Cryptography and System Security (CSS)

Course Code: CSC 604

Subject Incharge

Ankita Karia

Assistant Professor

Room No. 421

email: ankitakaria@sfit.ac.in

COURSE OBJECTIVES

1. To introduce classical encryption techniques and concepts of modular arithmetic and number theory.
2. To explore the working principles and utilities of various cryptographic algorithms including secret key cryptography, hashes and message digests, and public key algorithms
3. To explore the design issues and working principles of various authentication protocols, PKI standards and various secure communication standards including Kerberos, IPsec, and SSL/TLS and email.
4. To develop the ability to use existing cryptographic utilities to build programs for secure communication.

Syllabus Module-wise

Module No.	Unit No.	Topics	Course Outcome
1.0		**Introduction & Number Theory**	**CO 1**
	1.1	Security Goals, Services, Mechanisms and attacks, The OSI security architecture, Network security model, Classical Encryption techniques, Symmetric cipher model, mono-alphabetic and poly- alphabetic substitution techniques: Vigenere cipher, playfair cipher, Hill cipher, transposition techniques: keyed and keyless transposition ciphers, steganography.	To explain system security goals and concepts, classical encryption techniques and acquire fundamental knowledge on the concepts of modular arithmetic and number theory.
	1.2	Modular Arithmetic and Number Theory:- Euclid‘s algorithm—Prime numbers-Fermat‘s and Euler‘s theorem- Testing for primality –The Chinese remainder theorem, Discrete logarithms.	

Syllabus Module-wise

Module No.	Unit No.	Topics	Course Outcome
2.0		**Symmetric and Asymmetric key Cryptography and key Management**	**CO 2** To discuss, compare and apply different encryption and decryption techniques to solve problems related to confidentiality and authentication
	2.1	Block cipher principles, block cipher modes of operation, DES, Double DES, Triple DES, Advanced Encryption Standard (AES), Stream Ciphers: RC5 algorithm.	
	2.2	Public key cryptography: Principles of public key cryptosystems-The RSA algorithm, The knapsack algorithm, ElGamal Algorithm.	
	2.3	Key management techniques: using symmetric and asymmetric algorithms and trusted third party. Diffie Hellman Key exchange algorithm.	

Syllabus Module-wise

Module No.	Unit No.	Topics	Course Outcome
3.0		**Hashes, Message Digests and Digital Certificates**	**CO 3** To apply the knowledge of cryptographic checksums and evaluate the performance of different message digest algorithms for verifying the integrity of varying message sizes.
	3.1	Cryptographic hash functions, Properties of secure hash function, 3 MD5, SHA-1, MAC, HMAC, CMAC.	
	3.2	**Digital Certificate: X.509, PKI**	

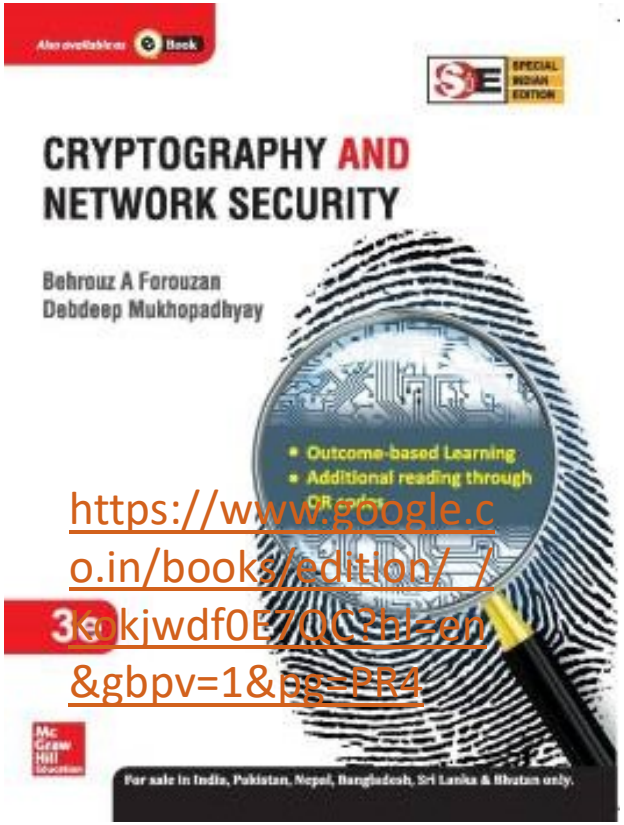
Syllabus Module-wise

Module No.	Unit No.	Topics	Course Outcome
4.0		**Authentication Protocols & Digital signature schemes**	**CO 4**
	4.1	User Authentication and Entity Authentication, One-way and mutual authentication schemes, Needham Schroeder Authentication protocol, Kerberos Authentication protocol.	To apply different digital signature algorithms to achieve authentication and design secure applications
	4.2	Digital Signature Schemes – RSA, EIGamal and Schnorr signature schemes.	

Syllabus Module-wise

Module No.	Unit No.	Topics	Course Outcome
5.0		**Network Security and Applications**	**CO 5** To discuss network security basics, analyze different attacks on networks and evaluate the performance of firewalls and security protocols like SSL, IPSec, and PGP.
	5.1	Network security basics: TCP/IP vulnerabilities (Layer wise), Packet Sniffing, ARP spoofing, port scanning, IP spoofing, TCP syn flood, DNS Spoofing.	
	5.2	Denial of Service: Classic DOS attacks, Source Address spoofing, ICMP flood, SYN flood, UDP flood, Distributed Denial of Service, Defenses against Denial of Service Attacks.	
	5.3	Internet Security Protocols: SSL, IPSEC, Secure Email: PGP, Firewalls, IDS and types, Honey pots	
6.0	6.1	**System Security**	**CO 6** To analyze and apply system security concept to recognize malicious code
		Software Vulnerabilities: Buffer Overflow, Format string, cross-site scripting, SQL injection, Malware: Viruses, Worms, Trojans, Logic Bomb, Bots, Rootkits.	

Text Books to Refer



https://www.google.co.in/books/edition/_/kokjwdf0E7QC?hl=en&gbpv=1&pg=PR4

http://www.cs.vsb.cz/ochodkova/courses/kpb/cryptography-and-network-security_-principles-and-practice-7th-global-edition.pdf

TOPICS TO COVER

1. **Background**

2. **Basic Definitions**

3. **Security Goals**
   - ✓ Confidentiality
   - ✓ Integrity
   - ✓ Availability

The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.

—*The Art of War*, Sun Tzu

Background

1. Human being from ages had two inherent needs –
   (a) to communicate and share information and
   (b) to communicate selectively.
2. These two needs gave rise to the art of coding the messages in such a way that only the intended people could have access to the information.
3. Unauthorized people could not extract any information, even if the scrambled messages fell in their hand.

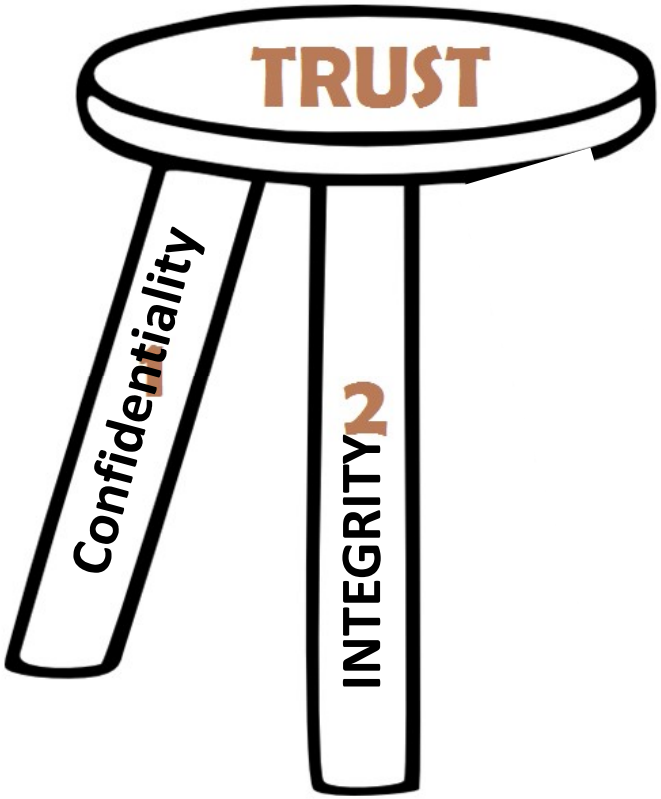
1. Information is an asset that has a value associated to it.
2. As an asset, information needs to be secured from unauthorized access (attacks).
3. With the advent of computers and distributed systems, there should be some mechanism to protect the data which is stored on computers or transmitted through network.

Basic Defintions

THREAT	VULNERABILITY	ATTACK
A possible security violation that might exploit the vulnerability of a system or asset	Refers to a known weakness of an asset that can be exploited by one or more attackers	An action that exploits a vulnerability or enacts a threat
Its origin may be accidental, environmental, human negligence or human failure	It is a weakness that makes threat possible	It is an deliberate unauthorized action on a system or asset.
Types of threat: 1. Interruption 2. Interception 3. Fabrication 4. Modification	This may be because of:- 1. Poor design 2. Configuration mistakes 3. Inappropriate or insecure coding techniques	It will have a motive and will follow a method when opportunity arises.

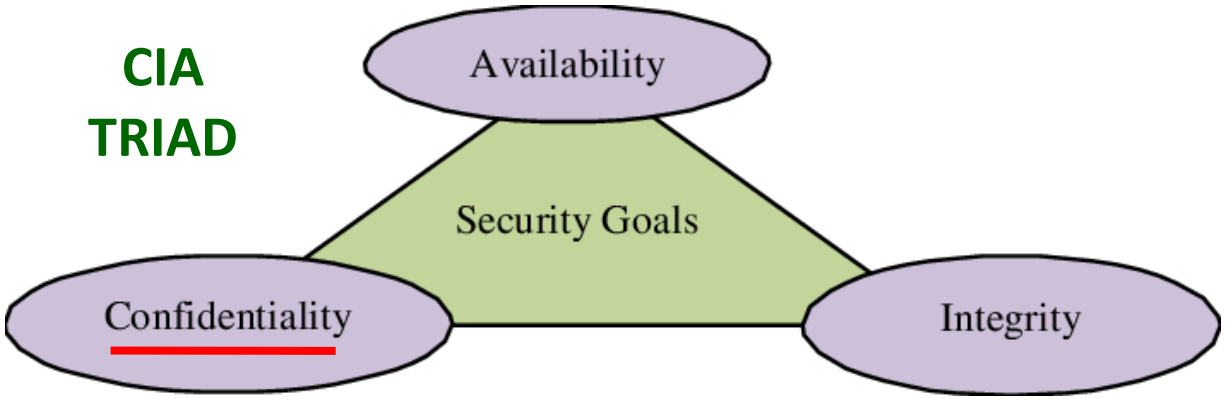
An attack can be classified as : **ACTIVE or PASSIVE** Attack

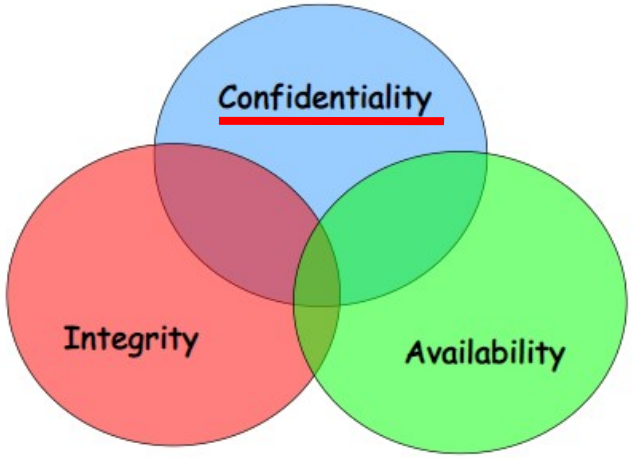
Security Goals



Security Goals

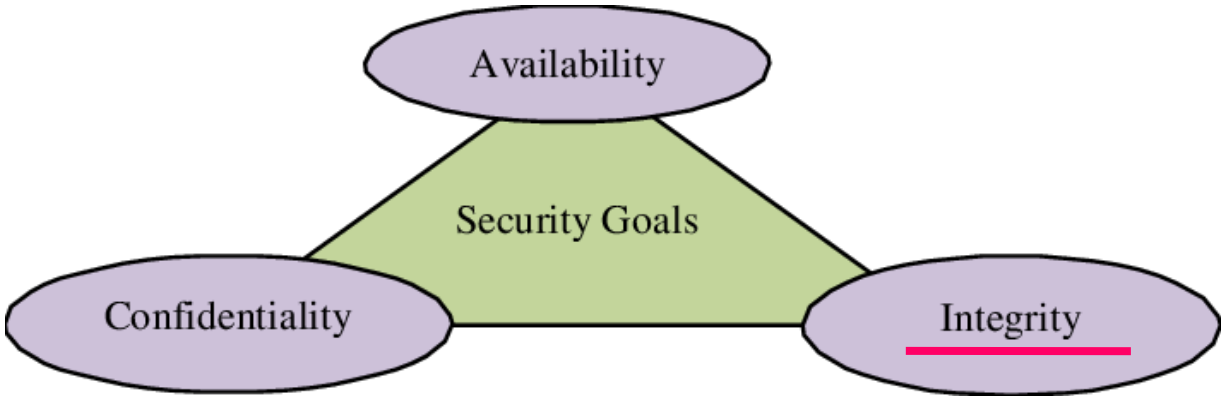
CIA TRIAD

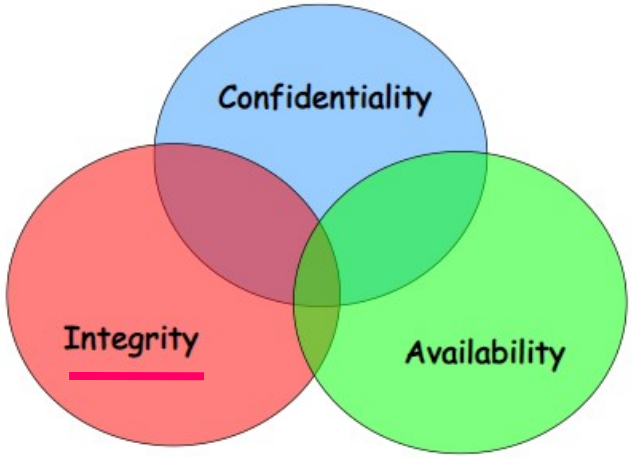




1. Its function is to protect precious/sensitive information from unauthorized persons
2. It ensures that the data is available only to intended and authorized persons
3. Encryption techniques can protect data at rest or in transit and prevents unauthorized access to protected data.

