or X, may attempt to recover X or K or both X and K.

Cryptography

- Cryptographic systems are characterized along three independent dimensions:
- **The type of operations used for transforming plaintext to ciphertext.**
  - Substitution, in which each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element.
  - Transposition, in which elements in the plaintext are rearranged.
- **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 asymmetric, two-key, or public-key encryption.

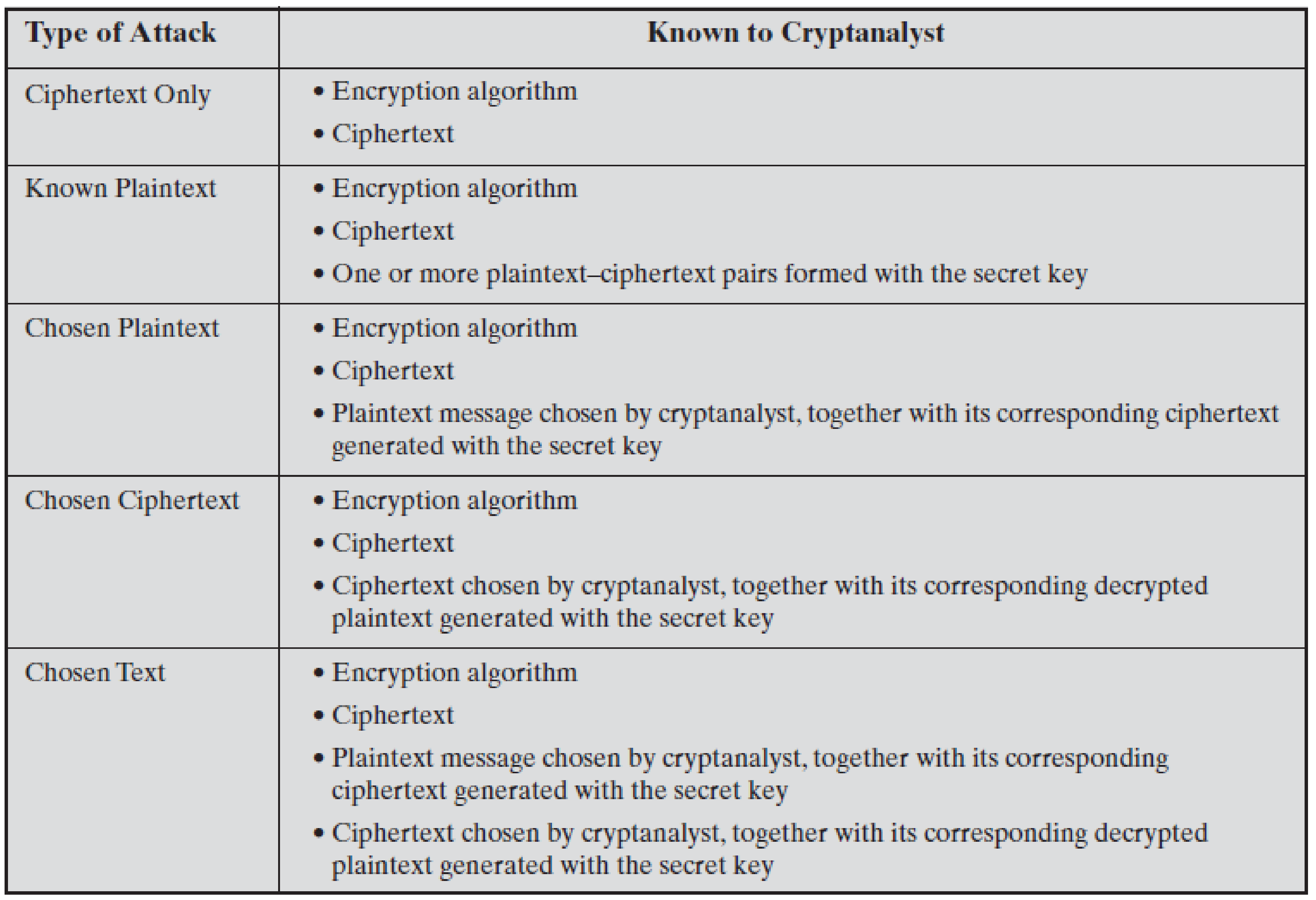
Cryptography

- **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.

Cryptanalysis and Brute-Force Attack

- There are two general approaches to attacking a conventional encryption scheme:
- **Cryptanalysis:** Cryptanalytic attacks rely on the nature of the algorithm plus perhaps 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.

Various Types of Cryptanalytic Attacks



Type of Attack	Known to Cryptanalyst
Ciphertext Only	• Encryption algorithm • Ciphertext
Known Plaintext	• Encryption algorithm • Ciphertext • One or more plaintext–ciphertext pairs formed with the secret key
Chosen Plaintext	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen Ciphertext	• Encryption algorithm • Ciphertext • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key
Chosen Text	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

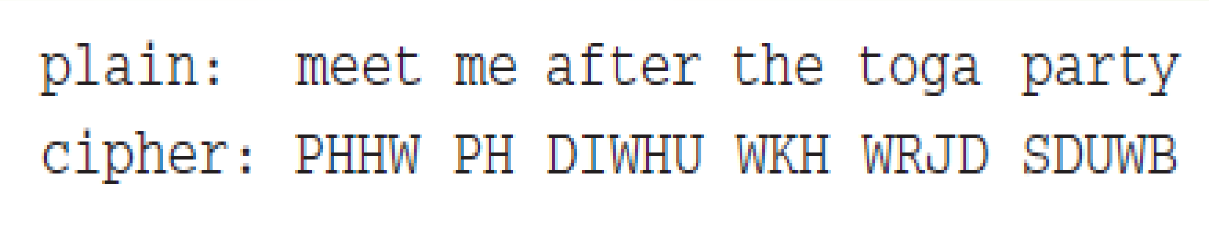
SUBSTITUTION TECHNIQUES

- **Classical Encryption Techniques:**

1. Caesar Cipher
2. Mono-alphabetic Cipher
3. Playfair Cipher
4. Hill Cipher
5. Poly-alphabetic Cipher
    a) Autokey Cipher
    b) Vignere Cipher
6. Vernam Cipher
7. One Time Pad

Caesar Cipher

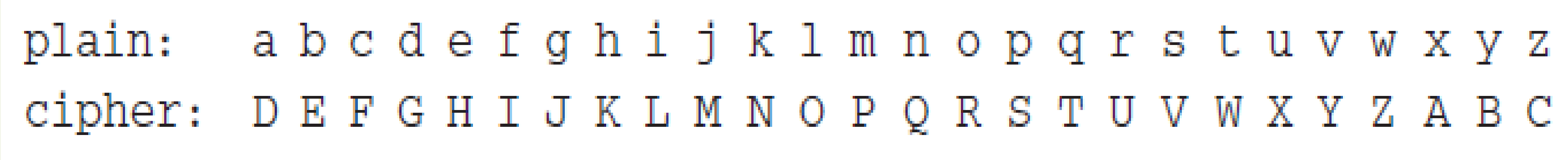
- The simplest use of a substitution cipher was by Julius Caesar.
- The Caesar cipher involves replacing each letter of the alphabet with the letter standing **three** places further down the alphabet.
- Example:



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

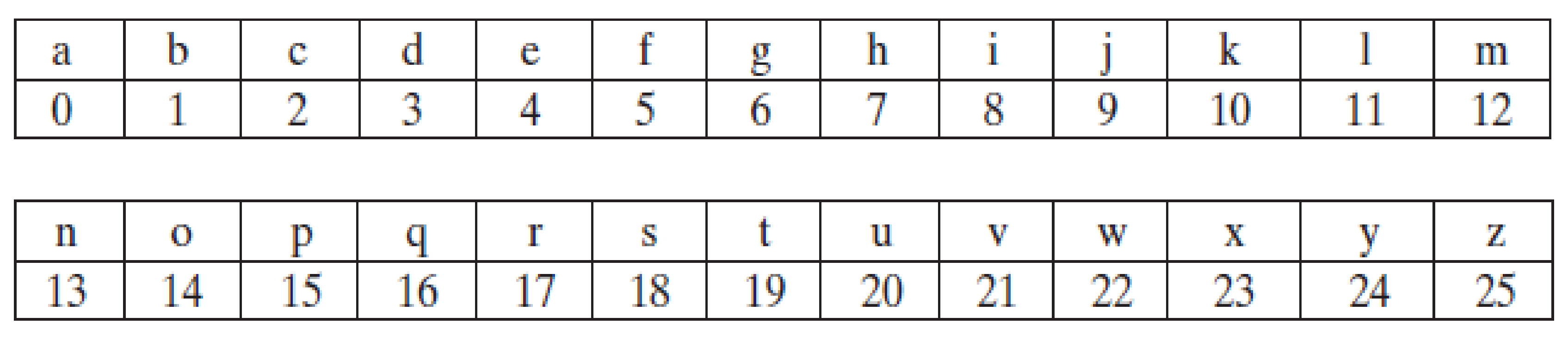
Caesar Cipher (conti…)

- **Technique:**
- 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

- Let us assign a numerical equivalent to each letter:



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

Caesar Cipher (conti…)

- The General Caesar algorithm can be expressed as follows:
- **Encryption**:

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

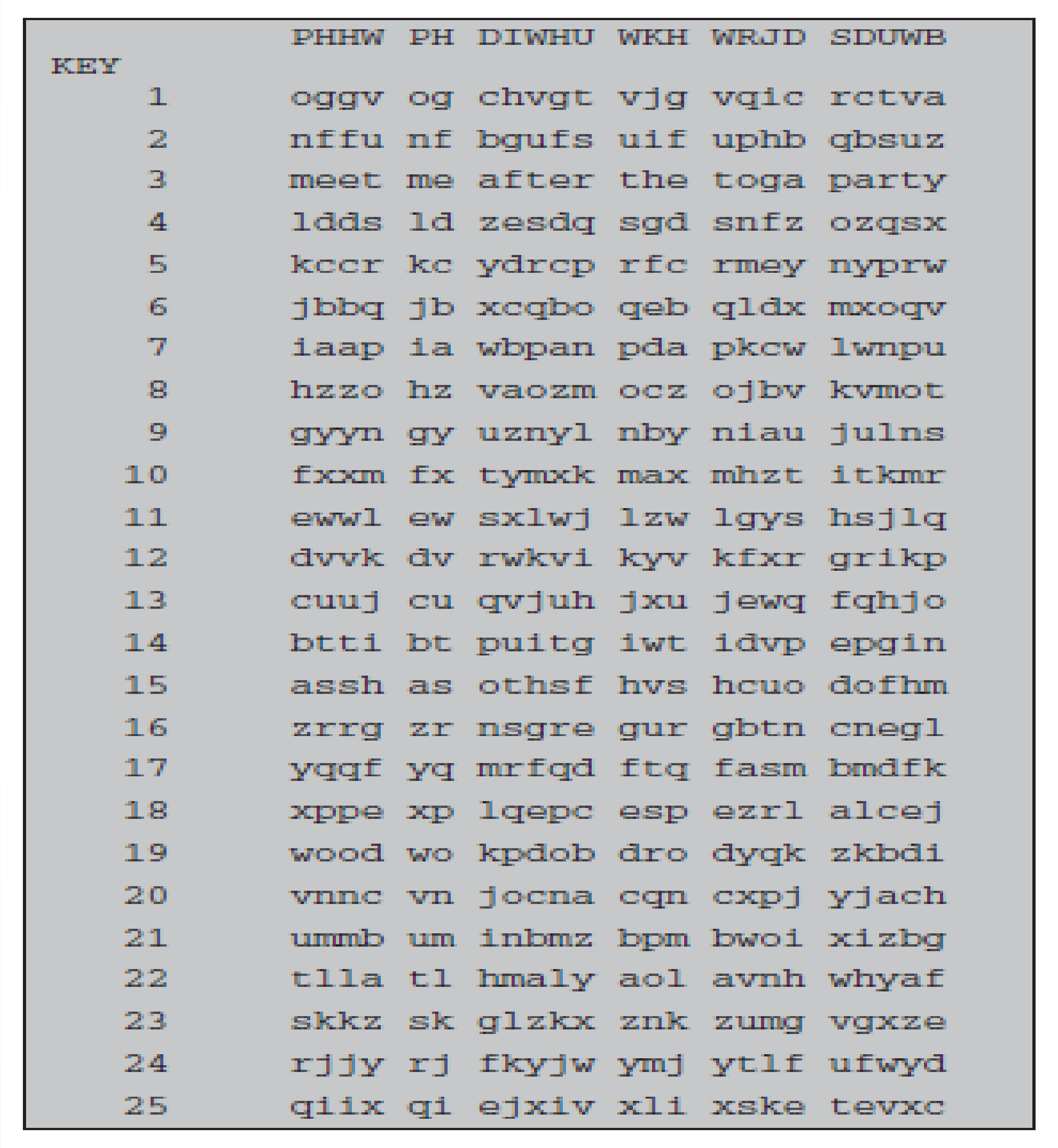
- **Decryption**:

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

- If it is known that a given ciphertext is a Caesar cipher, then a brute-force cryptanalysis is easily performed:

simply try all the 25 possible keys.

Brute force cryptanalysis of Caesar Cipher



	PHHW	PH	DIWHU	WKH	WRJD	SDUWB
KEY						
1	oggv	og	chvgt	vjg	vqic	rctva
2	nffu	nf	bgufs	uif	uphb	qbsuz
3	meet	me	after	the	toga	party
4	ldds	ld	zesdq	sgd	snfz	ozqsx
5	kccr	kc	ydrcp	rfc	rmey	nyprw
6	jbbq	jb	xcqbo	qeb	qldx	mxoqv
7	iaap	ia	wbpan	pda	pkcw	lwnpu
8	hzzo	hz	vaozm	ocz	ojbv	kvmot
9	gyyn	gy	uznyl	nby	niau	julns
10	fxxm	fx	tymxk	max	mhzt	itkmr
11	ewwl	ew	sxlwj	lzw	lgys	hsjlq
12	dvvk	dv	rwkvi	kyv	kfxr	grikp
13	cuuj	cu	qvjuh	jxu	jewq	fqhjo
14	btti	bt	puitg	iwt	idvp	epgin
15	assh	as	othsf	hvs	hcuo	dofhm
16	zrrg	zr	nsgre	gur	gbtn	cnegl
17	yqqf	yq	mrfqd	ftq	fasm	bmdfk
18	xppe	xp	lqepc	esp	ezrl	alcej
19	wood	wo	kpdob	dro	dyqk	zkbdi
20	vnnc	vn	jocna	cqn	cxpj	yjach
21	ummb	um	inbmz	bpm	bwoi	xizbg
22	tlla	tl	hmaly	aol	avnh	whyaf
23	skkz	sk	glzkx	znk	zumg	vgxze
24	rjjy	rj	fkyjw	ymj	ytlf	ufwyd
25	qiix	qi	ejxiv	xli	xske	tevxc

Caesar Cipher Example

- Example:
- Encryption : C = (p + k) mod 26
- Plaintext : “Gitam University”

Plaintext	G	I	T	A	M	U	N	I	V	E	R	S	I	T	Y
P Value	6	8	19	0	12	20	13	8	21	4	17	18	8	19	24
Key = 3	9 mod 26	11 mod 26	22 mod 26	3 mod 26	15 mod 26	23 mod 26	16 mod 26	11 mod 26	24 mod 26	7 mod 26	20 mod 26	21 mod 26	11 mod 26	22 mod 26	27 mod 26
C Value	9	11	22	3	15	23	16	11	24	7	20	21	11	22	1
Ciphertext	J	L	W	D	P	X	Q	L	Y	H	U	V	L	W	B

- Ciphertext : “JLWDPXQLYHUVLWB”

Thank You

CLASSICAL ENCRYPTION TECHNIQUES

Introduction

- **Symmetric encryption** is a form of cryptosystem in which encryption and decryption are performed using the same key. It is also known as **conventional encryption**.
- Symmetric encryption transforms **plaintext into ciphertext** using a secret key and an encryption algorithm. Using the same key and a decryption algorithm, the **plaintext is recovered from the ciphertext**.

Symmetric Cipher Model

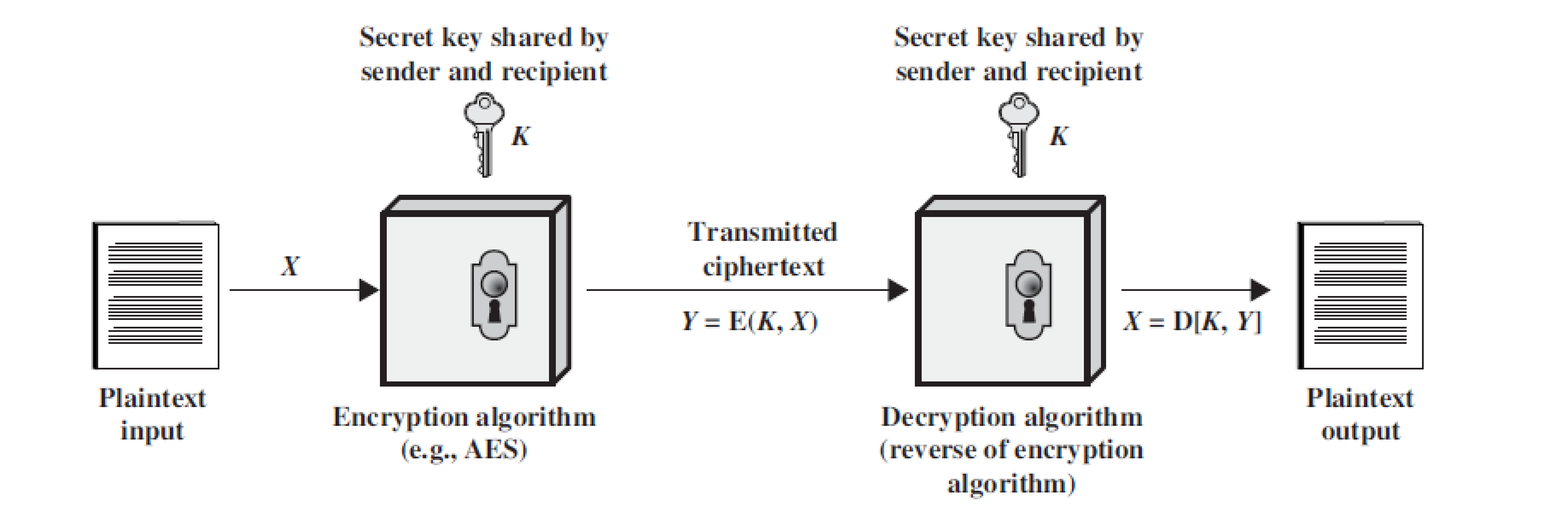
- **A Symmetric encryption scheme has five ingredients :-**

1. **Plaintext:** 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.
4. **Ciphertext:** This is the scrambled message produced as output. It depends on the plaintext and the secret key.
5. **Decryption algorithm:** This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