Security Goals

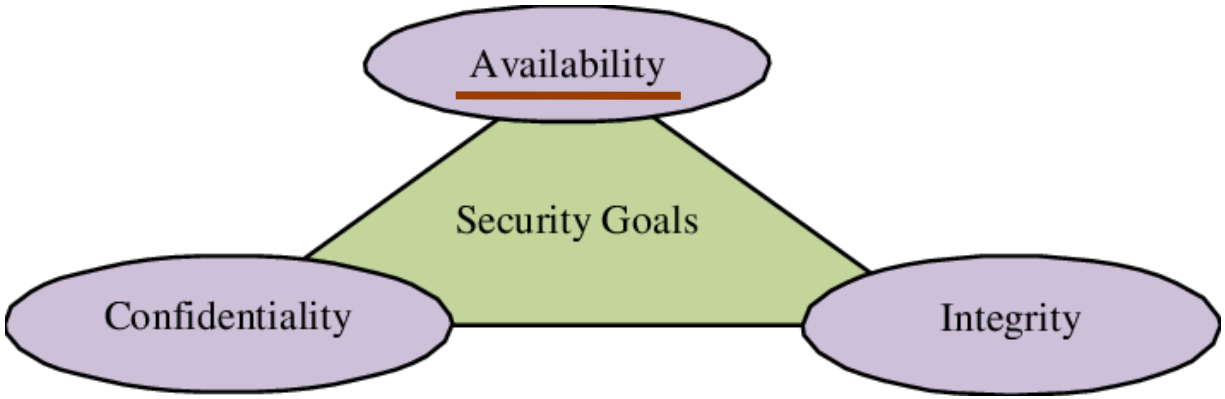


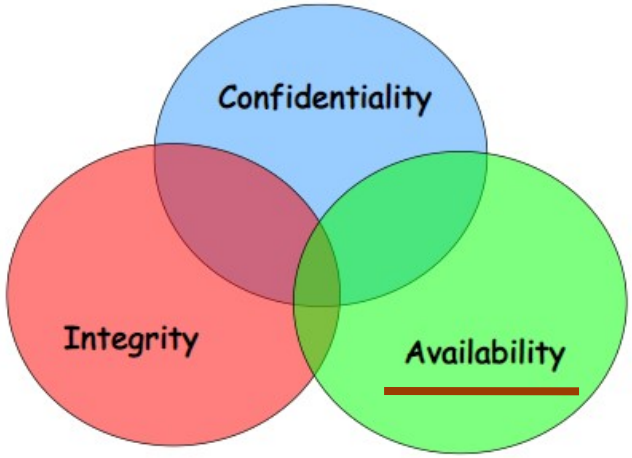


1. Aims at maintaining and assuring the accuracy and consistency of data
2. Its function is to make sure that the data is accurate and reliable and is not allowed by unauthorized persons or hackers
3. Integrity violation is not necessarily the result of malicious act; an interruption in the system may also create unwanted changes in some information.

HASHING AND CHECKSUMS

Security Goals

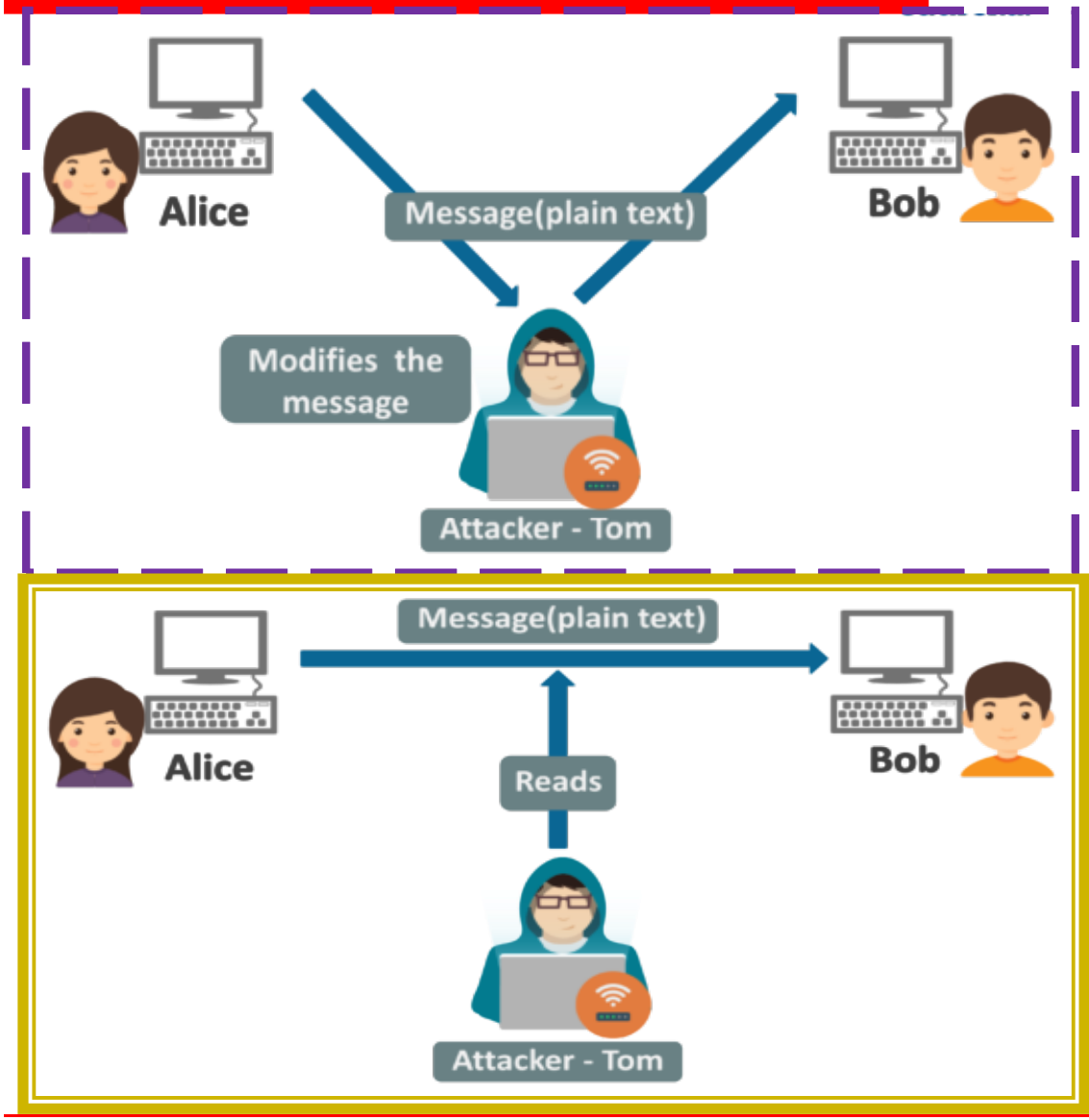




1. Information is useless if it is not available.
2. Function:- To make sure that the data , network resources are continuously available to the legitimate users whenever required.
3. Resolving hardware and software conflicts, along with regular maintenance is crucial to keep the system up and available.

LOAD BALANCER, RAID or SERVER CLUSTERING

Types of Attacks



ACTIVE ATTACK

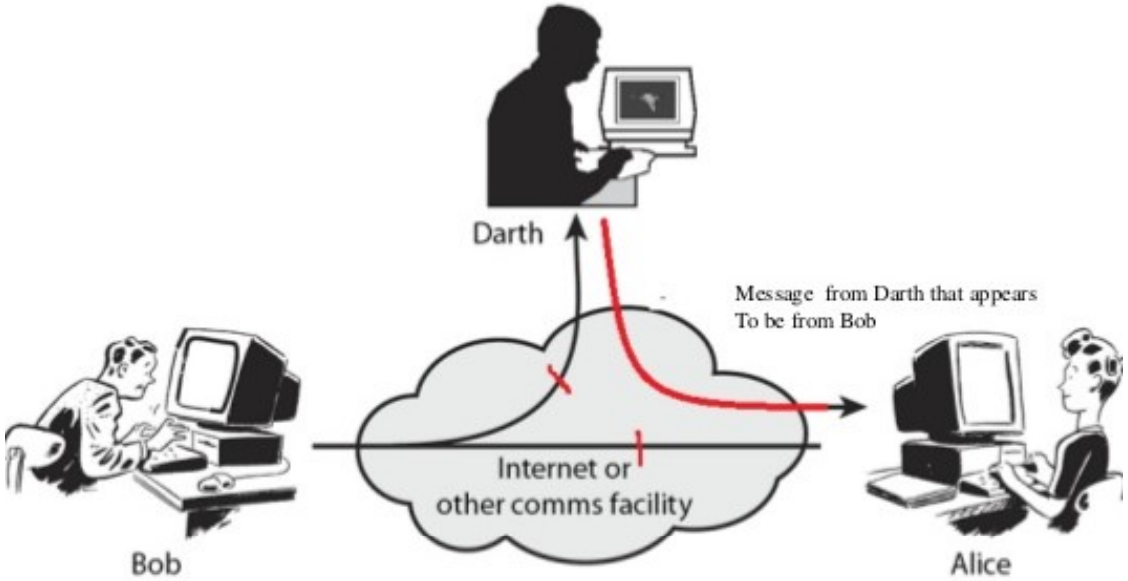
PASSIVE ATTACK

Types of Attacks

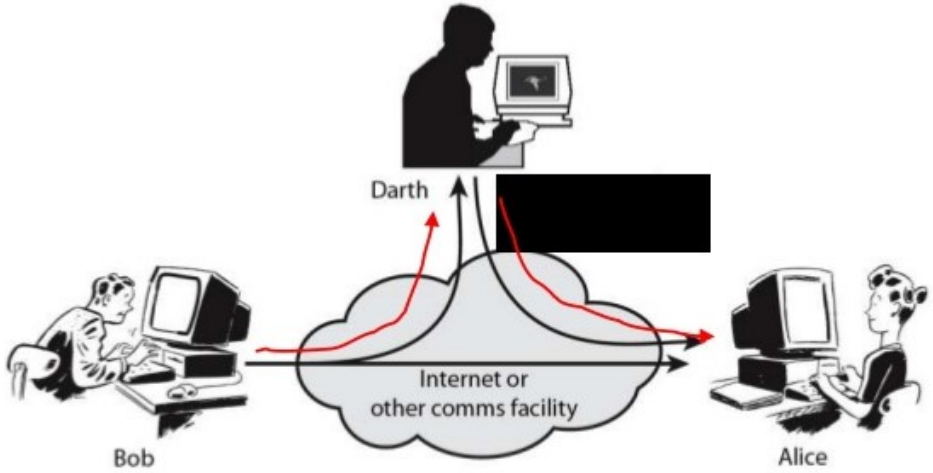
ACTIVE ATTACK

1. Are attacks in which the hacker attempts to change or transform the content of the message or information
2. An active attack attempts to alter system resources or effect their operations
3. These attacks are threat to **THE INTEGRITY** and **AVAILABILITY** of the system.
4. **EASIER TO DETECT THAN TO PREVENT**
5. Thus, instead of preventing, emphasis should be on detection of attack and recovery from any disruption or delay caused by it.

Types of ACTIVE Attacks

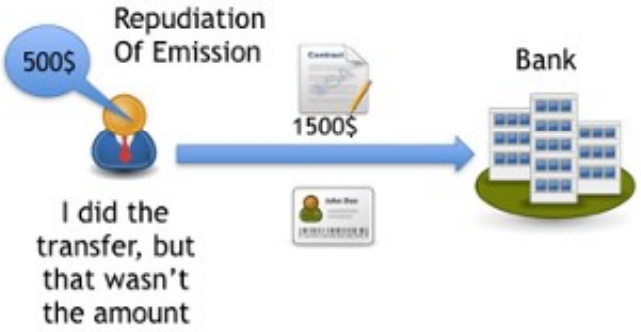


MASQUERADE



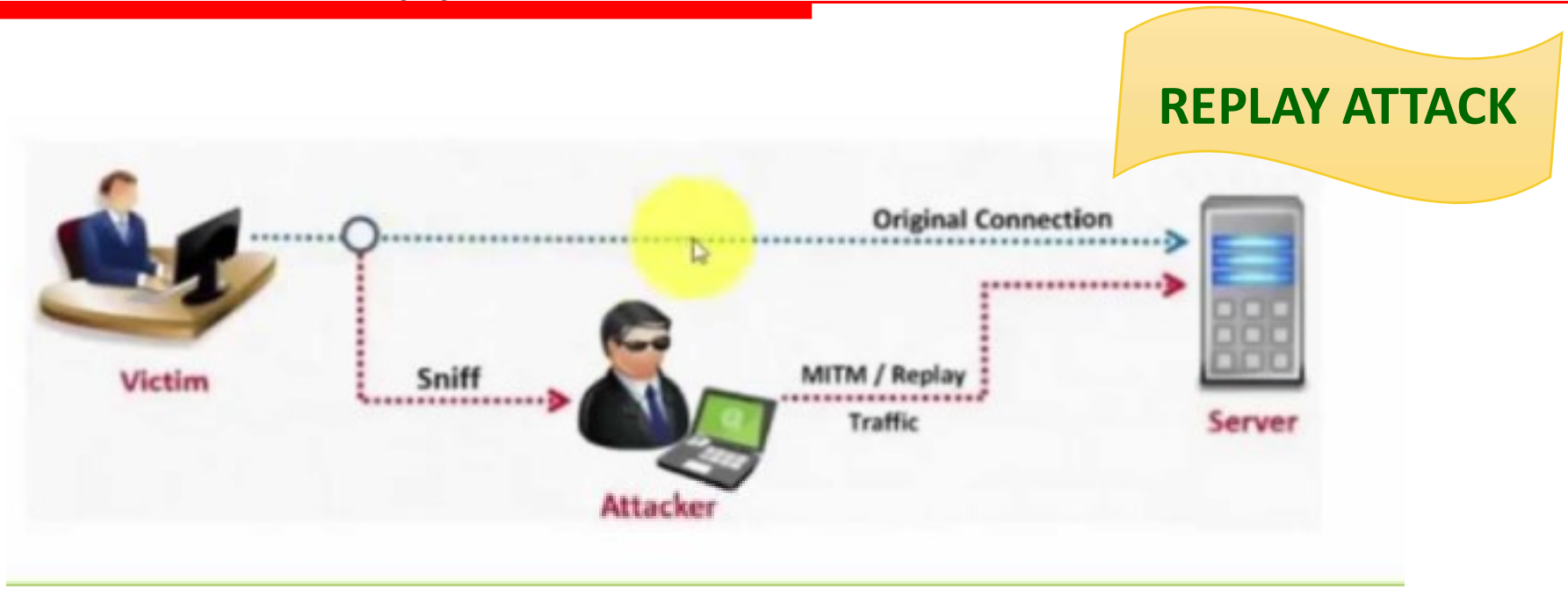
MODIFICATION OF MESSAGES

Types of ACTIVE Attacks



REPUDIATION

Types of ACTIVE Attacks



Denial of Service (DoS): DoS is one of the oldest forms of attack. It may slow down or totally interrupt the service of a system

EXAMPLE: If a railway website is brought down, it fails to serve the people who want to book tickets.

- There is another form of DoS attack called a DDoS attack. A DoS attack uses a single computer to carry out the attack. A DDoS attack uses a series of computers to carry out the attack. Sometimes the target server is flooded with so much data that it can’t handle it. Another way is to exploit the workings of internal protocols. A DDoS attack that deals with extortion is often termed a ransom DDoS. We will now talk about various types of the DoS attacks that might occur.

Types of Attacks

PASSIVE ATTACK

1. Are the ones in which the attacker observes all the messages and copies the content of messages
2. They focus on monitoring all the transmission and gaining the data
3. No potential harm to the system.
4. But significant danger to your data's **CONFIDENTIALITY.**
5. **DIFFICULT TO DETECT.**
6. **PREVENTION IS POSIBLE** using some **ENCRYPTION** techniques

Types of PASSIVE ATTACK

1. RELEASE OF MESSAGGE CONTENT (SNOOPING)

Snooping refers to unauthorized access to or interception of data.

2. TRAFFIC ANALYSIS

Traffic analysis refers to obtaining some other type of information by monitoring online traffic.

SUMMARY OF ATTACKS

ACTIVE ATTACKS

1. Masquerade
2. Modification of messages
3. Repudiation
4. Replaying
5. Denial of Service

PASSIVE ATTACKS

1. Release of messages
2. Traffic Analysis

Active vs. Passive Attack

ACTIVE ATTACK	PASSIVE ATTACK
Tries to change the system resources or affect their operation.	Tries to read or make use of information from the system but does not influence system resources.
Modification in information take place.	Modification in the information does not take place.
It is danger for Integrity as well as availability.	Passive Attack is danger for Confidentiality.
In active attack attention is on detection.	While in passive attack attention is on prevention.
Due to active attack system is always damaged.	While due to passive attack, there is no any harm to the system.
Victim gets informed about the attack.	Victim does not get informed about the attack.
information collected through passive attacks are used during executing.	While passive attack are performed by collecting the information such as passwords, messages by itself.

Active vs. Passive Attack

Attacks	*Passive/Active*	*Threatening*
Snooping Traffic analysis	Passive	Confidentiality
Modification Masquerading Replaying Repudiation	Active	Integrity
Denial of service	Active	Availability

Security Service

- ITU-T provides some security services and some mechanisms to implement those services
- Security and mechanisms are closely related.
- A security service makes use **of one or more security mechanisms**

TYPES OF SECURITY SERVICES

1. **Data Confidentiality**
2. **Data Integrity**
3. **Authentication**
4. **Non-Repudiation**
5. **Access Control**

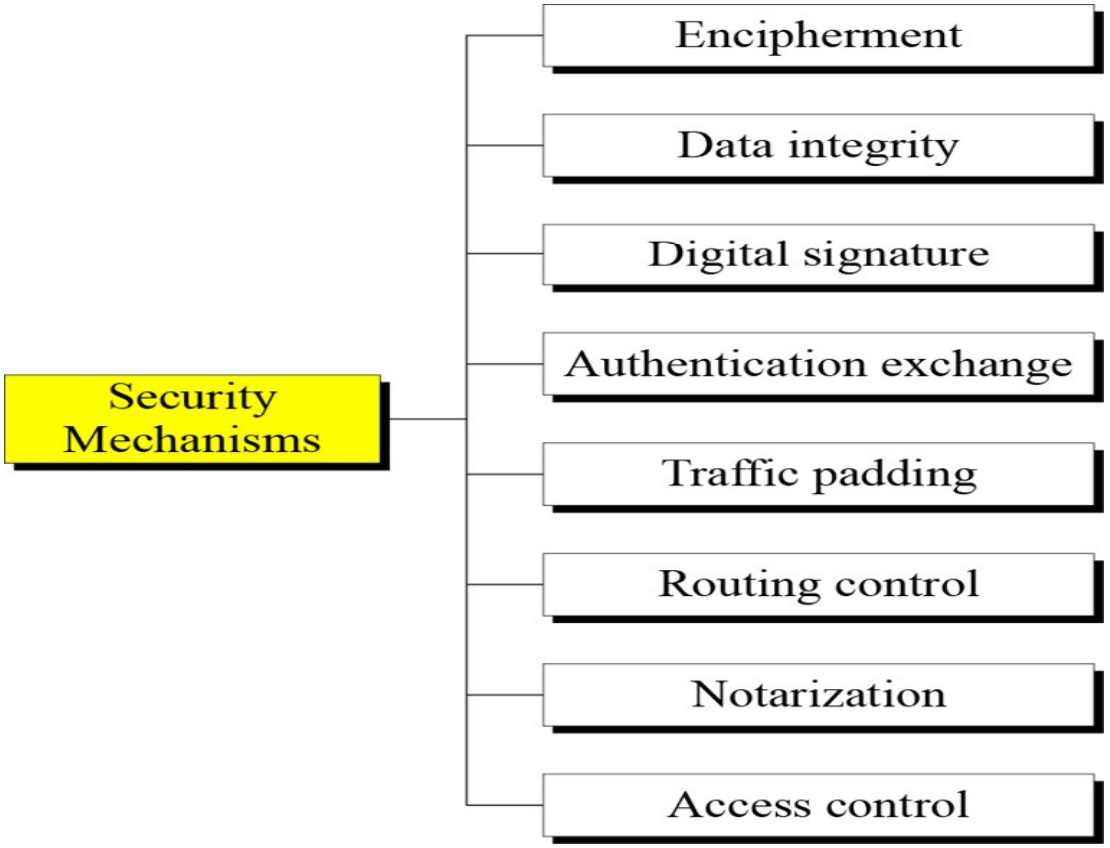
Security Services (X.800)

X.800 defines security services in 5 major categories

- **Data Confidentiality** –protection of data from unauthorized disclosure
- **Data Integrity** - assurance that data received is as sent by an authorized entity
- **Authentication -** assurance that the communicating entity is the one claimed
- **Non-Repudiation -** protection against denial by one of the parties in a communication
- **Access Control -** prevention of the unauthorized use of a resource

Security Mechanism

A mechanism that is designed to detect, prevent, or recover from a security attack



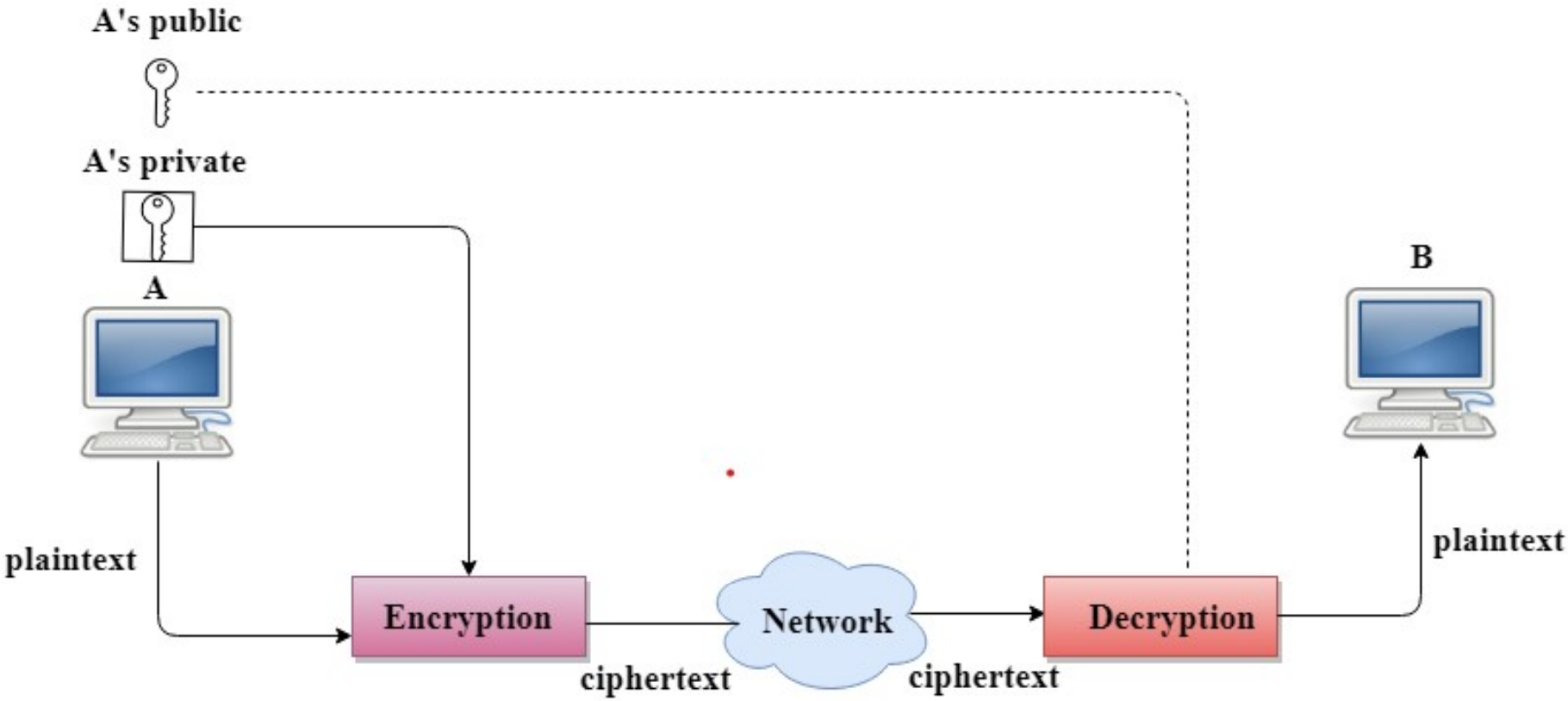
Security Mechanisms

1. **Encipherment:** This security mechanism deals with hiding and covering of data which helps data to become confidential.

2. **Data Integrity:** This security mechanism is used by appending value to data to which is created by data itself.

3. **Digital Signature:** This security mechanism is achieved by adding digital data that is not visible to eyes. It is form of electronic signature which is added by sender which is checked by receiver electronically.

4. **Authentication Exchange:** Two entities exchange some messages to prove their identity to each other.


A's public
A's private
A
B
plaintext
Encryption
Network
Decryption
plaintext
ciphertext
ciphertext

Security Mechanisms

5. **Traffic Padding:** Means inserting some bogus data into the data traffic to thwart the adversary's attempt to use the traffic analysis

6. **Routing Control:** Means selecting and continuously changing different available router between sender and receiver to prevent the opponent from eavesdropping on a particular route.

7. **Notarization:** This security mechanism involves use of trusted third party in communication. It acts as mediator between sender and receiver so that if any chance of conflict is reduced. This mediator keeps record of requests made by sender to receiver for later denied.

8. **Access Control:** This mechanism is used to stop unattended access to data which you are sending. It can be achieved by various techniques such as applying passwords, using firewall, or just by adding PIN to data.

Relation between Services and Mechanisms

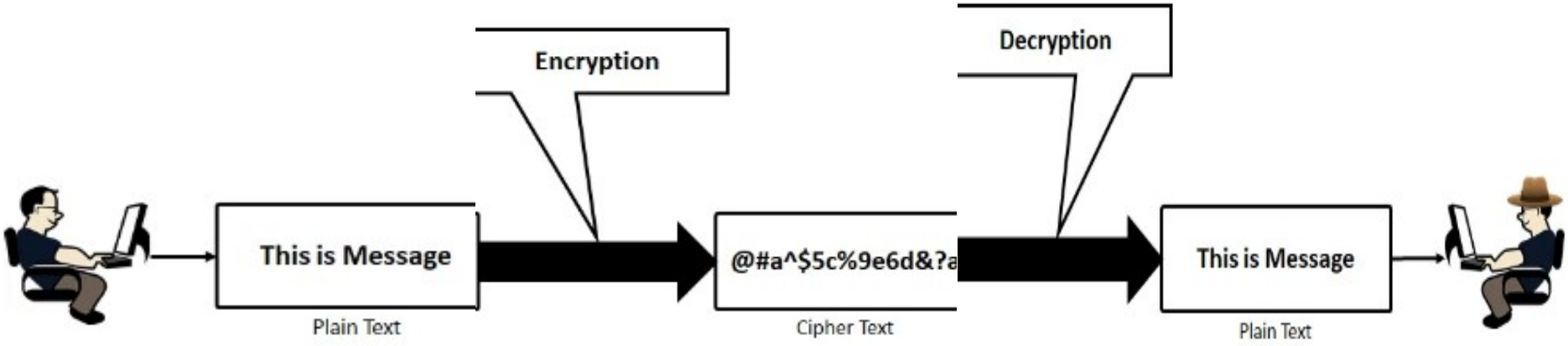
Security Service	*Security Mechanism*
Data confidentiality	Encipherment and routing control
Data integrity	Encipherment, digital signature, data integrity
Authentication	Encipherment, digital signature, authentication exchanges
Nonrepudiation	Digital signature, data integrity, and notarization
Access control	Access control mechanism

1. **Plaintext:** Original text
2. **Cipher text:** Coded or scrambled message produced as output
3. **Encryption or Enciphering:** converts original text into ciphertext.
4. **Decryption or Deciphering:** Restoring the plaintext from ciphertext
5. **Secret Key:** Set of values that is provided as an input to encryption algorithm in order to produce cipher text
6. **Cryptography:** Various schemes used for encryption constitute the area of study known as Cryptography
7. **Cryptanalysis:** breaking of "secret codes"
8. **Cryptology: Cryptography + Cryptanalysis**

   Cryptology is the art and science of making and breaking "secret codes"

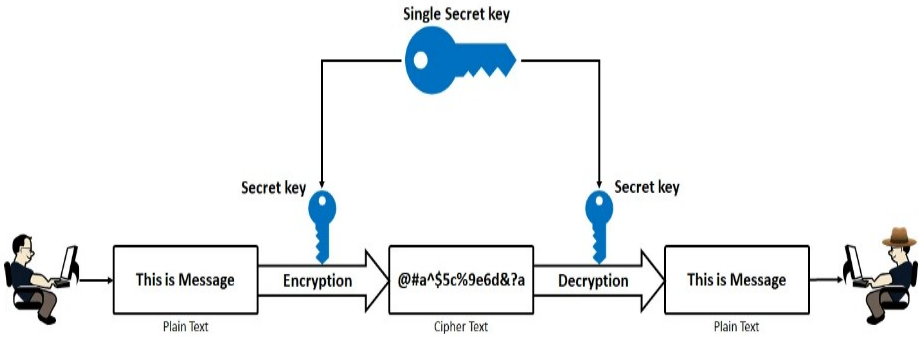
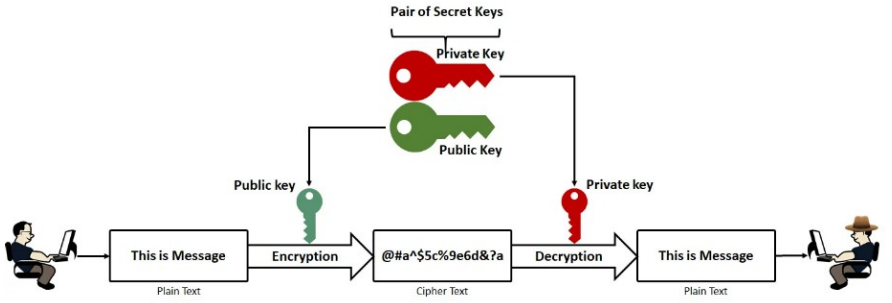
TYPES OF CRYPTOGRAPHY