Symmetric Cipher Model

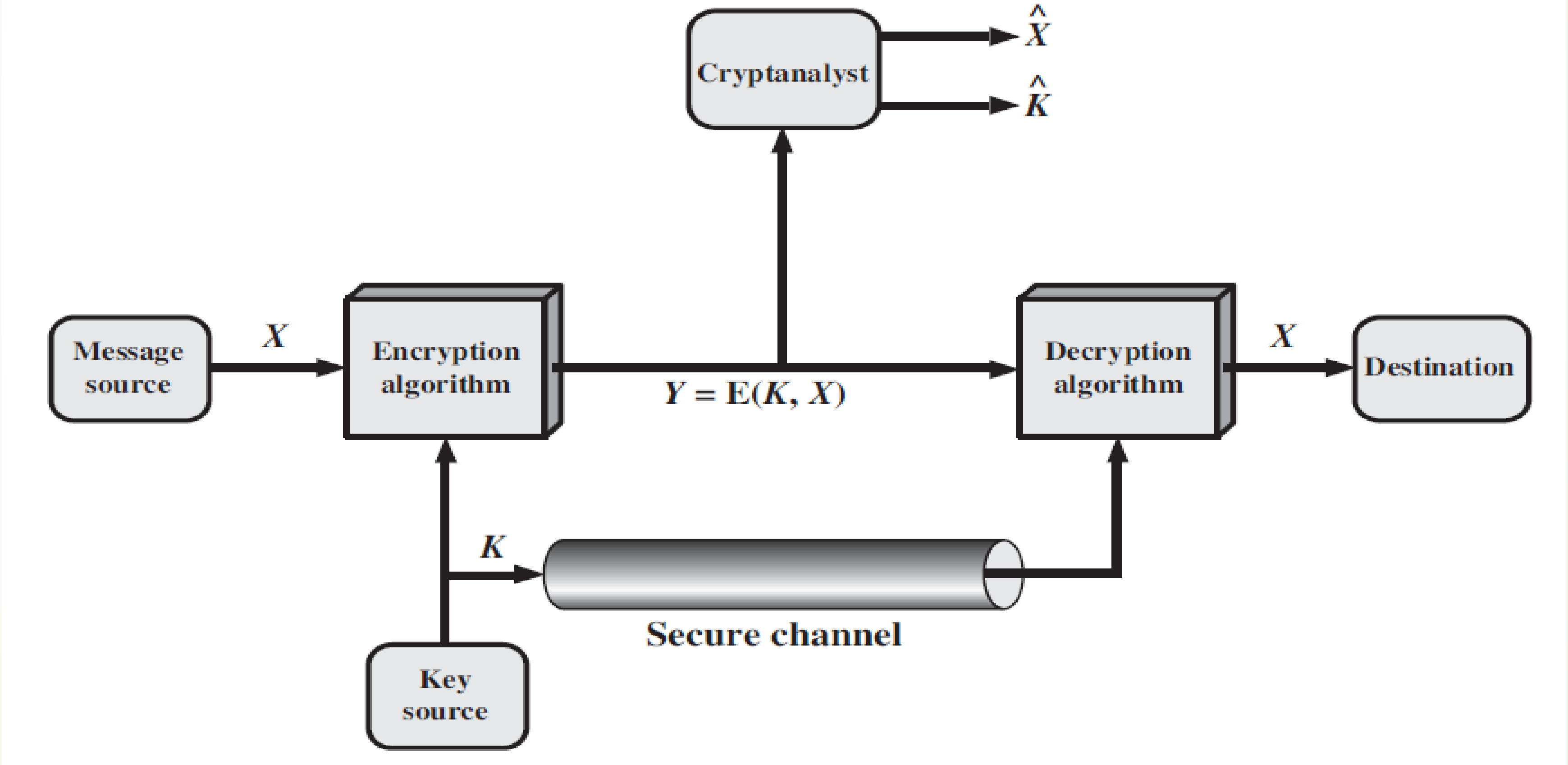
- There are two requirements for secure use of conventional encryption:

1. We need a strong encryption algorithm.
2. Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure.


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

Model of Symmetric Cryptosystem

- A closer look at the essential elements of a symmetric encryption scheme.



Model of Symmetric Cryptosystem

- A source produces a message in plaintext, X.
- For encryption, a key of the form K is generated.
- With the message X and the encryption key K as input, the encryption algorithm forms the ciphertext Y as:

$$Y = E(K,X)$$

- The intended receiver, in possession of the key, is able to invert the transformation as:

$$X = D(K,Y)$$

- An opponent, observing Y but not having access to K or X, may attempt to recover X or K or both X and K.

Cryptography

- Cryptographic systems are characterized along three independent dimensions:
- **The type of operations used for transforming plaintext to ciphertext.**
  - Substitution, in which each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element.
  - Transposition, in which elements in the plaintext are rearranged.
- **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 asymmetric, two-key, or public-key encryption.

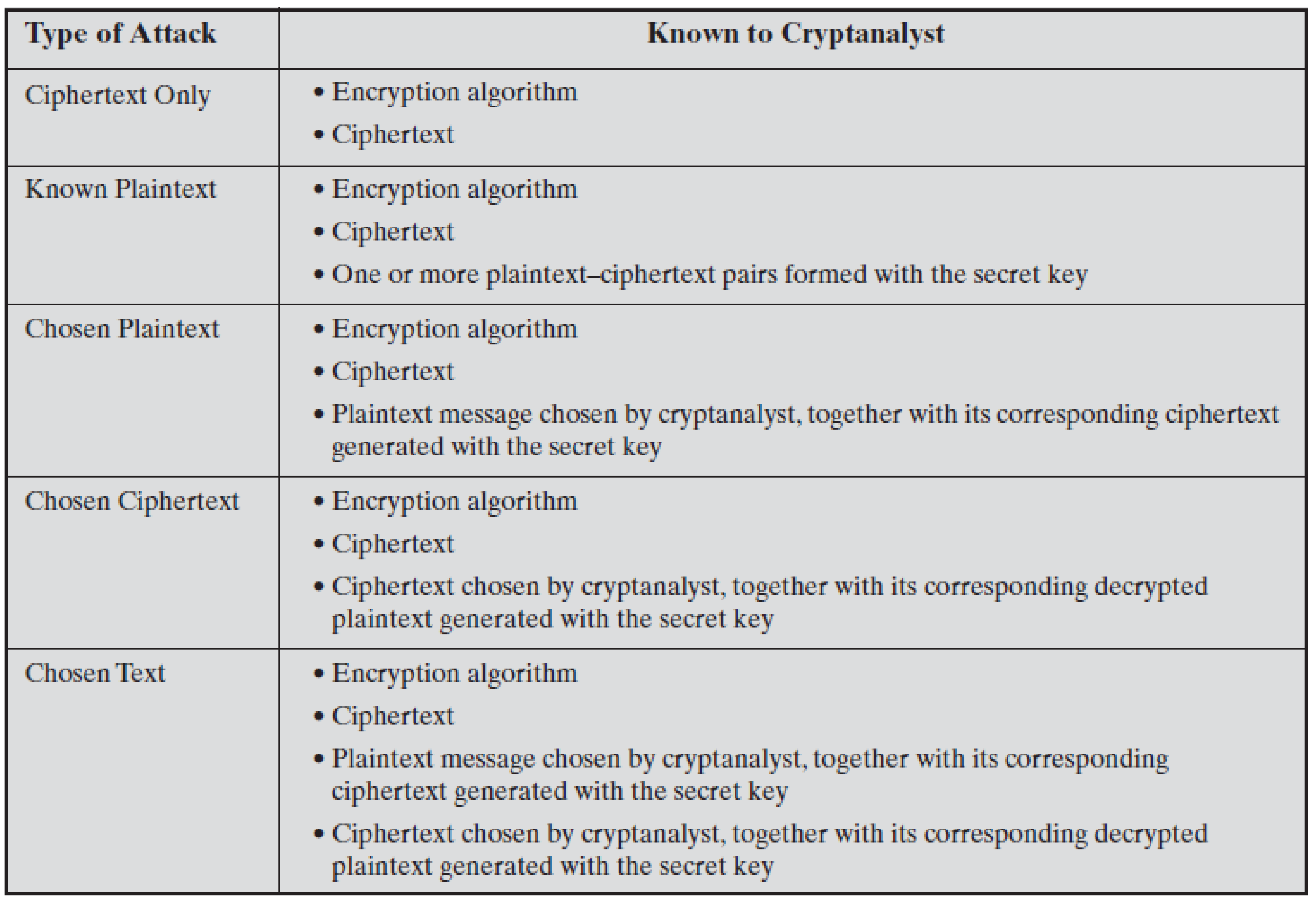
Cryptography

- **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.

Cryptanalysis and Brute-Force Attack

- There are two general approaches to attacking a conventional encryption scheme:
- **Cryptanalysis:** Cryptanalytic attacks rely on the nature of the algorithm plus perhaps 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.

Various Types of Cryptanalytic Attacks



Type of Attack	Known to Cryptanalyst
Ciphertext Only	• Encryption algorithm • Ciphertext
Known Plaintext	• Encryption algorithm • Ciphertext • One or more plaintext–ciphertext pairs formed with the secret key
Chosen Plaintext	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen Ciphertext	• Encryption algorithm • Ciphertext • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key
Chosen Text	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

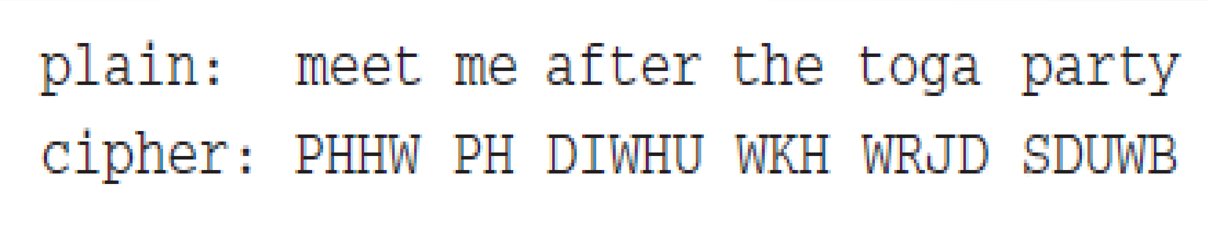
SUBSTITUTION TECHNIQUES

- **Classical Encryption Techniques:**

1. Caesar Cipher
2. Mono-alphabetic Cipher
3. Playfair Cipher
4. Hill Cipher
5. Poly-alphabetic Cipher
   a) Autokey Cipher
   b) Vignere Cipher
6. Vernam Cipher
7. One Time Pad

CAESAR CIPHER

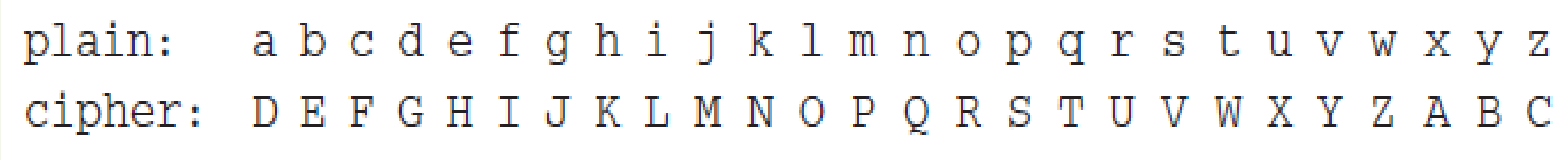
- The simplest use of a substitution cipher was by Julius Caesar.
- The Caesar cipher involves replacing each letter of the alphabet with the letter standing **three** places further down the alphabet.
- Example:



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

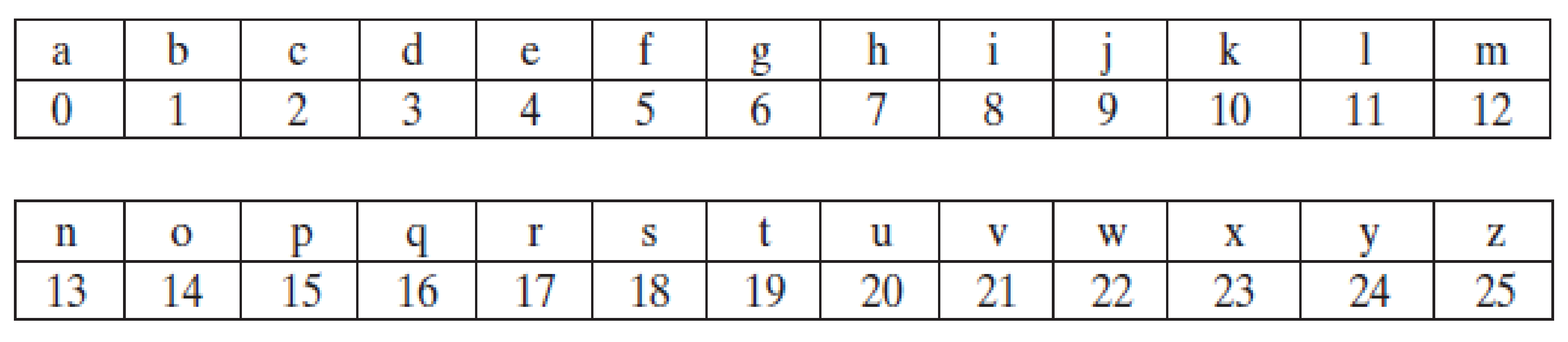
Caesar Cipher (conti…)