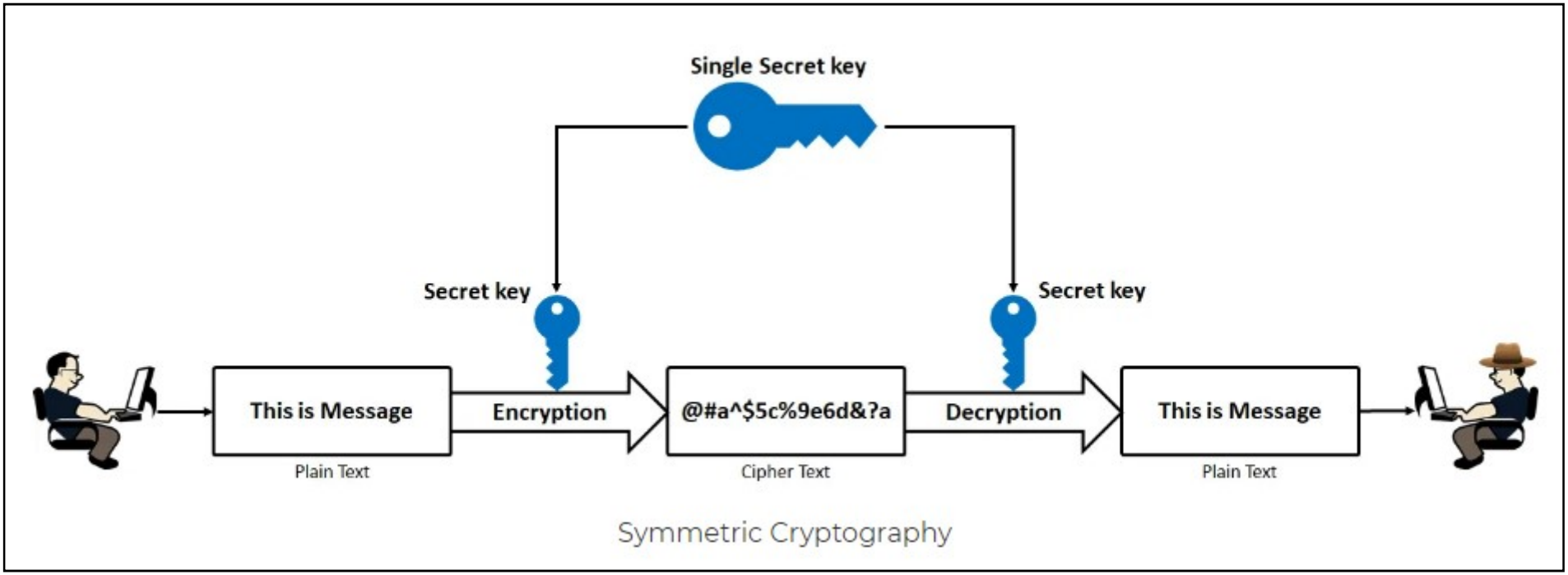
- Crypt – ‘hidden’ Graphy – ‘writing’.
- In layman language, hiding information from the outside world and let only the right receiver know how to see it.
- Cryptography is technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it. Thus preventing unauthorized access to information

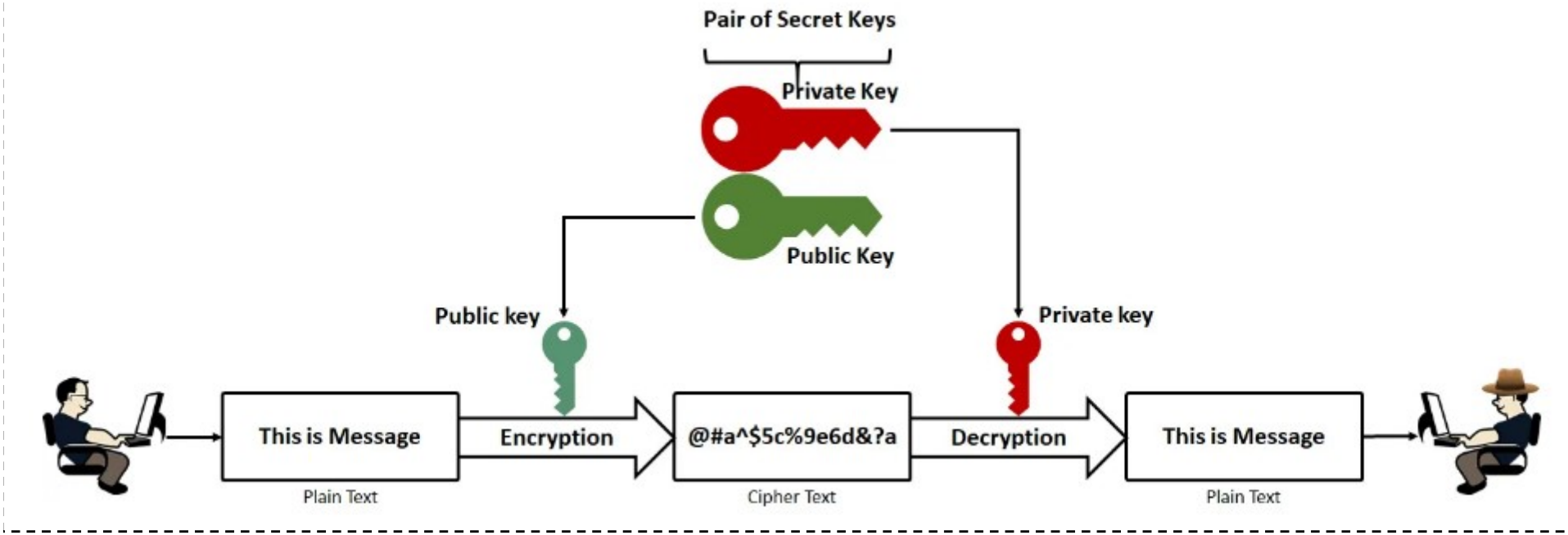


TYPES OF CRYPTOGRAPHY

Based on **types of keys** used for encryption and decryption operations, there are **two** types of cryptography

Symmetric Key Cryptography	Asymmetric Key Cryptography
Also called Private key Cryptography	Also called as Public-key cryptography
Both the sender and receiver will use the same key for encrypting and decrypting the message.	·A public key is used for encryption and a private key is used for decryption
	


Single Secret key
Secret key
Secret key
This is Message
Encryption
@#a^$5c%9e6d&?a
Decryption
This is Message
Plain Text
Cipher Text
Plain Text
Symmetric Cryptography

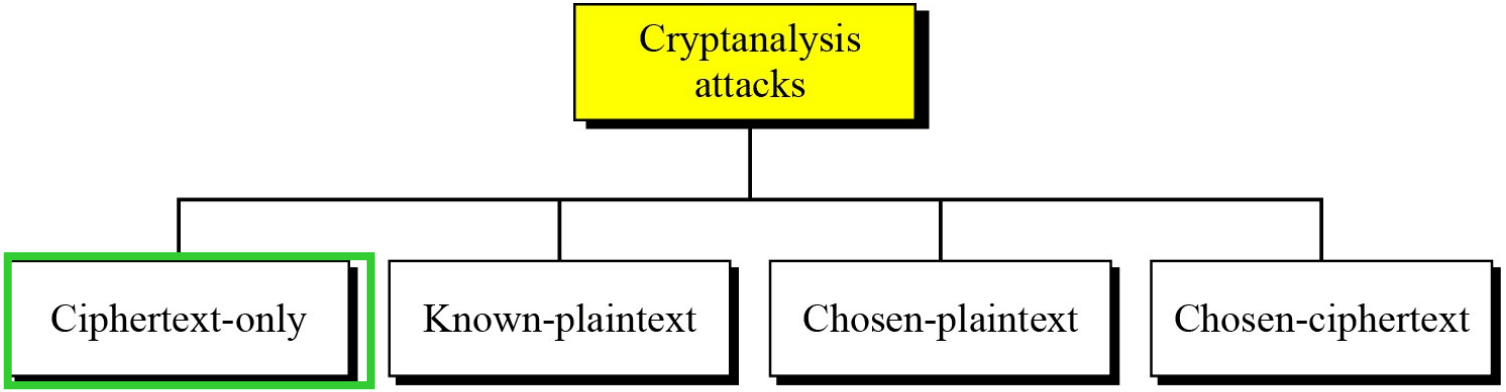

Pair of Secret Keys
Private Key
Public Key
Public key
Private key
This is Message
Encryption
@#a^$5c%9e6d&?a
Decryption
This is Message
Plain Text
Cipher Text
Plain Text

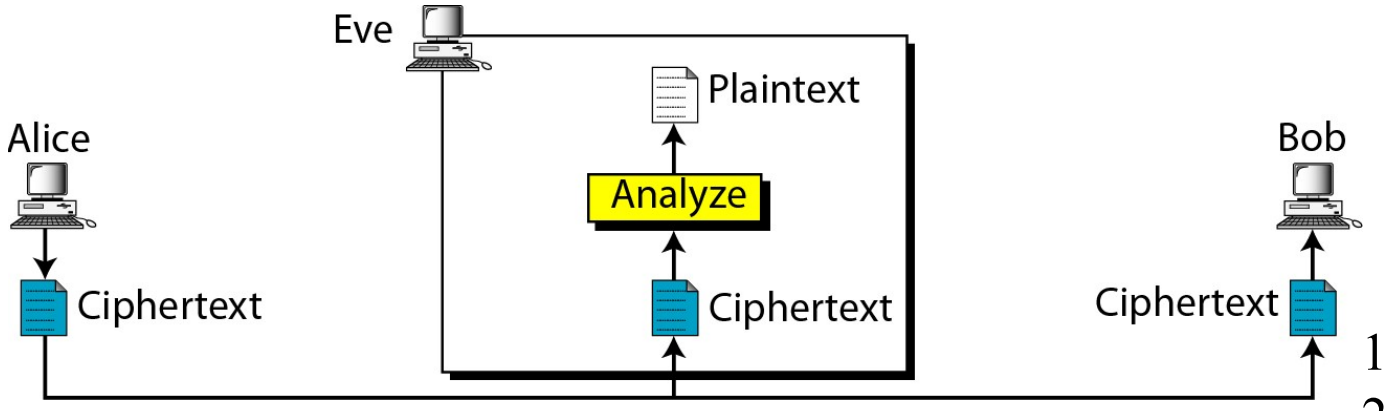
1. **Plaintext:** Original text
2. **Cipher text:** Coded or scrambled message produced as output
3. **Encryption or Enciphering:** converts original text into ciphertext.
4. **Decryption or Deciphering:** Restoring the plaintext from ciphertext
5. **Secret Key:** Set of values that is provided as an input to encryption algorithm in order to produce cipher text
6. **Cryptography:** Various schemes used for encryption constitute the area of study known as Cryptography
7. **Cryptanalysis:** breaking of "secret codes"
8. **Cryptology: Cryptography + Cryptanalysis**

   Cryptology is the art and science of making and breaking "secret codes"

TYPES OF CRYPTANALYSIS ATTACK

As cryptography is the science and art of creating secret codes, cryptanalysis is the science and art of breaking those codes

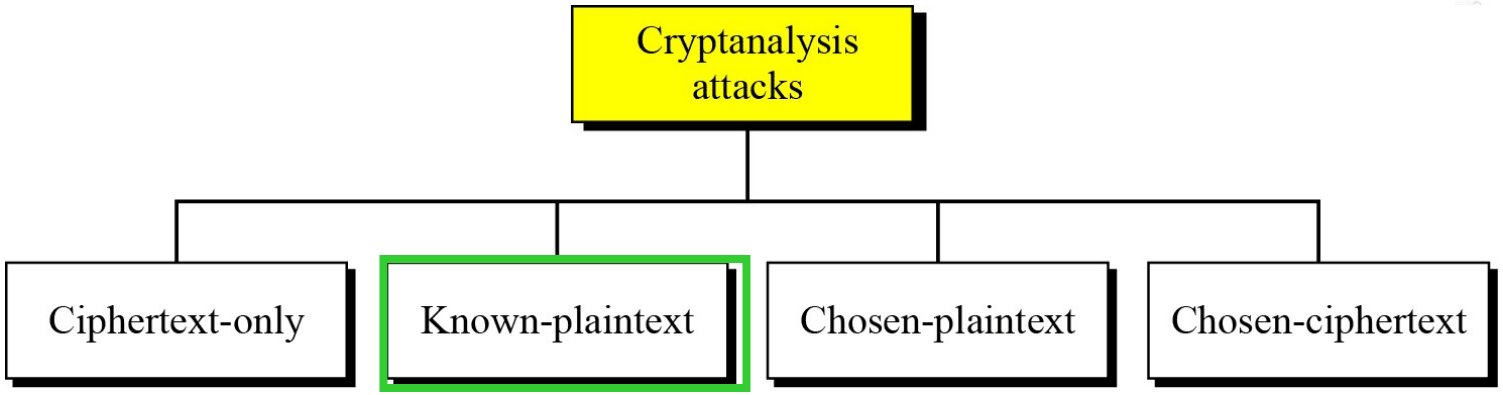


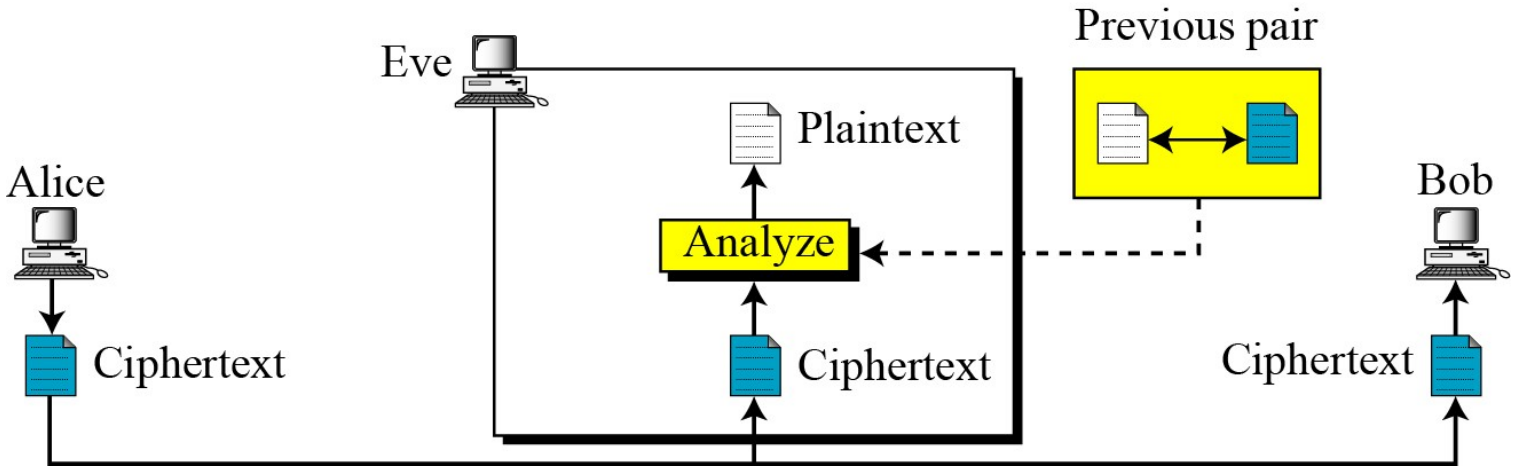


1. Brute Force Attack
2. Statistical Attack
3. Pattern Attack

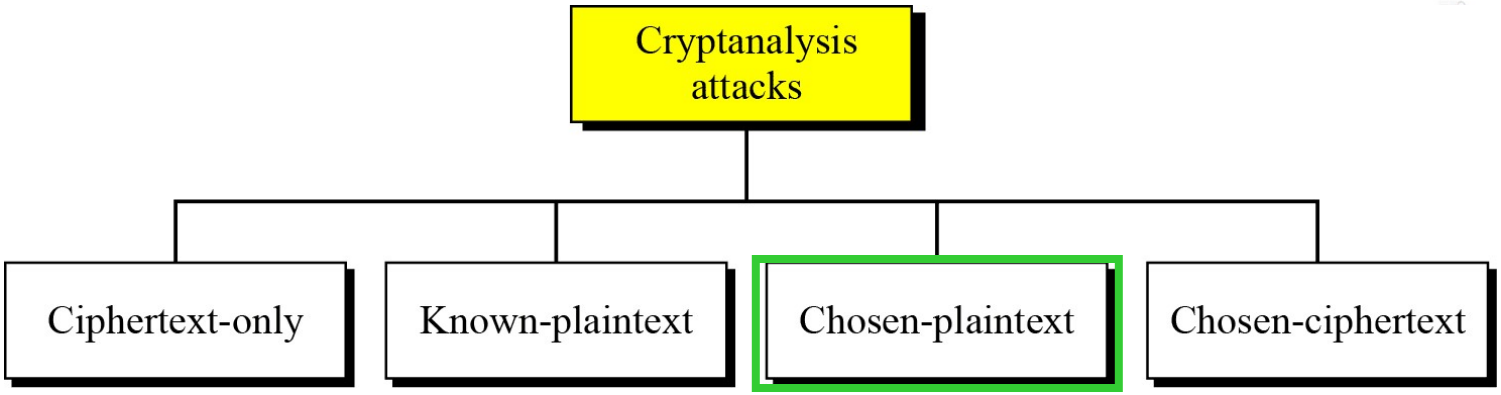
Letter	*Frequency*	*Letter*	*Frequency*	*Letter*	*Frequency*	*Letter*	*Frequency*
E	12.7	H	6.1	W	2.3	K	0.08
T	9.1	R	6.0	F	2.2	J	0.02
A	8.2	D	4.3	G	2.0	Q	0.01
O	7.5	L	4.0	Y	2.0	X	0.01
I	7.0	C	2.8	P	1.9	Z	0.01
N	6.7	U	2.8	B	1.5		
S	6.3	M	2.4	V	1.0		

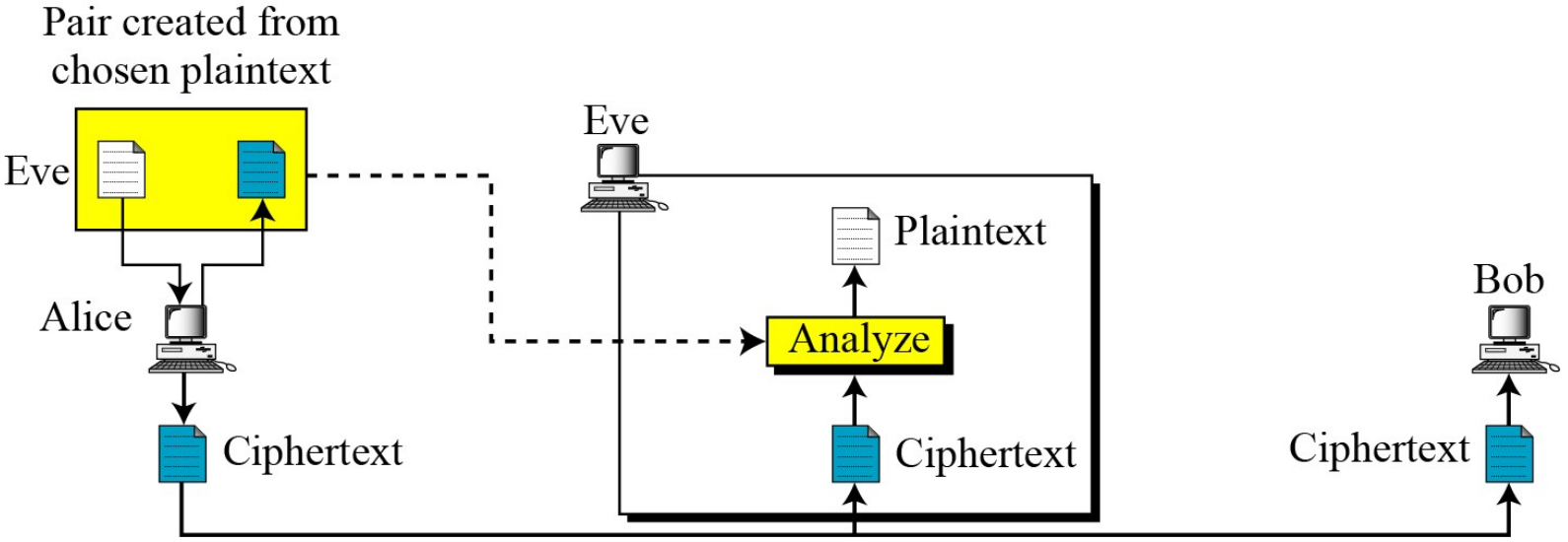
TYPES OF CRYPTANALYSIS ATTACK



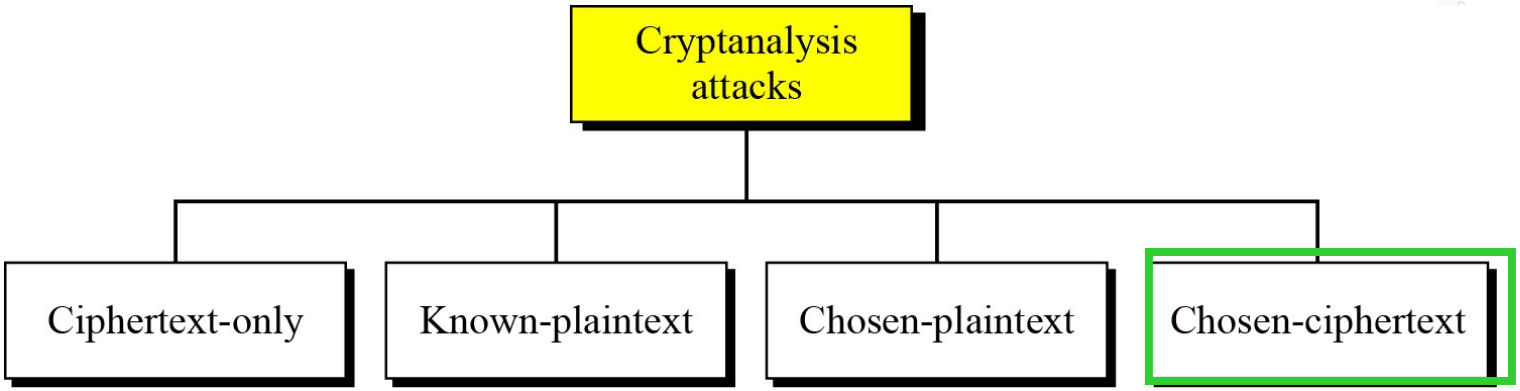


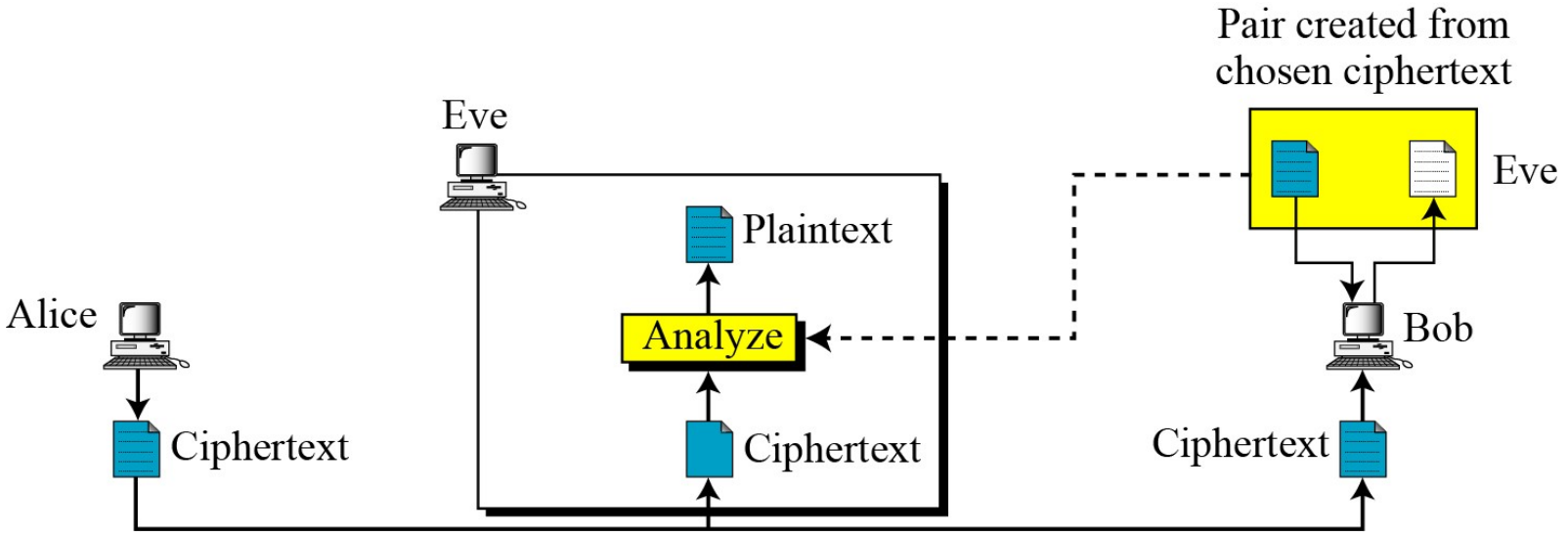
TYPES OF CRYPTANALYSIS ATTACK



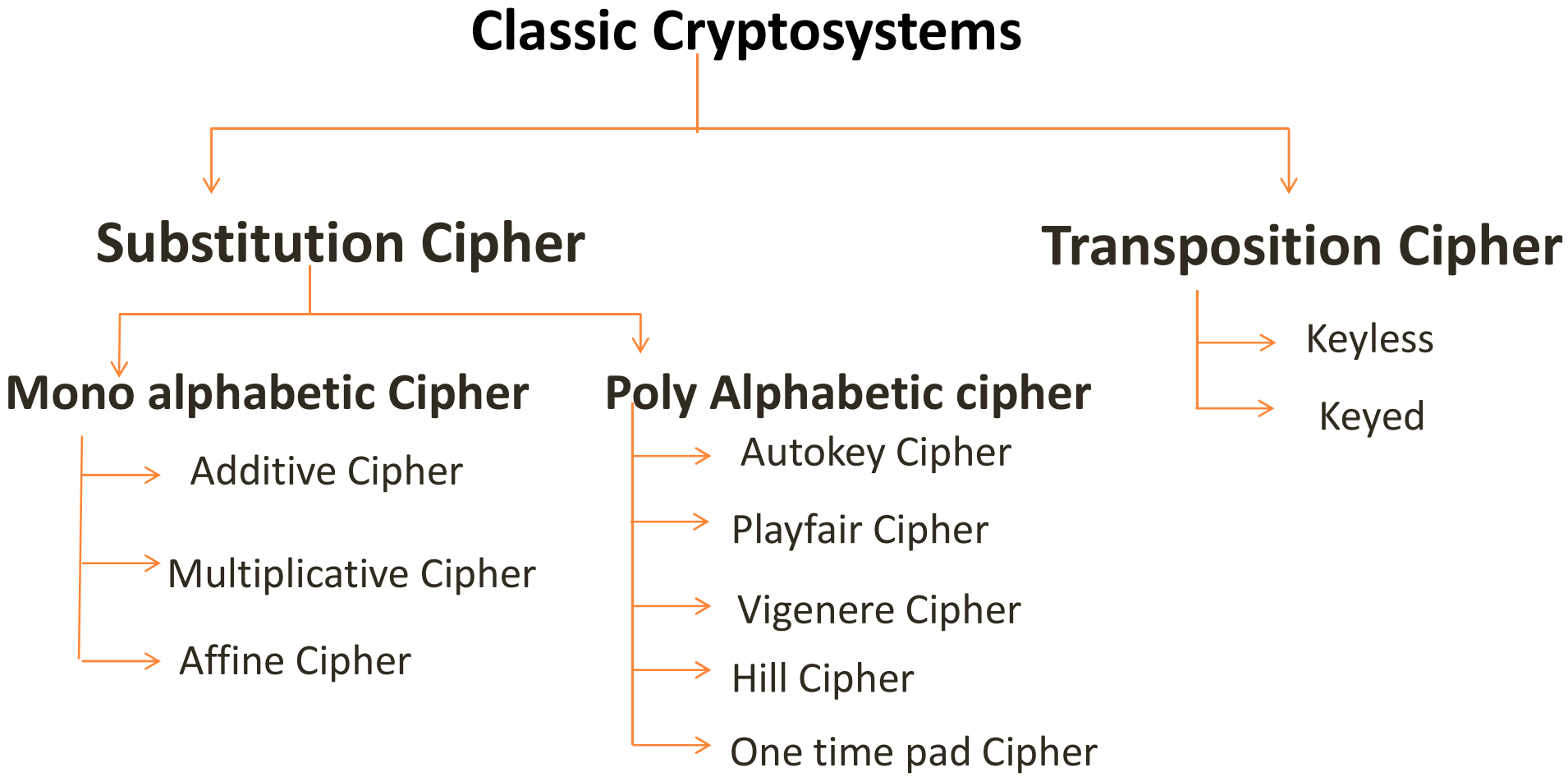


TYPES OF CRYPTANALYSIS ATTACK





CATEGORIES OF TRADITIONAL CIPHERS



SUBSTITUTION CIPHER

1. A substitution cipher replaces one symbol with another.
2. Substitution ciphers can be categorized as either **monoalphabetic ciphers or polyalphabetic ciphers.**

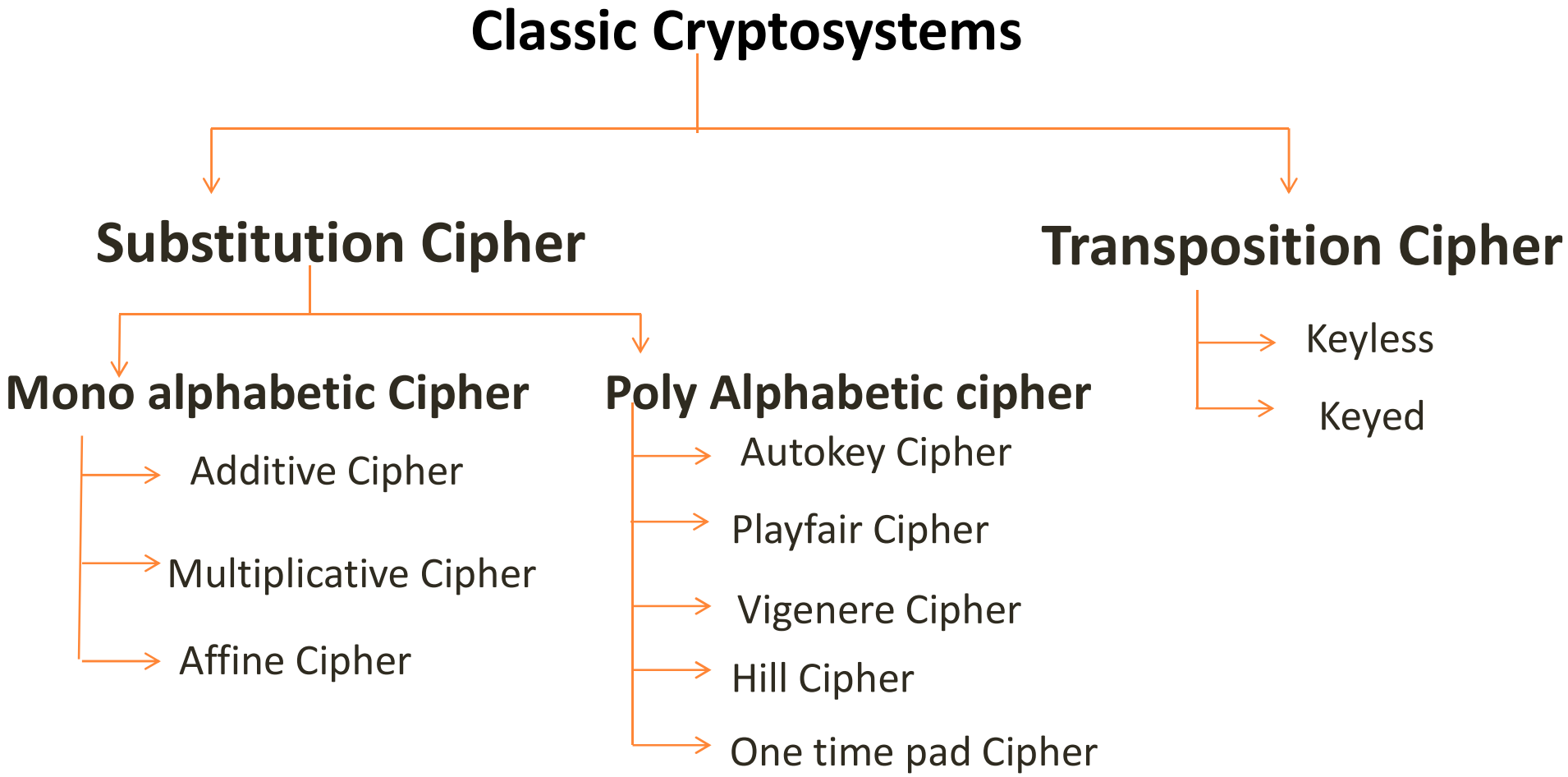
Monoalphabetic Ciphers

In monoalphabetic substitution, the relationship between a symbol in the plaintext to a symbol in the ciphertext is always one-to-one.