- **Technique:**
- 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
```

- Let us assign a numerical equivalent to each letter:



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

Caesar Cipher (conti…)

- The General Caesar algorithm can be expressed as follows:
- **Encryption**:

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

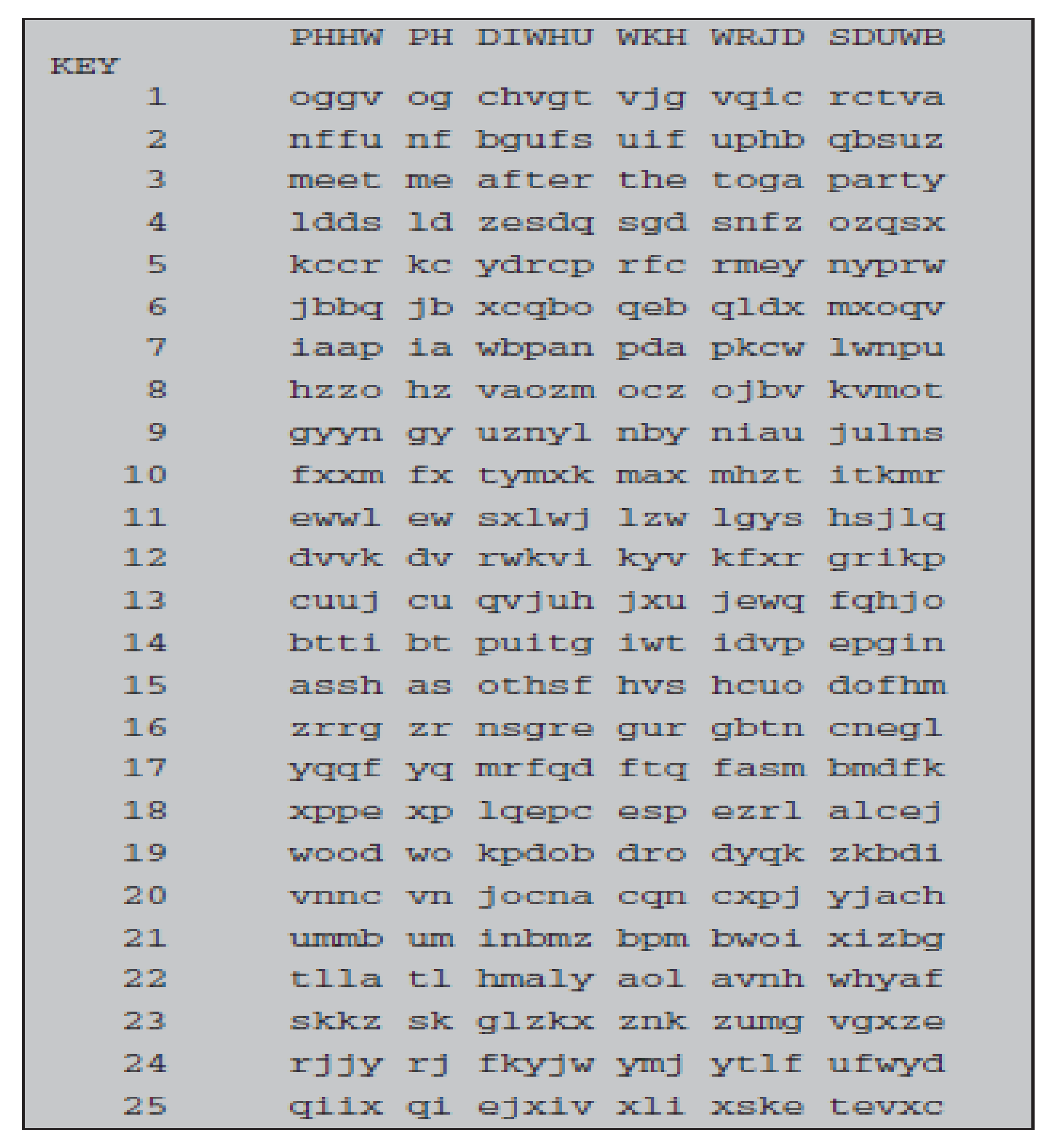
- **Decryption**:

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

- If it is known that a given ciphertext is a Caesar cipher, then a brute-force cryptanalysis is easily performed:

simply try all the 25 possible keys.

Brute force cryptanalysis of Caesar Cipher



	PHHW	PH	DIWHU	WKH	WRJD	SDUWB
KEY						
1	oggv	og	chvgt	vjg	vqic	rctva
2	nffu	nf	bgufs	uif	uphb	qbsuz
3	meet	me	after	the	toga	party
4	ldds	ld	zesdq	sgd	snfz	ozqsx
5	kccr	kc	ydrcp	rfc	rmey	nyprw
6	jbbq	jb	xcqbo	qeb	qldx	mxoqv
7	iaap	ia	wbpan	pda	pkcw	lwnpu
8	hzzo	hz	vaozm	ocz	ojbv	kvmot
9	gyyn	gy	uznyl	nby	niau	julns
10	fxxm	fx	tymxk	max	mhzt	itkmr
11	ewwl	ew	sxlwj	lzw	lgys	hsjlq
12	dvvk	dv	rwkvi	kyv	kfxr	grikp
13	cuuj	cu	qvjuh	jxu	jewq	fqhjo
14	btti	bt	puitg	iwt	idvp	epgin
15	assh	as	othsf	hvs	hcuo	dofhm
16	zrrg	zr	nsgre	gur	gbtn	cnegl
17	yqqf	yq	mrfqd	ftq	fasm	bmdfk
18	xppe	xp	lqepc	esp	ezrl	alcej
19	wood	wo	kpdob	dro	dyqk	zkbdi
20	vnnc	vn	jocna	cqn	cxpj	yjach
21	ummb	um	inbmz	bpm	bwoi	xizbg
22	tlla	tl	hmaly	aol	avnh	whyaf
23	skkz	sk	glzkx	znk	zumg	vgxze
24	rjjy	rj	fkyjw	ymj	ytlf	ufwyd
25	qiix	qi	ejxiv	xli	xske	tevxc

Caesar Cipher Example

- Example:
- Encryption : C = (p + k) mod 26
- Plaintext : “Gitam University”

Plaintext	G	I	T	A	M	U	N	I	V	E	R	S	I	T	Y
P Value	6	8	19	0	12	20	13	8	21	4	17	18	8	19	24
Key = 3	9 mod 26	11 mod 26	22 mod 26	3 mod 26	15 mod 26	23 mod 26	16 mod 26	11 mod 26	24 mod 26	7 mod 26	20 mod 26	21 mod 26	11 mod 26	22 mod 26	27 mod 26
C Value	9	11	22	3	15	23	16	11	24	7	20	21	11	22	1
Ciphertext	J	L	W	D	P	X	Q	L	Y	H	U	V	L	W	B

- Ciphertext : “JLWDPXQLYHUVLWB”

MONOALPHABETIC CIPHER

- With only 25 possible keys, the Caesar cipher is far from secure.
- 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	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
KEY	D	K	V	Q	F	I	B	J	W	P	E	S	C	X	H	T	M	Y	A	U	O	L	R	G	Z	N

- Plaintext : “if we wish to replace letters”
- Ciphertext : ?

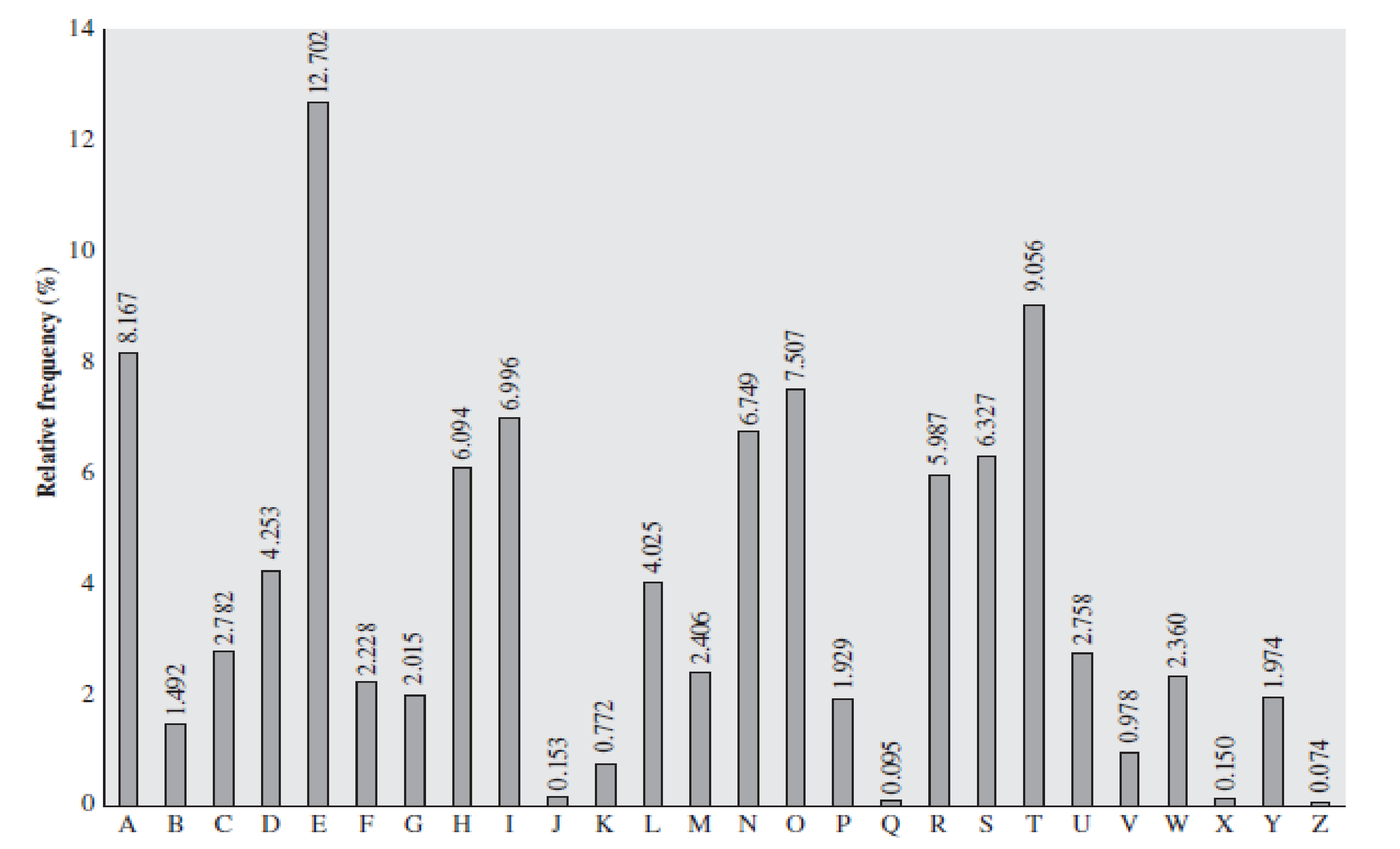
P.T	i	f	w	e	w	i	s	h	t	o	r	e	p	l	a	c	e	l	e	t	t	e	r	s
C.T	W	I	R	F	R	W	A	J	U	H	Y	F	T	S	D	V	F	S	F	U	U	F	Y	A

Monoalphabetic cipher (conti…)

- **Monoalphabetic Cipher Security:**
- Now have a total of 26! Keys.
- With so many keys, might think the system is secure.
- But would be **!!!WRONG!!!**
- Problem is the regularities of the language.
- Human languages are redundant, letters are not equally commonly used.
- The English letter e is by far the most common letter, then T,R,N,I,O,A,S.
- Other letters are fairly rare like Z,J,K,Q,X.

Monoalphabetic cipher (conti…)

- **English letter frequencies:**



Monoalphabetic cipher (conti…)

- **Use in Cryptanalysis:**
- Key concept - monoalphabetic substitution ciphers do not change relative letter frequencies.
- Discovered by Arabian scientists in 9th century.
- Calculate letter frequencies for ciphertext and compare counts against known values.

Monoalphabetic cipher (conti…)

- Given ciphertext:

  UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ

  VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX

  EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
- Count relative letter frequencies.
- The most common letters are P & Z and are equivalent to *e* and *t*.
- The most common Digram are ZW is equivalent to ‘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

PLAYFAIR CIPHER

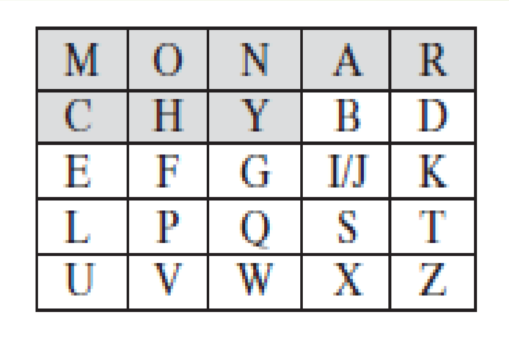
- Not even the large number of keys in a monoalphabetic cipher provides security.
- One approach to improving security was to encrypt multiple letters, the **Playfair Cipher** is an example.
- Invented by **Charles Wheatstone in 1854**, but named after his friend Baron Playfair.
- Playfair cipher is the best-known multiple-letter encryption cipher.
- Based on a **5 x 5** matrix of letters constructed using a **keyword**, fill in the spaces in the table with the letters of the keyword (dropping any duplicate letters).
- Then fill the remaining spaces with the rest of the letters of the alphabet in order (usually **omitting "J" or "Q"** to reduce the alphabet to fit; other versions put both **"I" and "J" in the same space**.)

Playfair Cipher (conti…)

- Plaintext is encrypted two letters at a time with following rules:
  - Repeating plaintext letters that are in the same pair are separated with a filler letter, such as x.
    - Example:

      balloon is written as ba ll oo n and then will be separated 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.
    - Example:

      ar is encrypted as RM.



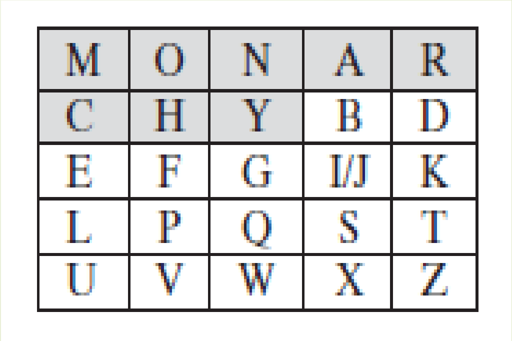
M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

Playfair Cipher (conti…)

- 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.
  - 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.
  - Example:

    hs becomes BP and ea becomes IM (or JM, as the encipherer wishes).



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 (conti…)

- Security much improved over monoalphabetic since have 26 x 26 = 676 digrams.
- It would need a 676 entry frequency table to analyse (verses 26 for a monoalphabetic)
- It was widely used for many years (eg. US & British military in WW1)
- It can be broken, given a few hundred letters since still has much of plaintext structure.

Plaintext – jitter
Key - monarchy

- Playfair cipher uses a 5 by 5 table containing a key.
- fill in the spaces in the table with the letters of the keyword (dropping any duplicate letters)
- Then fill the remaining spaces with the rest of the letters of the alphabet in order (usually **omitting "J" or "Q"** to reduce the alphabet to fit; other versions put both **"I" and "J" in the same space**.)
- Omit Q (because we have i and j both in the plaintext)

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

- If repeating plaintext letters are in same pair, separate them with a filler letter.

ji tt er → ji tx te rx

- According to 2nd rule:

ji → EJ

- According to 4th rule:

tx → SZ

- According to 4th rule:

te → KJ

- According to 4th rule:

rx → AZ

- **The Ciphertext is:**

“EJSZKJAZ”

HILL CIPHER

- Developed by the mathematician Lester Hill in 1929.
- The encryption algorithm takes m successive plain text and substitute for them m cipher text letters.
- Each character is assigned a numerical value (a=0,…z=25).
- Encryption: Multiply each block by **K** and then reduce mod 26.
- Decryption: multiply each block by the inverse of **K**, and reduce mod 26.

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

$$C = KP \bmod 26$$

$$P = K^{-1}C \bmod 26 = KK^{-1}P = P$$

Hill cipher (conti…)

- **Example:**
- Plain text: “LOVE”, Secret Key: $\begin{bmatrix} 20 & 3 \\ 15 & 7 \end{bmatrix}$
- “LO” → $\begin{bmatrix} 20 & 3 \\ 51 & 7 \end{bmatrix} \begin{bmatrix} 11 \\ 14 \end{bmatrix} = \begin{bmatrix} 262 \\ 263 \end{bmatrix} = \begin{bmatrix} 2 \\ 3 \end{bmatrix} \mod 26$
- “VE” → $\begin{bmatrix} 20 & 3 \\ 51 & 7 \end{bmatrix} \begin{bmatrix} 21 \\ 4 \end{bmatrix} = \begin{bmatrix} 432 \\ 343 \end{bmatrix} = \begin{bmatrix} 16 \\ 5 \end{bmatrix} \mod 26$
- 2, 3, 16, 5 are transformed to cipher text “CDQF”

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

Hill cipher (conti…)

- **How to decode?**