Plaintext: hello **Ciphertext:** KHOOR

Plaintext: hello **Ciphertext:** **ABNZF**

CATEGORIES OF TRADITIONAL CIPHERS



ADDITIVE CIPHER

1. Also called as SHIFT CIPHER and sometimes as “CAESAR CIPHER”.
2. The term additive cipher better reveals its mathematical nature.

ENCRYPTION

$$C = (P + k) \bmod 26$$

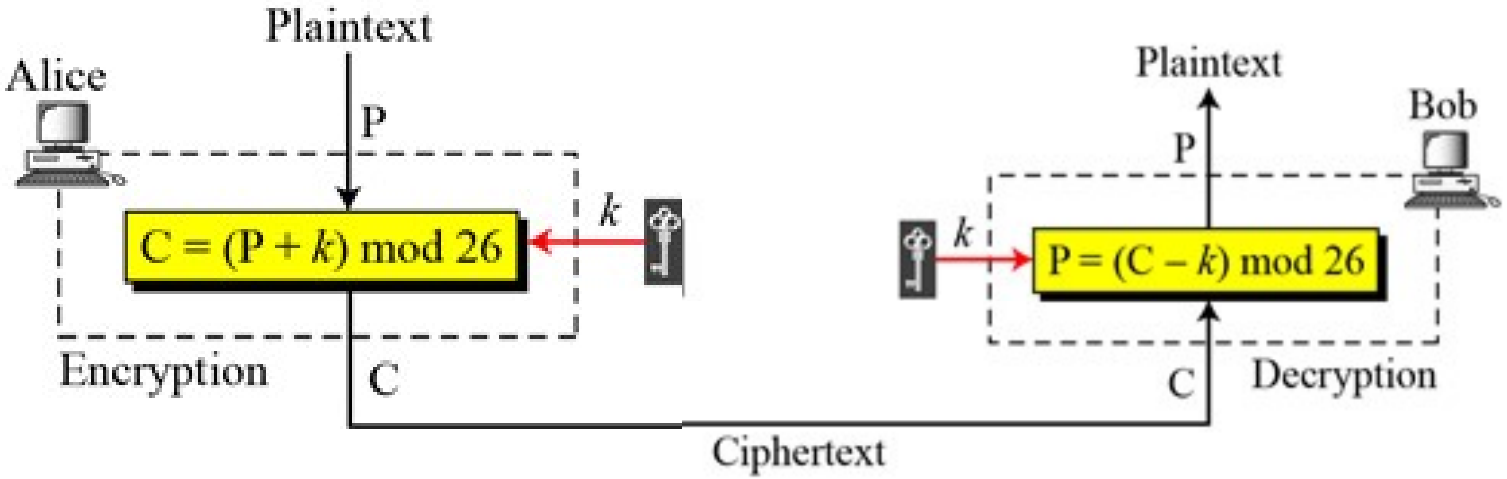
DECRYPTION

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

Plaintext →	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
Ciphertext →	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
Value →	00	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

When the cipher is additive, the plaintext, ciphertext, and key are integers in Z26.

Additive Cipher



Plaintext →	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
Ciphertext →	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
Value →	00	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

Use the additive cipher with key = 15 to encrypt the message "hello".

Solution

We apply the encryption algorithm to the plaintext, character by character:

PLAIN TEXT	ENCRYPTION	CIPHERTEXT
h → 07	(07 + 15) mod 26	22 → W
e → 04	(04 + 15) mod 26	19 → T
l → 11	(11 + 15) mod 26	00 → A
l → 11	(11 + 15) mod 26	00 → A
o → 14	(14 + 15) mod 26	03 → D

hello → ENCRYPTED → **WTAAD**

ENCRYPTION
C = (P + k) mod 26

Plaintext →	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
Ciphertext →	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
Value →	00	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

DECRYPTION

Solution: **P = (C - k) mod 26**

We apply the decryption algorithm to the plaintext character by ch aracter:

Ciphertext: W → 22	Decryption: (22 – 15) mod 26	Plaintext: 07 → h
Ciphertext: T → 19	Decryption: (19 – 15) mod 26	Plaintext: 04 → e
Ciphertext: A → 00	Decryption: (00 – 15) mod 26	Plaintext: 11 → l
Ciphertext: A → 00	Decryption: (00 – 15) mod 26	Plaintext: 11 → l
Ciphertext: D → 03	Decryption: (03 – 15) mod 26	Plaintext: 14 → o

hello ← DECRYPTION **WTAAD**

SHIFT CIPHER and CAESAR CIPHER

- Historically, additive ciphers are called **Shift Ciphers.**
- Julius Caesar used an additive cipher to communicate with his officers.
- For this reason, additive ciphers are sometimes referred to as the **Caesar cipher.**
- Caesar used a **key of 3** for his communications.

Note

Additive ciphers are sometimes referred to as shift ciphers or Caesar cipher.

CRYPTANALYSIS OF ADDITIVE CIPHER

- Are vulnerable to CIPHER TEXT ONLY Attack using Exhaustive key searches.
- The key domain of Additive cipher is very small i.e. only 26 keys
- Since one of the key is ZERO, we are left with only 25 keys, due to which an attacker can easily launch a BRUTE – FORCE ATTACK on Ciphertext

ADDITIVE CIPHER are Subject to

1. BRUTE FORCE ATTACK
2. STATISTICAL ATTACK

Example 3.5

Eve has intercepted the ciphertext "UVACLYFZLJBYL". Show how she can use a brute-force attack to break the cipher.

Solution

Eve tries keys from 1 to 7. With a key of 7, the plaintext is "not very secure", which makes sense.

Ciphertext: UVACLYFZLJBYL

K = 1	→	**Plaintext:** tuzbkxeykiaxk
K = 2	→	**Plaintext:** styajwdxjhzwj
K = 3	→	**Plaintext:** rsxzivcwigyvi
K = 4	→	**Plaintext:** qrwyhubvhfxuh
K = 5	→	**Plaintext:** pqvxgtaugewtg
K = 6	→	**Plaintext:** opuwfsztfdvsf
K = 7	→	**Plaintext:** notverysecure

Statistical attack on Additive Cipher

Table 3.1 *Frequency of characters in English*

Letter	*Frequency*	*Letter*	*Frequency*	*Letter*	*Frequency*	*Letter*	*Frequency*
E	12.7	H	6.1	W	2.3	K	0.08
T	9.1	R	6.0	F	2.2	J	0.02
A	8.2	D	4.3	G	2.0	Q	0.01
O	7.5	L	4.0	Y	2.0	X	0.01
I	7.0	C	2.8	P	1.9	Z	0.01
N	6.7	U	2.8	B	1.5		
S	6.3	M	2.4	V	1.0		

Table 3.2 *Frequency of diagrams and trigrams*

Digram	TH, HE, IN, ER, AN, RE, ED, ON, ES, ST, EN, AT, TO, NT, HA, ND, OU, EA, NG, AS, OR, TI, IS, ET, IT, AR, TE, SE, HI, OF
Trigram	THE, ING, AND, HER, ERE, ENT, THA, NTH, WAS, ETH, FOR, DTH

3.2.1 Continued

Example 3.6

Eve has intercepted the following ciphertext. Using a statistical attack, find the plaintext.

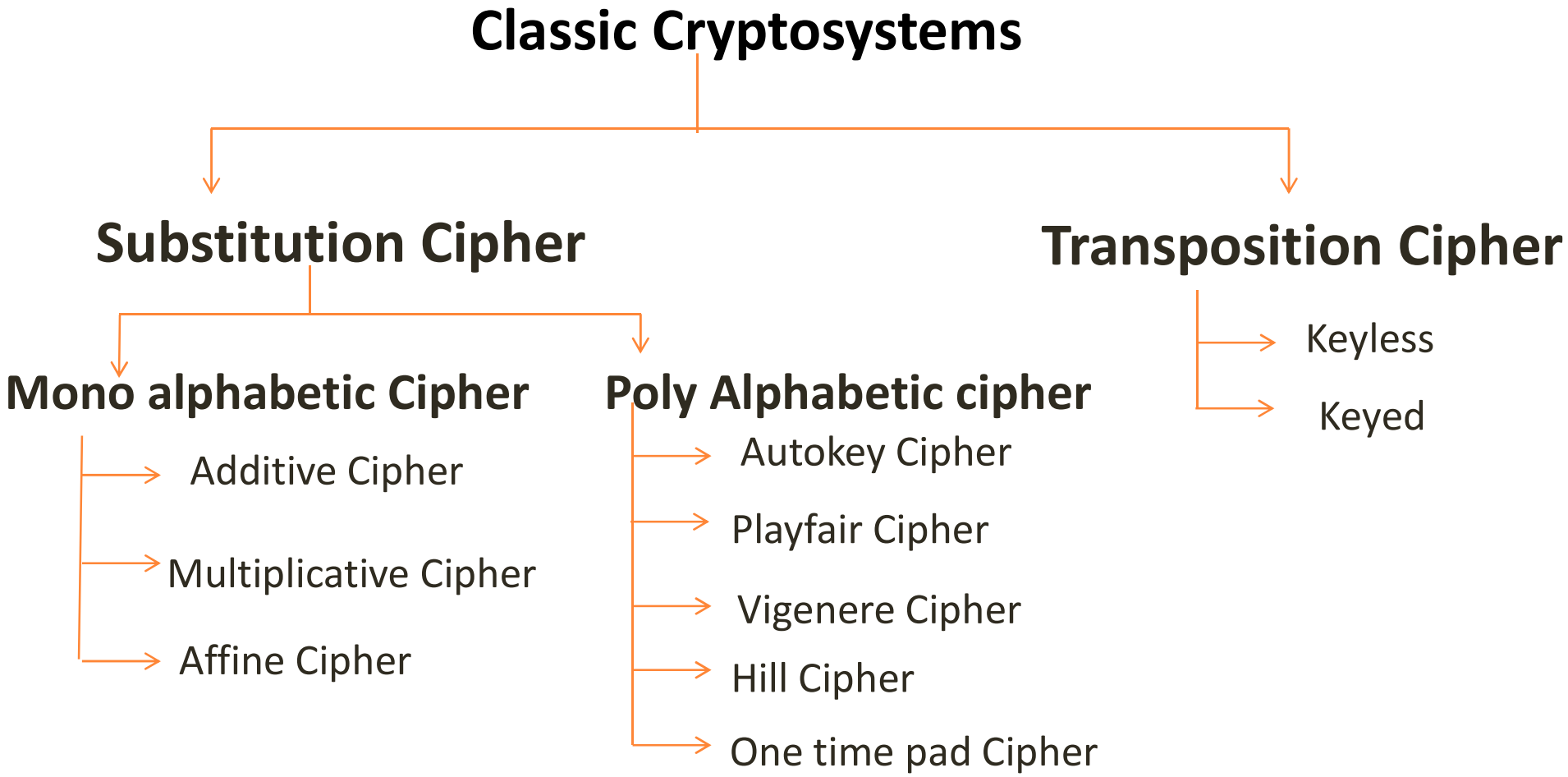
```
XLILSYWIMWRSAJSVWEPIJSVJSYVQMPPMSRHSPPEVWMXMWASVX-LQSVILY-
VVCFIJSVIXLIWIPPIVVIGIMZIWQSVISJJIVW
```

Solution

When Eve tabulates the frequency of letters in this ciphertext, she gets: I =14, V =13, S =12, and so on. The most common character is I with 14 occurrences. This means key = 4.

```
the house is now for sale for four million dollars it is worth more hurry before the seller
receives more offers
```

CATEGORIES OF TRADITIONAL CIPHERS



The following word was encrypted using a Caesar cipher with a shift of 2: ecguct. What word is it?

Who was the first know user of the Caesar Cipher?

MULTIPLICATIVE CIPHER

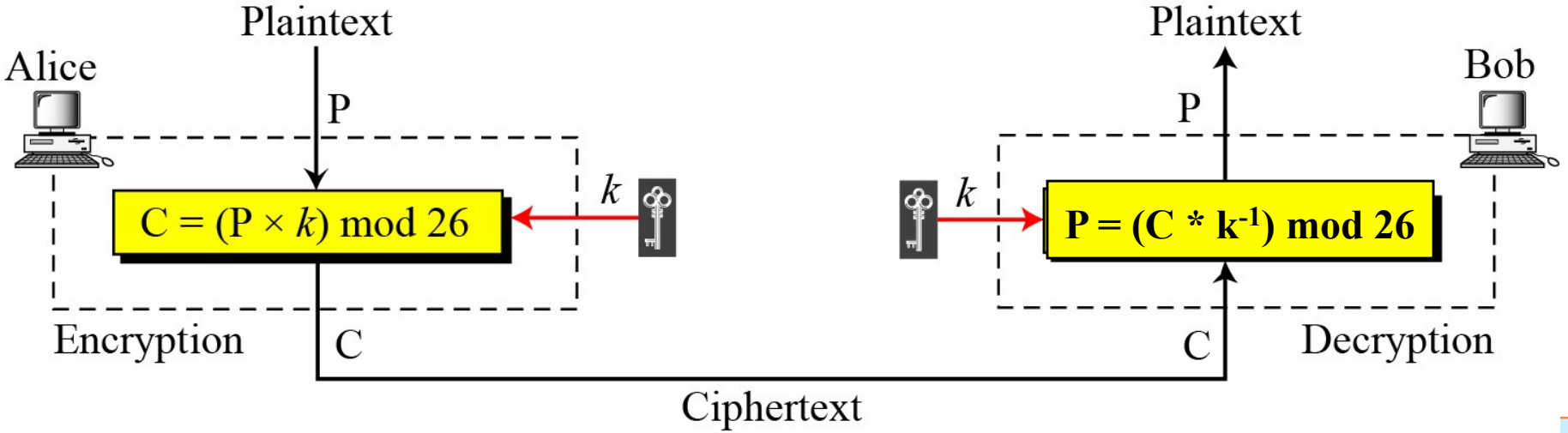
1. Encryption algorithm specifies multiplication of the plaintext by the key
2. Decryption algorithm specifies division of the ciphertext by the key
3. Key belongs to Z^*_{26}

ENCRYPTION

$C = (P * k) \bmod 26$

DECRYPTION

$P = (C * k^{-1}) \bmod 26$



Z^*_{26} include 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25

Use a multiplicative cipher to encrypt the message “ankita” with a key of 4

PLAIN TEXT	ENCRYPTION	CIPHERTEXT
a - 00	(00 * 4) mod 26	00 – A
n – 13	(13 * 4) mod 26	00 – A
k – 10	(10 * 4) mod 26	14 -- O
i – 08	(08 * 4) mod 26	06 -- G
t – 19	(19 * 4) mod 26	24 -- Y
a -- 00	(00 * 4) mod 26	00 -- A

Plaintext →	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
Ciphertext →	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
Value →	00	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

Example

1. What is the key domain for any multiplicative cipher?

2. We use a multiplicative cipher to encrypt the message “hello” with a key of 7

Plaintext: h $\rightarrow$ 07	Encryption: $(07 \times 07) \bmod 26$	ciphertext: 23 $\rightarrow$ X
Plaintext: e $\rightarrow$ 04	Encryption: $(04 \times 07) \bmod 26$	ciphertext: 02 $\rightarrow$ C
Plaintext: l $\rightarrow$ 11	Encryption: $(11 \times 07) \bmod 26$	ciphertext: 25 $\rightarrow$ Z
Plaintext: l $\rightarrow$ 11	Encryption: $(11 \times 07) \bmod 26$	ciphertext: 25 $\rightarrow$ Z
Plaintext: o $\rightarrow$ 14	Encryption: $(14 \times 07) \bmod 26$	ciphertext: 20 $\rightarrow$ U

Multiplicative Inverse

Inverses mod 26												
x	1	3	5	7	9	11	15	17	19	21	23	25
x^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

Multiplicative Inverse

1. Find Multiplicative Inverse of 11 in Z_{26}

r1 = 26
r2 = 11

Terms used:

1. r1 – greatest of 2 nos.
2. r2 - Smallest no.
   (r2, r1)
3. t1 = 0
4. t2 = 1
5. t = t1 – t2 * q

q	r1	r2	r	t1	t2	t
2	26	11	4	0	1	-2
2	11	4	3	1	-2	5
1	4	3	1	-2	5	-7
3	3	1	0	5	-7	26
	1	0		-7	26	

AFFINE CIPHER

1. It is the combination of ADDITIVE and MULTIPLICATIVE cipher.
2. It uses a combination of both ciphers with a pair of keys.
3. First key --- Multiplicative Cipher
4. Second Key --- Additive Cipher

ENCRYPTION

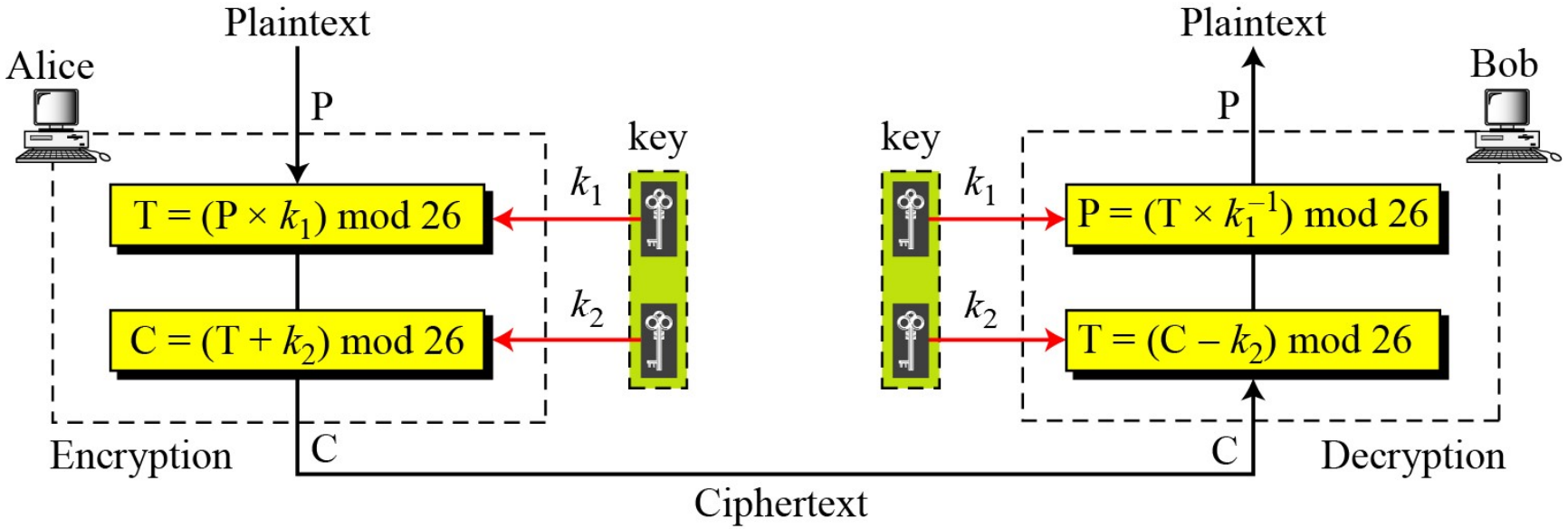
$$C = (P * k1 + k2) \bmod 26$$

DECRYPTION

$$P = ([C - k2] * k^{-1}) \bmod 26$$

AFFINE CIPHER

Affine Ciphers



$$C = (P \times k_1 + k_2) \bmod 26$$

$$P = ((C - k_2) \times k_1^{-1}) \bmod 26$$

where k_1^{-1} is the multiplicative inverse of k_1 and $-k_2$ is the additive inverse of k_2

AFFINE CIPHER

1. The Affine Cipher uses a pair of keys in which;

First key is from Z^*_{26}

Second Key is from Z_{26}

Thus, the size of the key domain is 26 * 12 = 312.

AFFINE CIPHER (ENCRYPTION)

Use an affine cipher to encrypt the message "hello" with the key pair (7, 2).

PLAIN TEXT	ENCRYPTION	CIPHERTEXT
h → 07	(07 * 7 + 2) mod 26	25 → Z
e → 04	(04 * 7 + 2) mod 26	04 → E
l → 11	(11 * 7 + 2) mod 26	01 → B
l → 11	(11 * 7 + 2) mod 26	01 → B
o → 14	(14 * 7 + 2) mod 26	22 → W

AFFINE CIPHER (DECRYPTION)

Use the affine cipher to decrypt the message "ZEBBW" with the key pair (7, 2) in modulus 26.

Solution

C: Z $\rightarrow$ 25	Decryption: $((25 - 2) \times 7^{-1}) \bmod 26$	P:07 $\rightarrow$ h
C: E $\rightarrow$ 04	Decryption: $((04 - 2) \times 7^{-1}) \bmod 26$	P:04 $\rightarrow$ e
C: B $\rightarrow$ 01	Decryption: $((01 - 2) \times 7^{-1}) \bmod 26$	P:11 $\rightarrow$ l
C: B $\rightarrow$ 01	Decryption: $((01 - 2) \times 7^{-1}) \bmod 26$	P:11 $\rightarrow$ l
C: W $\rightarrow$ 22	Decryption: $((22 - 2) \times 7^{-1}) \bmod 26$	P:14 $\rightarrow$ o

Monoalphabetic Substitution Cipher

Because additive, multiplicative, and affine ciphers have small key domains, they are very vulnerable to brute-force attack.

A better solution is to create a mapping between each plaintext character and the corresponding ciphertext character. Alice and Bob can agree on a table showing the mapping for each character.

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

An example key for monoalphabetic substitution cipher

3.2.1 Continued

Example 3.13

We can use the key in Figure 3.12 to encrypt the message

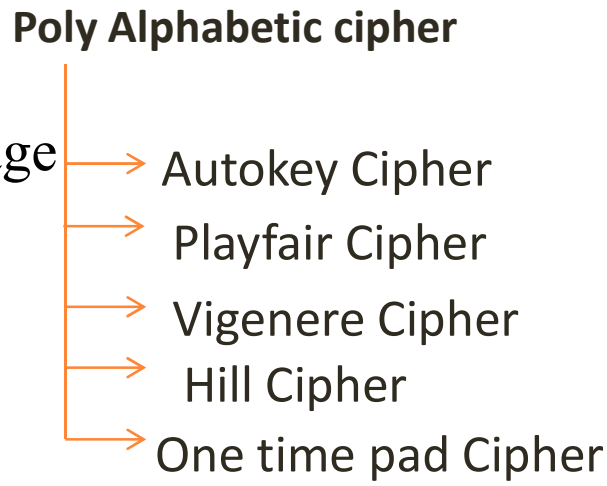
this message is easy to encrypt but hard to find the key

The ciphertext is

ICFVQRVVNEFVRNVSIYRGAHSLIOJICNHTIYBFGTICRXRS

POLYALPHABETIC CIPHER

1. In polyalphabetic substitution, each occurrence of a character may have a different substitute.
2. The relationship between a character in the plaintext to a character in the ciphertext is one-to-many.
3. Hides the letter frequency of the underlying language
4. Each Ciphertext character is dependent on
    - Corresponding Plaintext Character.
    - Position of Plaintext Character.
5. A stream of keys, k = (k_1,k_2,k_3,…..) is used in which k_i is used to encipher i^{th} character in the plaintext to create i^{th} character in Ciphertext



AUTOKEY CIPHER

Plaintext: followwolf
Autokey: P

1. The key is stream of subkeys.

Ciphertext: UTZWZKSKZQ

2. Each subkey is used to encrypt the corresponding character in the plaintext.
3. The 1st subkey is predetermined value secretly agreed upon by the sender and receiver
4. The 2nd subkey is the value of the first plaintext character [0 - 25]
5. The name itself implies that the subkeys are automatically created from the plaintext character during the encryption process.

Plaintext	f	o	l	l	o	w	w	o	l	f
P's value	5	14	11	11	14	22	22	14	11	5
Keys	15	05	14	11	11	14	22	22	14	11
C's Value	20	19	25	22	25	10	18	10	25	16
Ciphertext	U	T	Z	W	Z	K	S	K	Z	Q

AUTOKEY CIPHER

$$K = (k_1, P_1, P_2, \ldots)$$

ENCRYPTION

$$C_i = (P_i + k_i) \bmod 26$$

DECRYPTION

$$P_i = (C_i - k_i) \bmod 26$$

CRYPTANALYSIS

1. Vulnerable to Brute-Force Attack.
2. The first sub-key can be only one of the 25 values .
3. Polyalphabetic ciphers should not only hide the characteristic of the language but should also have large domain.

Example: k1 = 12
Plaintext: “Attack is today”.

3.2.2 Continued

Example 3.14

k1 = 12

Plaintext: “Attack is today”.

Plaintext:	a	t	t	a	c	k	i	s	t	o	d	a	y
P’s Values:	00	19	19	00	02	10	08	18	19	14	03	00	24
Key stream:	*12*	*00*	*19*	*19*	*00*	*02*	*10*	*08*	*18*	*19*	*14*	*03*	*00*
C’s Values:	12	19	12	19	02	12	18	00	11	7	17	03	24
Ciphertext:	**M**	**T**	**M**	**T**	**C**	**M**	**S**	**A**	**L**	**H**	**R**	**D**	**Y**

PLAYFAIR CIPHER

1. Was used by British Army during World War I
2. The secret key in this cipher is made of 25 alphabet letters arranged in 5*5 matrix
3. Different arrangements of the letters in the matrix can create may different secret keys.

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

If the letters in a paur are same then a bogus letter is inserted to separate them.

If odd characters in plaintext, then add extra character at the end to make no. of characters EVEN.

PLAYFAIR CIPHER

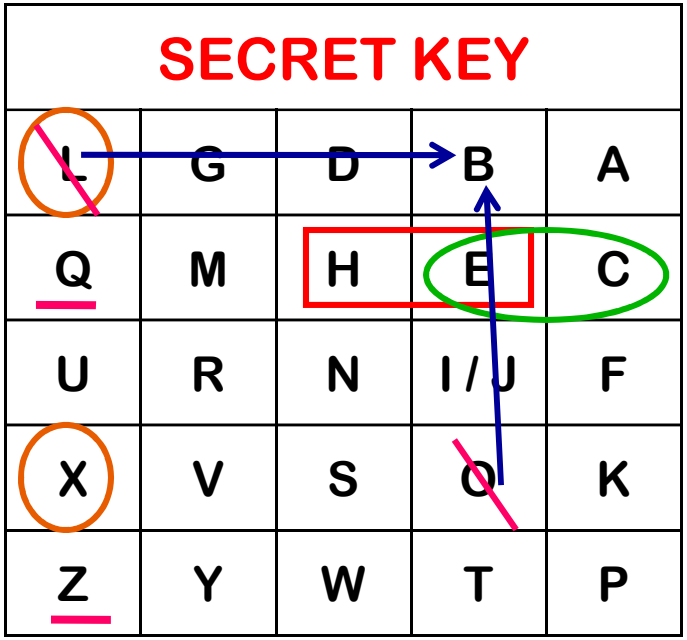
RULES FOR ENCRYPTION

Plain Text: hello Cipher Text: **ECQZBX**

Inserting Bogus Character: helxlo

PAIRING CHARCATERS:

he	lx	lo
EC	**QZ**	**BX**



- If two letters in a pair are located in the same row of the secret key, then the corresponding encrypted character for each letter is the next letter to one right in the same row.
- If two letters in a pair are located in the same column of the secret key, then the corresponding encrypted character for each letter is the letter beneath it.

Not in same row or column, the corresponding encrypted character for each letter is a letter that is in its own row but in the same column as the other letter

PLAYFAIR CIPHER

$$K = [(k_1, k_2), (k_3, k_4), \ldots..)$$

ENCRYPTION

$$C_i = k_i$$

DECRYPTION

$$P_i = k_i$$

CRYPTANALYSIS

1. The size of the key domain is 25!.
2. Brute – Force attack is very difficult
3. Frequency of diagrams are preserved, so a cryptanalyst can use a ciphertext only attack based on the diagram frequency test to find a key.