- Given “CDQF”, and the encryption matrix $\begin{bmatrix} 20 & 3 \\ 15 & 7 \end{bmatrix}$
- How do we decrypt?
  - We need to compute the inverse of $\begin{bmatrix} 20 & 3 \\ 15 & 7 \end{bmatrix}$
- Remind that all arithmetic are mod 26. There is no fraction and care should be taken in computing multiplicative inverse mod 26.

Hill cipher (conti…)

- **Determinant**
- The determinant of $\begin{bmatrix} 20 & 3 \\ 15 & 7 \end{bmatrix}$ equals 20(7) - 3(15), which is 17 mod 26.
- Find the multiplicative inverse of 17 mod 26, i.e., find integer x such that

  17. x = 1 mod 26.
- Just try all 26 possibilities for x:

17×1 = 17 mod 26
17×2= 8 mod 26
17×3 = 25 mod 26
17×4 = 16 mod 26
17×5 = 7 mod 26
17×6 = 24 mod 26
17×7 = 15 mod 26

17×8 = 6 mod 26
17×9= 23 mod 26
17×10 = 14 mod 26
17×11 = 5 mod 26
17×12 = 22 mod 26
17×13 = 13 mod 26
17×14 = 4 mod 26

17×15 = 21 mod 26
17×16= 12 mod 26
17×17 = 3 mod 26
17×18 = 20 mod 26
17×19 = 11 mod 26
17×20 = 2 mod 26
17×21 = 19 mod 26

17×22 = 10 mod 26
17×23= 1 mod 26
17×24 = 18 mod 26
17×25 = 9 mod 26
17×0 = 0 mod 26

Hill cipher (conti…)

- **Computing the inverse mod 26**
- From 17×23= 1 mod 26, we know that the multiplicative inverse of 17 mod 26 is 23.
- Using the formula for 2 × 2 matrix inverse

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = (ad - bc)^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

we get

Replace $(17)^{-1}$ mod 26 by 23

$$\begin{bmatrix} 20 & 3 \\ 15 & 7 \end{bmatrix}^{-1} = (17)^{-1} \begin{bmatrix} 7 & -3 \\ -15 & 20 \end{bmatrix} = 23 \begin{bmatrix} 7 & 23 \\ 11 & 20 \end{bmatrix} = \begin{bmatrix} 5 & 9 \\ 19 & 18 \end{bmatrix} \text{ mod } 26$$

Hill cipher (conti…)

- **Decryption**
- Given the ciphertext "CDQF", we decrypt by multiplying by $\begin{bmatrix} 5 & 9 \\ 19 & 18 \end{bmatrix}$

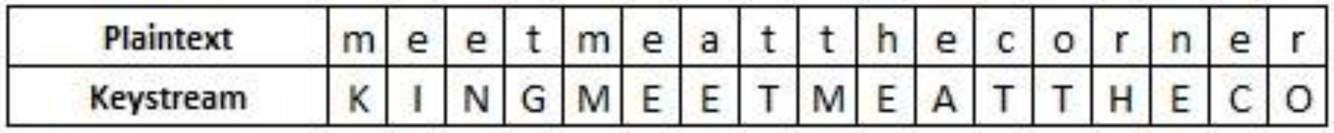
$$\begin{bmatrix} 5 & 9 \\ 19 & 18 \end{bmatrix} \begin{bmatrix} 2 \\ 3 \end{bmatrix} = \begin{bmatrix} 37 \\ 92 \end{bmatrix} = \begin{bmatrix} 11 \\ 14 \end{bmatrix} \mod 26$$

$$\begin{bmatrix} 5 & 9 \\ 19 & 18 \end{bmatrix} \begin{bmatrix} 16 \\ 5 \end{bmatrix} = \begin{bmatrix} 125 \\ 394 \end{bmatrix} = \begin{bmatrix} 21 \\ 4 \end{bmatrix} \mod 26$$

- 11, 14, 21, 4 is "LOVE".

POLYALPHABETIC CIPHER

- **Autokey Cipher:**
- The term *autokey* refers to any cipher where the key is based on the original plaintext.
- Encryption using the Autokey Cipher is very similar to the Vigenère Cipher, except in the creation of the keystream.
- The keystream is made by starting with the keyword, and then appending to the end of this the plaintext itself.
- Plaintext : “meet me at the corner”
- Key : KING

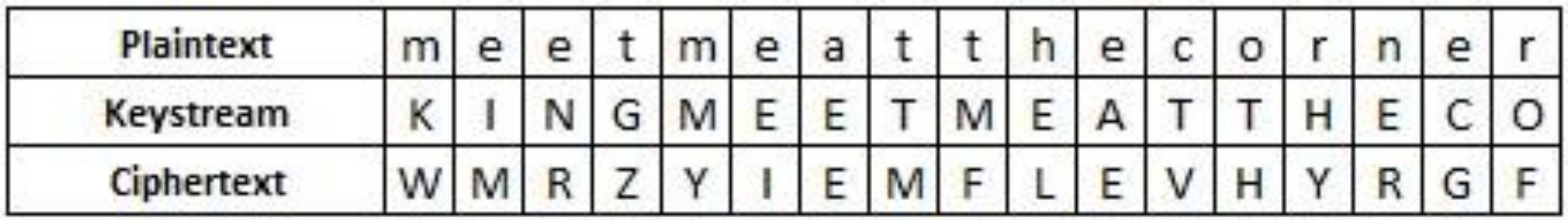


Plaintext	m	e	e	t	m	e	a	t	t	h	e	c	o	r	n	e	r
Keystream	K	I	N	G	M	E	E	T	M	E	A	T	T	H	E	C	O

Polyalphabetic cipher (conti…)

- **Encryption : $C_i = (p_i + k_{i \bmod m}) \bmod 26$**
- **Decryption : $p_i = (C_i - k_{i \bmod m}) \bmod 26$**

P.T	12	4	4	19	12	4	0	19	19	7	4	2	14	17	13	4	17
Key	10	8	13	6	12	4	4	19	12	4	0	19	19	7	4	2	14
C.T	22	12	17	25	24	8	4	12	5	11	4	21	7	24	17	6	5



Plaintext	m	e	e	t	m	e	a	t	t	h	e	c	o	r	n	e	r
Keystream	K	I	N	G	M	E	E	T	M	E	A	T	T	H	E	C	O
Ciphertext	W	M	R	Z	Y	I	E	M	F	L	E	V	H	Y	R	G	F

Polyalphabetic cipher (conti…)

- **Vigenere Cipher**
  - One of the simplest, polyalphabetic cipher.
  - Assume a sequence of Plaintext letters P,

$$P = p_{0,} p_1, p_2, \ldots., p_{n-1}$$

  - A Key consisting of the sequence of letters K,

$$K = k_0, k_1, k_2, \ldots, k_{m-1}$$

where m < n

  - The sequence of Ciphertext letters C,

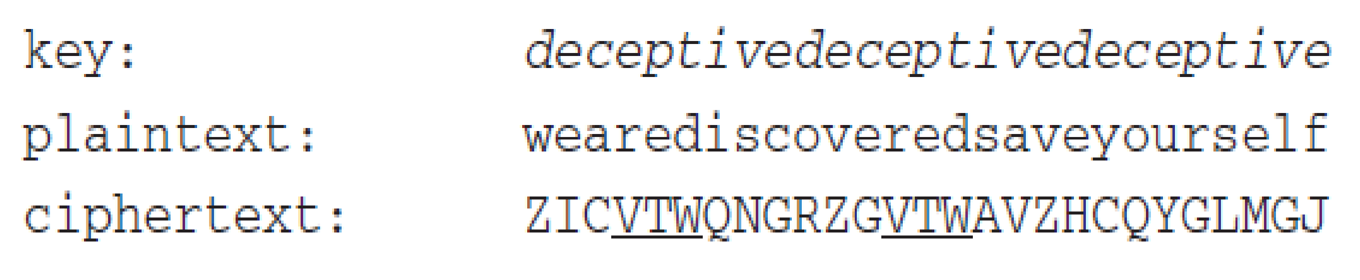
$$C = C_0, C_1, C_2, \ldots.. , C_{n-1}$$

is calculated as: $\mathbf{C_i = (p_i + k_{i \bmod m}) \bmod 26}$

Polyalphabetic cipher (conti…)

- Decryption: $\mathbf{p_i = (C_i - k_{i \bmod m}) \bmod 26}$
- To encrypt a message, a key is needed that is as long as the message.
- The key is a repeating keyword.
- **Example:**
  - keyword = deceptive
  - Plaintext = we are discovered save yourself

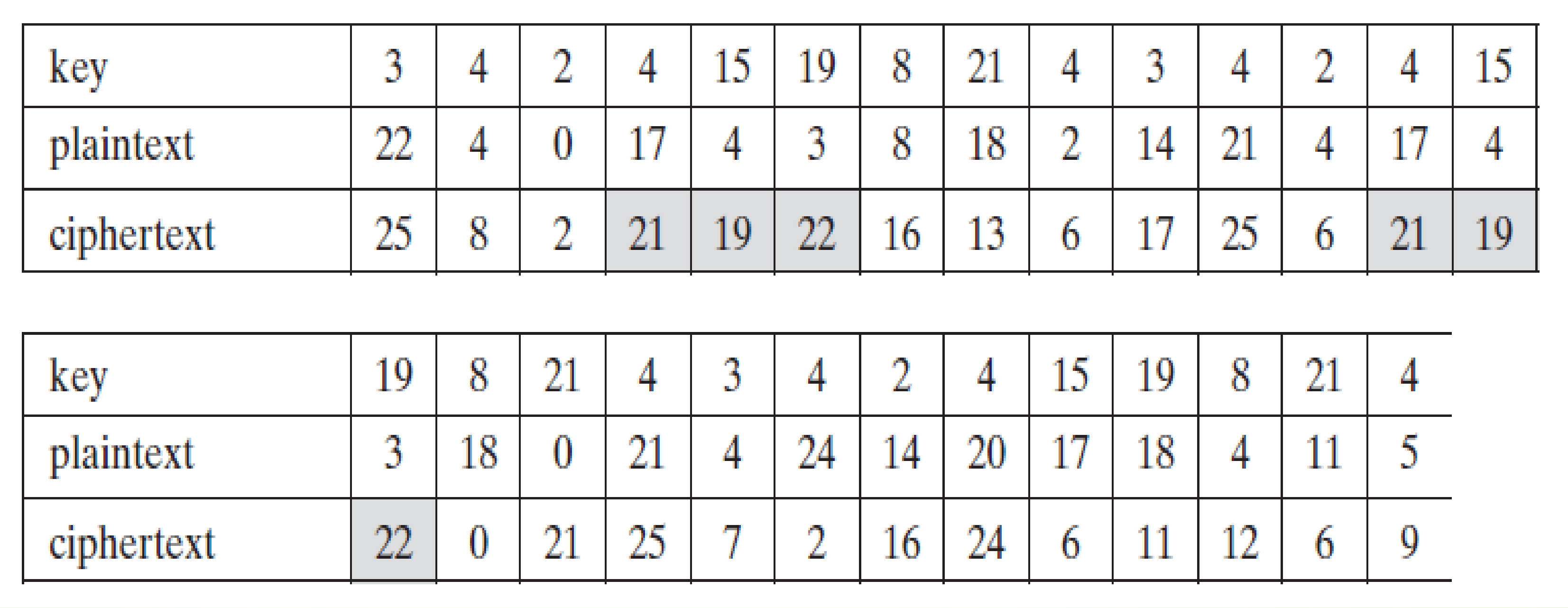
is encrypted as



key:	*deceptivedeceptivedeceptive*
plaintext:	wearediscoveredsaveyourself
ciphertext:	ZICVTWQNGRZGVTWAVZHCQYGLMGJ

Polyalphabetic cipher (conti…)

- 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

VERNAM CIPHER

- The system can be expressed as:

$$\mathbf{c_i = p_i \oplus k_i}$$

where

p_i = ith binary digit of plaintext

k_i = ith binary digit of key

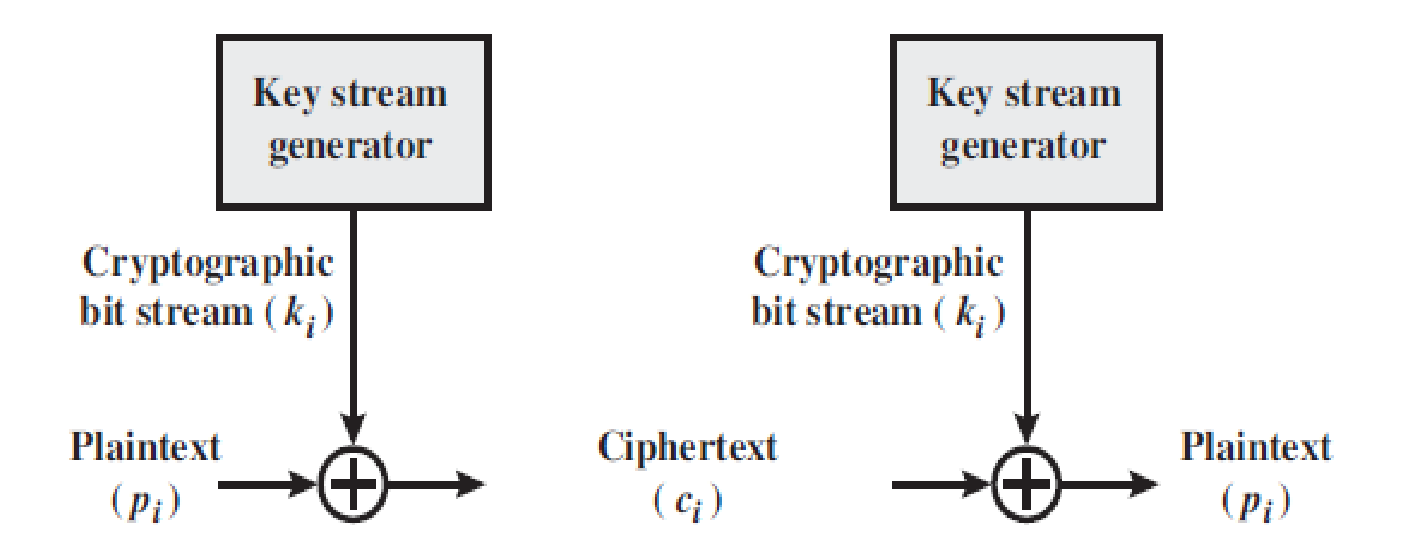
c_i = ith binary digit of ciphertext

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

- The ciphertext is generated by performing the bitwise XOR of the plaintext and the key.
- Because of the properties of the XOR, decryption is given as:

$$\mathbf{p_i = c_i \oplus k_i}$$

Vernam cipher (conti…)



Vernam cipher (conti…)

- In Vernam cipher algorithm,

  length of key = length of plaintext

- Example,

Plaintext = H e l l o
7 4 11 11 14

Key = D G H B C
3 6 7 1 2

Ciphertext = 10 10 18 12 16
K K S M Q

ONE TIME PAD (OTP)

- An Army Signal Corp officer, Joseph Mauborgne, proposed an improvement to the Vernam cipher that yields the ultimate in security.
- He suggested using a random key that is as long as the message, so that the key need not be repeated.
- The key is used to encrypt and decrypt a single message, and then it is discarded.
- Each new message requires a new key of the same length as the new message.
- Plaintext : hello
- Key : XMCKL

Plaintext	h	e	l	l	o
P.T Value	7	4	11	11	14
Key	X	M	C	K	L
Key Value	23	12	2	10	11
C.T Value	30mod26= 4	16mod26= 16	13mod26= 13	21mod26= 21	25mod26= 25
CIPHERTEXT	E	Q	N	V	Z

One Time Pad (conti…)

- The resulting ciphertext will be impossible to decrypt or break if the following four conditions are met:
  1. The key must be truly random.
  2. The key must be at least as long as the plaintext.
  3. The key must never be reused in whole or in part.
  4. The key must be kept completely secret.

TRANSPOSITION CIPHERS

- **Introduction :**
- A transposition cipher is one which rearranges the order of the letters in the ciphertext (encoded text), according to some predetermined method, **without making any substitutions**.
- Transposition cipher types:
  - Rail fence
  - Columnar Transposition Cipher
  - Double Transposition Cipher

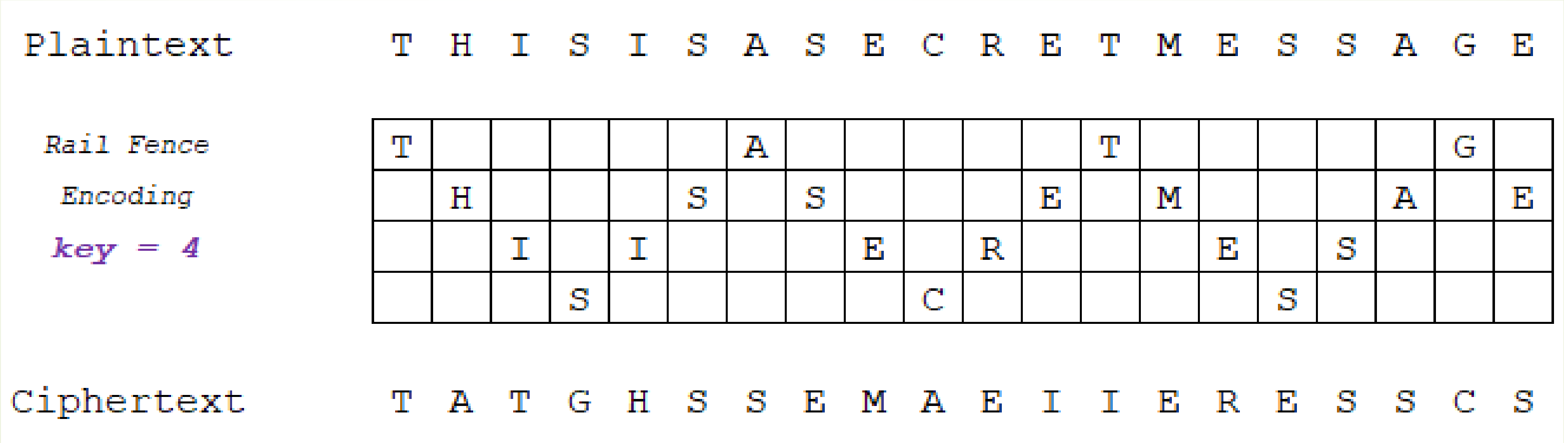
Rail Fence

- The simplest transposition cipher.
- **Rail fence** - the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.
- example,
    - to encipher the message “**meet me after the toga party**” with a rail fence of depth 2, we write:
    - 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**
- This sort of thing would be trivial to cryptanalyze.

Example

- Plaintext : This is a secret message
- Depth : 4



Plaintext	T	H	I	S	I	S	A	S	E	C	R	E	T	M	E	S	S	A	G	E
Rail Fence Encoding *key = 4*	T						A						T						G	
		H				S		S				E		M				A		E
			I		I				E		R				E		S			
				S						C						S				
Ciphertext	T	A	T	G	H	S	S	E	M	A	E	I	I	E	R	E	S	S	C	S

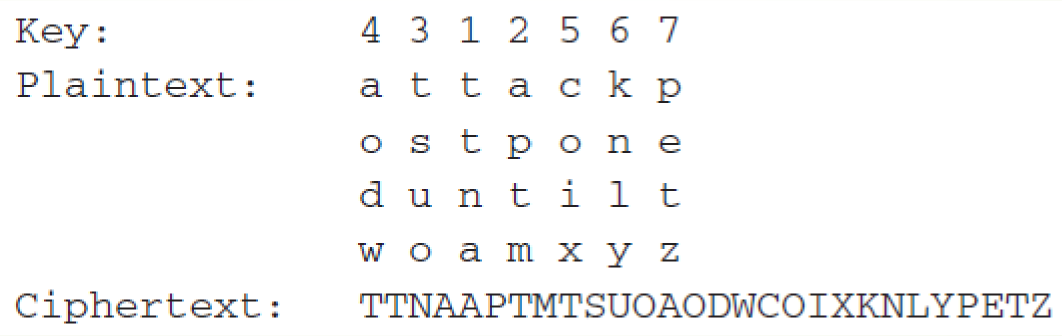
Rail Fence (conti…)

- To **decipher a Rail fence** cipher:
  - divide the ciphertext in half and reverse the order of the steps of encipherment, that is, write the ciphertext in two rows and read off the plaintext in a zig-zag fashion.
- Example:
  - Decipher the message

    “CITAT ODABT UHROE ELNES WOMYE OGEHW VR” that was enciphered using a rail fence cipher.

Columnar Transposition Cipher

- 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 the columns then becomes the key to the algorithm.
- 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
```

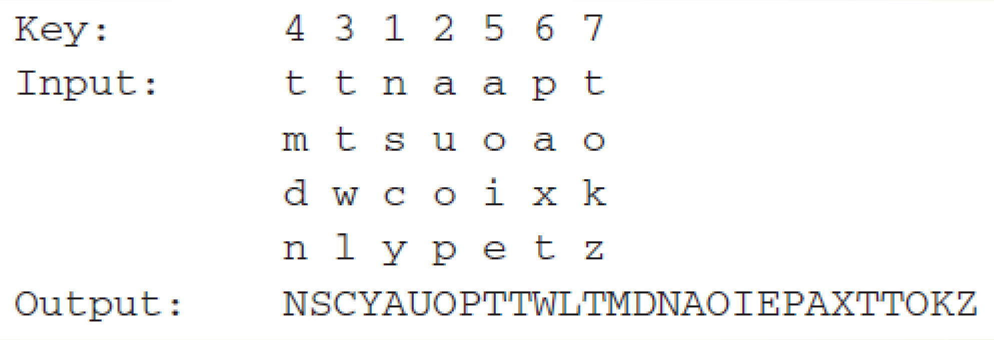
- Here, the key is 4312567.

Columnar Transposition (conti…)

- **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.
- Pure transposition cipher is **easily recognized** because it has the same letter frequencies as the original plaintext.
- **Cryptanalysis** is fairly straightforward and involves laying out the ciphertext in a matrix and playing around with column positions.

Double Tansposition

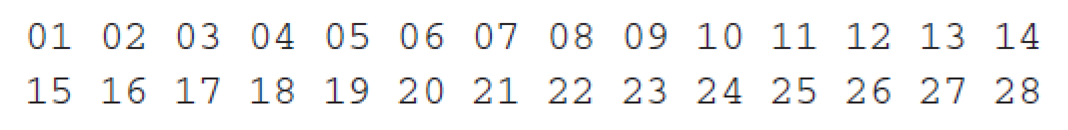
- Double transposition is simply a columnar transposition applied twice.
- The transposition cipher can be made significantly **more secure** by performing more than one stage of transposition.
- Resulting in a more complex permutation that is not easily reconstructed.
- The foregoing message is reencrypted using the same algorithm,



```
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
```

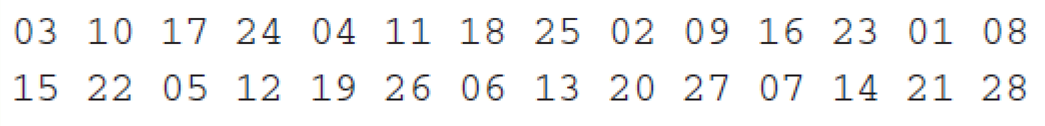
Double Tansposition (conti…)

- the **original sequence** of letters is



```
01 02 03 04 05 06 07 08 09 10 11 12 13 14
15 16 17 18 19 20 21 22 23 24 25 26 27 28
```

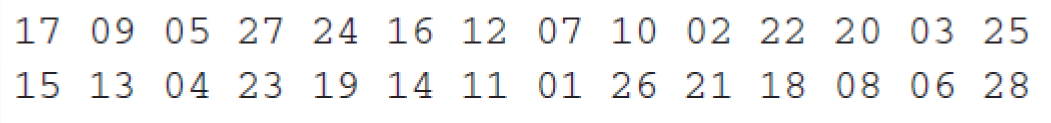
- After the **first transposition**, we have



```
03 10 17 24 04 11 18 25 02 09 16 23 01 08
15 22 05 12 19 26 06 13 20 27 07 14 21 28
```

which has a somewhat regular structure.

- After the **second transposition**, we have

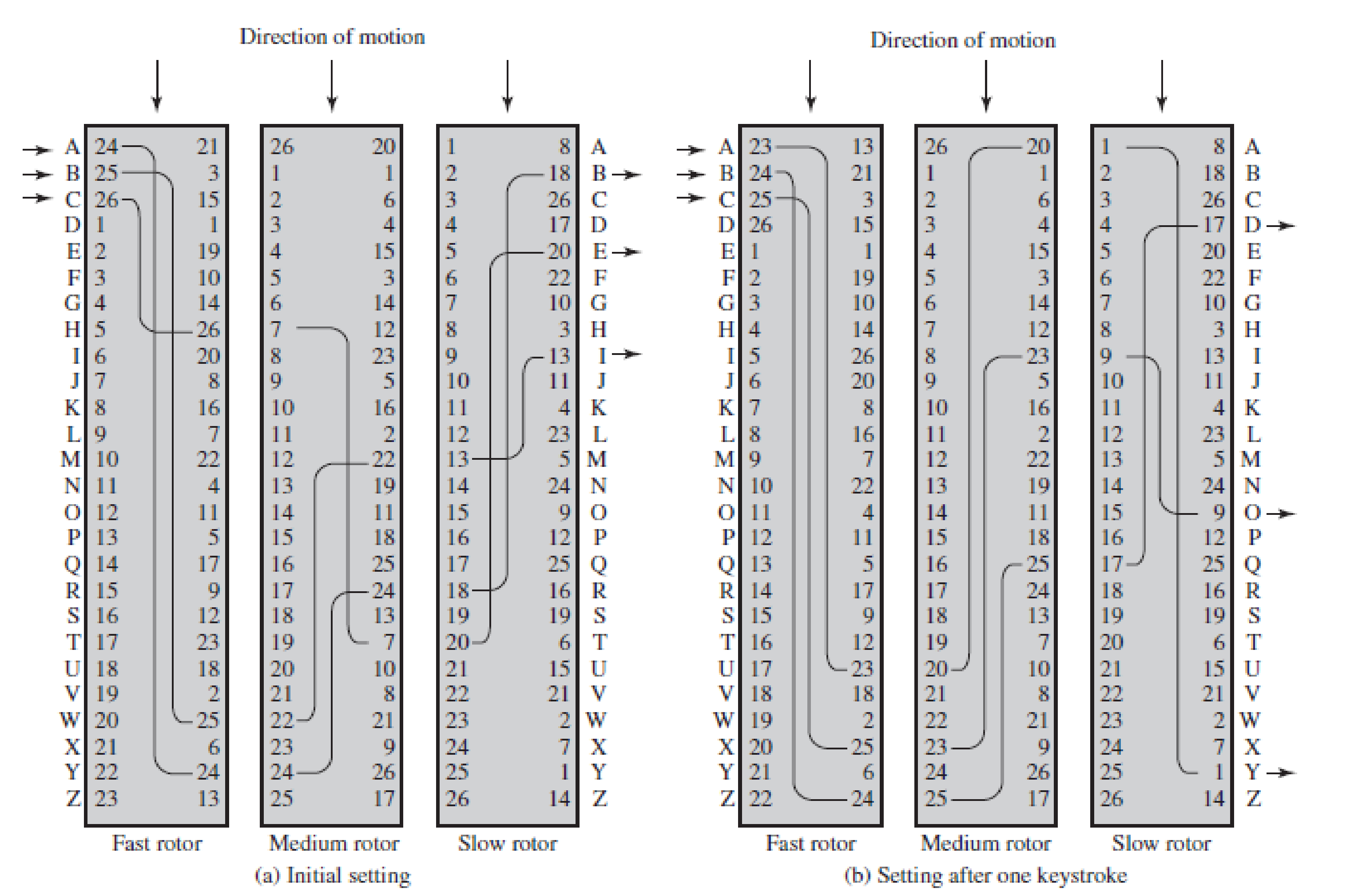


```
17 09 05 27 24 16 12 07 10 02 22 20 03 25
15 13 04 23 19 14 11 01 26 21 18 08 06 28
```

This is a much less structured permutation and is much more **difficult to cryptanalyze.**

ROTOR MACHINES

- The basic principle of the rotor machine is :



(a) Initial setting

A	24	21	26	20	1	8	A
B	25	3	1	1	2	18	B
C	26	15	2	6	3	26	C
D	1	1	3	4	4	17	D
E	2	19	4	15	5	20	E
F	3	10	5	3	6	22	F
G	4	14	6	14	7	10	G
H	5	26	7	12	8	3	H
I	6	20	8	23	9	13	I
J	7	8	9	5	10	11	J
K	8	16	10	16	11	4	K
L	9	7	11	2	12	23	L
M	10	22	12	22	13	5	M
N	11	4	13	19	14	24	N
O	12	11	14	11	15	9	O
P	13	5	15	18	16	12	P
Q	14	17	16	25	17	25	Q
R	15	9	17	24	18	16	R
S	16	12	18	13	19	19	S
T	17	23	19	7	20	6	T
U	18	18	20	10	21	15	U
V	19	2	21	8	22	21	V
W	20	25	22	21	23	2	W
X	21	6	23	9	24	7	X
Y	22	24	24	26	25	1	Y
Z	23	13	25	17	26	14	Z

(b) Setting after one keystroke

A	23	13	26	20	1	8	A
B	24	21	1	1	2	18	B
C	25	3	2	6	3	26	C
D	26	15	3	4	4	17	D
E	1	1	4	15	5	20	E
F	2	19	5	3	6	22	F
G	3	10	6	14	7	10	G
H	4	14	7	12	8	3	H
I	5	26	8	23	9	13	I
J	6	20	9	5	10	11	J
K	7	8	10	16	11	4	K
L	8	16	11	2	12	23	L
M	9	7	12	22	13	5	M
N	10	22	13	19	14	24	N
O	11	4	14	11	15	9	O
P	12	11	15	18	16	12	P
Q	13	5	16	25	17	25	Q
R	14	17	17	24	18	16	R
S	15	9	18	13	19	19	S
T	16	12	19	7	20	6	T
U	17	23	20	10	21	15	U
V	18	18	21	8	22	21	V
W	19	2	22	21	23	2	W
X	20	25	23	9	24	7	X
Y	21	6	24	26	25	1	Y
Z	22	24	25	17	26	14	Z

Rotor Machines (conti…)

- The machine consists of a set of independently rotating cylinders through which electrical pulses can flow.
- Each cylinder has 26 input pins and 26 output pins, with internal wiring that connects each input pin to a unique output pin.
- If we associate each input and output pin with a letter of the alphabet, then a single cylinder defines a **monoalphabetic substitution.**
- After each input key is depressed, the cylinder rotates one position, so that the internal connections are shifted accordingly.
- After 26 letters of plaintext, the cylinder would be back to the initial position.

Rotor Machines (conti…)

- The **power of the rotor machine** is in the use of multiple cylinders, in which the output pins of one cylinder are connected to the input pins of the next.
- The result of using 3 cylinders is 26 * 26 * 26 = 17,576 different substitution alphabets will be used before the system repeats.
- The addition of fourth and fifth rotors results in periods of 456,976 and 11,881,376 letters, respectively.
- The significance of the rotor machine today is that it points the way to the most widely used cipher ever: the Data Encryption Standard (DES).

STEGANOGRAPHY

- The word ***steganography*** comes from Greek word *steganographia*, which combines the words ***steganós*** , meaning "**covered or concealed**", and ***graphia*** meaning "**writing**“.
- **Steganography** is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination.
- The use of **steganography** can be scombined with encryption as an extra step for hiding or protecting data.

First Use

- The first recorded uses of steganography can be traced back to 440 BC in Greece, when **Herodotus** mentions two examples.

1. **Histiaeus** sent a message to his vassal, **Aristagoras**, by shaving the head of his most trusted servant, "marking" the message onto his scalp, then sending him on his way once his hair had regrown, with the instruction, "**When thou art come to Miletus, bid Aristagoras shave thy head, and look thereon**."
2. **Demaratus** sent a warning about a forthcoming attack to Greece by writing it directly on the wooden backing of a wax tablet before applying its beeswax surface. (Wax tablets were in common use then as reusable writing surfaces)

Examples

- **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.
- **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.

Drawbacks

- Steganography drawbacks when compared to encryption.

1. It requires a lot of overhead to hide a relatively few bits of information.
2. Once the system is discovered, it becomes virtually worthless.

Solution to the drawback

- This problem, can be overcome if the insertion method depends on some sort of key.
- The best use of steganography is when a message is first encrypted and then hidden using steganography.

Thank You