Example: Plaintext: instruments

Key: monarchy

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

Plain text: instruments

CIPHER TEXT: GATLMZCLRQTX

PLAYFAIR CIPHER (DECRYPTION)

Cipher text: CTQVSIRF

Cipher text: CT QV SI RF

Secret Key: INFORMATION

Plain text: ba lx lo on

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

VIGENERE CIPHER

1. Was designed by Blaise de Vigenere
2. The key stream is a repetition of an initial secret key stream of length m., where $1 \leq m \leq 26$.
3. **$(k_1, k_2, k_3, \ldots\ldots, k_m)$** is the initial secret key agreed upon by sender and receiver.
4. Vigenere key stream does not depend on the plaintext characters, but only on the position of the character in the plaintext.
5. Thus, key stream can be created without knowing the plaintext.

$P = P_1P_2P_3 \ldots$ $C = C_1C_2C_3 \ldots$ $K = [(k_1, k_2, \ldots, k_m), (k_1, k_2, \ldots, k_m), \ldots]$

Encryption: $C_i = P_i + k_i$ Decryption: $P_i = C_i - k_i$

VIGENERE CIPHER (ENCRYPTION

Plain text: attackatos

Keyword: Pascal

The initial key stream is = (15, 0, 18, 2, 0, 11).

Plaintext	a	t	t	a	c	k	a	t	o	s
P's value	00	19	19	00	02	10	00	19	14	18
Keys	15	00	18	02	00	11	15	00	18	02
C's Value	15	19	11	02	02	21	15	19	06	20
Ciphertext	P	T	L	C	C	V	P	T	G	U

Encrypt the message "She is listening" using the 6-character keyword "PASCAL"

SOLUTION

Plaintext:	s	h	e	i	s	l	i	s	t	e	n	i	n	g
P's values:	18	07	04	08	18	11	08	18	19	04	13	08	13	06
Key stream:	***15***	***00***	***18***	***02***	***00***	***11***	***15***	***00***	***18***	***02***	***00***	***11***	***15***	***00***
C's values:	**07**	**07**	**22**	**10**	**18**	**22**	**23**	**18**	**11**	**6**	**13**	**19**	**02**	**06**
Ciphertext:	**H**	**H**	**W**	**K**	**S**	**W**	**X**	**S**	**L**	**G**	**N**	**T**	**C**	**G**

Given plain text is : H E L L O
Intial Key : N

7 04 11 11 14
13 7 4 11 11

20 11 15 22 25
U L P W Z

20 11 15 22 25
13 7 4 11 11

7

HILL CIPHER

Note

The key matrix in the Hill cipher needs to have a multiplicative inverse.

1. Was invented by Lester S. Hill
2. In this, the plain text is divided into equal size blocks
3. The block are encrypted one at a time in such a way that each character in the block contributed to the encryption of other characters in the block.
4. Due to above property, Hill cipher belongs to the category of **BLOCK CIPHERS**
5. The key is a square matrix of size m*m, in which m is the size of the block.

$$K = \begin{bmatrix} k_{11} & k_{12} & \dots & k_{1m} \\ k_{21} & k_{22} & \dots & k_{2m} \\ \vdots & \vdots & & \vdots \\ k_{m1} & k_{m2} & \dots & k_{mm} \end{bmatrix}$$

$$C_1 = P_1 k_{11} + P_2 k_{21} + \cdots + P_m k_{m1}$$
$$C_2 = P_1 k_{12} + P_2 k_{22} + \cdots + P_m k_{m2}$$
$$\dots$$
$$C_m = P_1 k_{1m} + P_2 k_{2m} + \cdots + P_m k_{mm}$$

HILL CIPHER (ENCRYPTION EXAMPLE

Plain text: safemessages

Keyword: ciphering

KEY IS A BLOCK OF 3*3 matrix

Thus, k =

C	I	P
H	E	R
I	N	G

Integer

Equivalent

2	8	15
7	4	17
8	13	6

No. of columns in plaintext matrix should be equal to no of rows in key matrix

Arrange the plaintext in 4*3 matrix

s	**a**	**f**
e	**m**	**e**
s	**s**	**a**
g	**e**	**s**

Integer

Equivalent

18	**00**	**05**
04	**12**	**04**
18	**18**	**00**
06	**04**	**18**

HILL CIPHER (ENCRYPTION EXAMPLE

ENCRYPTION : C = P * k

18	00	05
04	12	04
18	18	00
06	04	18

*

2	8	15
7	4	17
8	13	6

C

24	01	14
20	02	02
06	08	04
02	12	06

=

Y	B	O
U	C	C
G	I	E
C	M	G

HILL CIPHER (DECRYPTION EXAMPLE

DECRYPTION : $P = C * k^{-1}$

24	**01**	**14**
20	**02**	**02**
06	**08**	**04**
02	**12**	**06**

*****

2	8	15
7	4	17
8	13	6

-1

$$A^{-1} = \frac{1}{|A|} Adj(A)$$

HILL CIPHER (DECRYPTION EXAMPLE

To find k^{-1}

$$A^{-1} = \frac{1}{|A|} Adj(A)$$

-1

2	8	15
7	4	17
8	13	6

Now, $\frac{1}{|k|} = |k|^{-1}$

k^{-1} = 1243 * 5 mod 26 = 1

To find | k |

| k | = 2 (24 – 221) – 8 (42 – 136) + 15 (91 – 32)

| k | = 2 (-197) – 8 (-94) + 15 (59)

| k | = - 394 + 752 + 885
= 1243

HILL CIPHER (DECRYPTION EXAMPLE

To find k^{-1}

$$A^{-1} = \frac{1}{|A|} Adj(A)$$

To find Adj (A) :

-1

2	8	15
7	4	17
8	13	6

2	8	15	2	8
7	4	17	7	4
8	13	6	8	13
2	8	15	2	8
7	4	17	7	4

-197	**147**	**76**
94	**-108**	**71**
59	**38**	**-48**

55	735	380
470	110	355
295	190	20

11	147	76
94	22	71
59	38	4

-197 + 26 (**8**) = **11**
-108 + 26 (5) = 22
-48 + 26 (2) = 4

HILL CIPHER (DECRYPTION EXAMPLE

To find k^{-1}

$$\begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix}^{-1}$$

$$\begin{bmatrix} 55 & 735 & 380 \\ 470 & 110 & 355 \\ 295 & 190 & 20 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 3 & 7 & 16 \\ 2 & 6 & 17 \\ 9 & 8 & 20 \end{bmatrix}$$

HILL CIPHER (DECRYPTION EXAMPLE

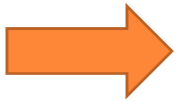
DECRYPTION : $P = C * k^{-1}$

24	01	14
20	02	02
06	08	04
02	12	06

*

3	7	16
2	6	17
9	8	20

18	00	05
04	12	04
18	18	00
06	04	18



s	a	f
e	m	e
s	s	a
g	e	s

Plain text: safemessages

Example:

- Plaintext: “We live in an insecure world”
- Key: $\begin{bmatrix} 03 & 02 \\ 05 & 07 \end{bmatrix}$

ONE TIME PAD CIPHER

1. Also known as Vernam Cipher (invented by Vernam) or Perfect Cipher.
2. Plaintext is combined with a random key
3. It is the only existing mathematically unbreakable encryption
4. A study by Shannon has shown that perfect secrecy can be achieved if each plaintext symbol is encrypted with a key randomly chosen from a key domain.
5. To encrypt each character a key is randomly chosen from the key domain (00, 01, 02, ……, 25)
6. The key has the same length as the plaintext and is chosen completely random
7. Even if it is a perfect cipher, it is almost impossible to implement commercially.

ONE TIME PAD CIPHER (ENCRYPTION)

```
      H       E       L       L       O
    7 (H)   4 (E)  11 (L)  11 (L)  14 (O)
+  23 (X)  12 (M)   2 (C)  10 (K)  11 (L)  key
=  30      16      13      21      25       message + key
=   4 (E)  16 (Q)  13 (N)  21 (V)  25 (Z)  message + key (mod 26)
       E       Q       N       V       Z   → ciphertext
```

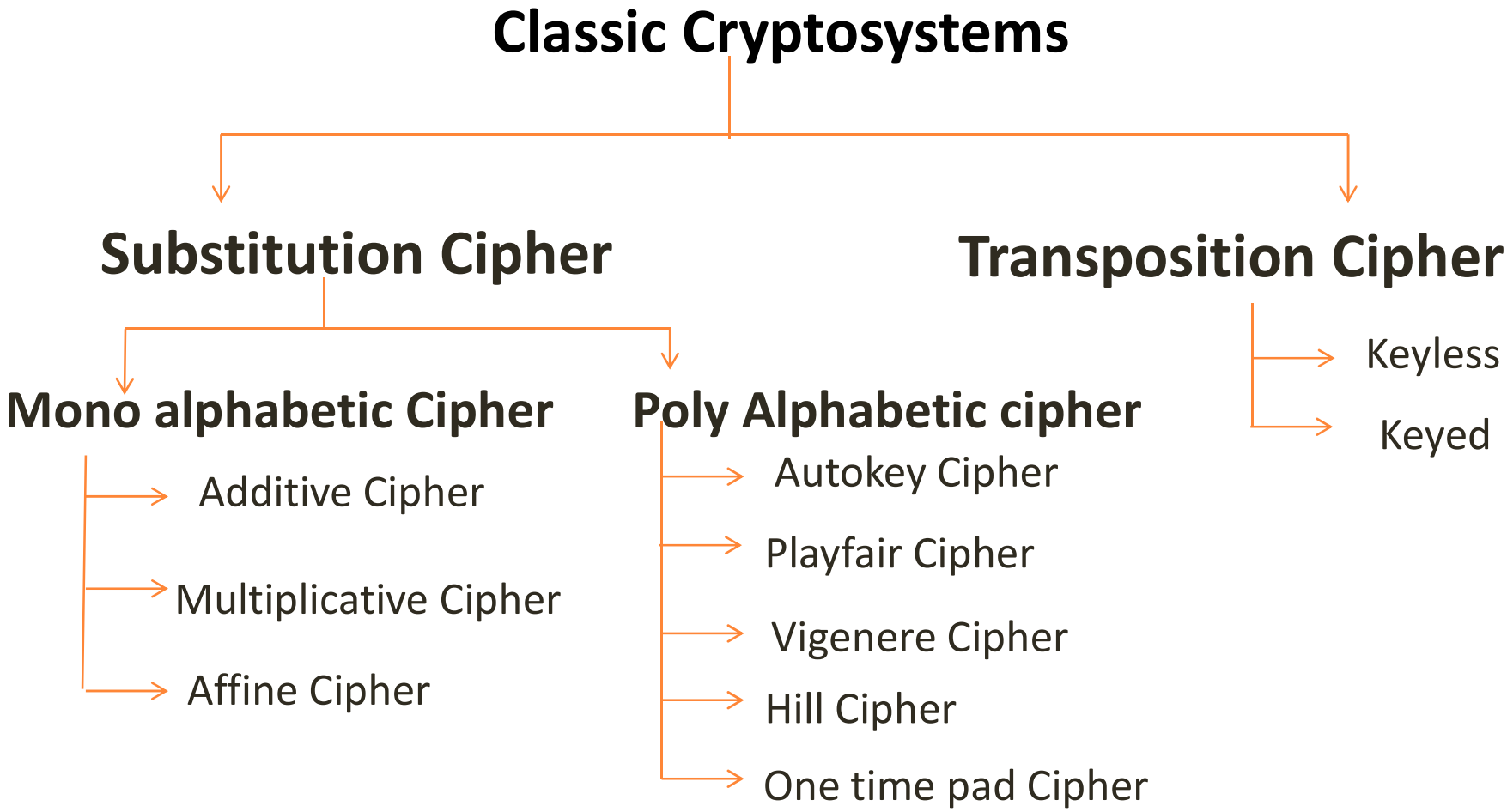
hello → ENCRYPTED → **EQNVZ**

ONE TIME PAD CIPHER (DECRYPTION)

```
      E       Q       N       V       Z  ciphertext
    4 (E)  16 (Q)  13 (N)  21 (V)  25 (Z) ciphertext
-  23 (X)  12 (M)   2 (C)  10 (K)  11 (L) key
= -19       4      11      11      14     ciphertext - key
=   7 (H)   4 (E)  11 (L)  11 (L)  14 (O) ciphertext - key (mod 26)
      H       E       L       L       O  → message
```

EQNVZ → **DECRYPTED** → **hello**

CATEGORIES OF TRADITIONAL CIPHERS



TRANSPOSITION CIPHER

1. A transposition cipher does not substitute one symbol for another, instead it changes the location of the symbols.
2. A symbol in the 1st position of the plaintext may apper in the 10th position of the ciphertext
3. It transposes the symbols

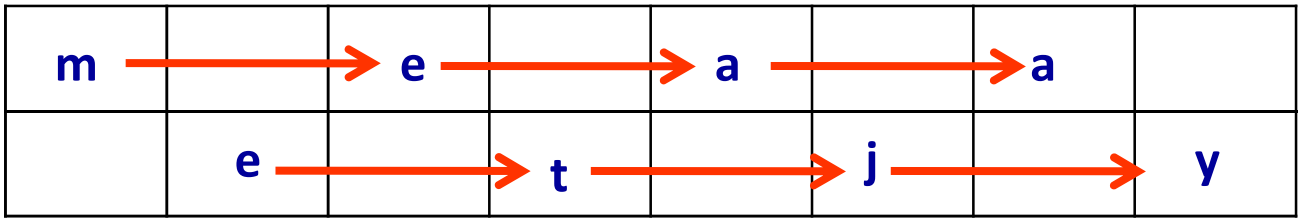
Note

A transposition cipher reorders symbols.

KEYLESS TRANSPOSITION CIPHER

1. Simple transposition ciphers, which were used in the past, are keyless.
2. There are 2 methods for permutation of characters

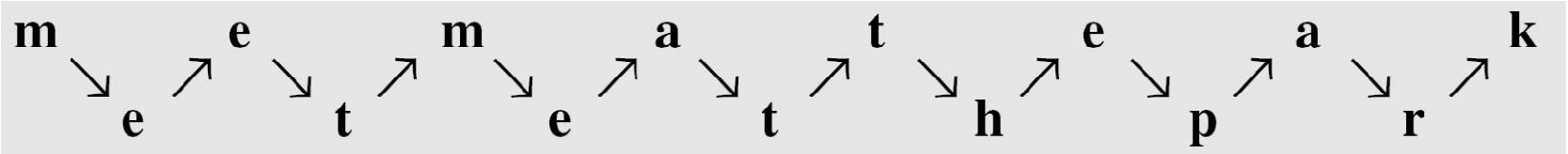
Text is written into a table column by column and then transmitted row by row



Plaintext: meet ajay **Ciphertext: m e a a e t j y**

Rail fence cipher:

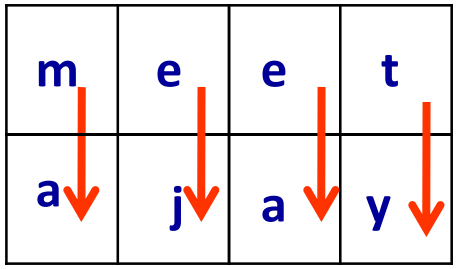
Plaintext: “Meet me at the park”



Ciphertext: “MEMATEAKETETHPR”.

KEYLESS TRANSPOSITION CIPHER

1. Simple transposition ciphers, which were used in the past, are keyless.
2. There are 2 methods for permutation of characters



Text is written into a table row by row and then transmitted column by column

Plaintext: meet ajay **Ciphertext: m a e j e a t y**

Alice and Bob can agree on the number of columns and use the second method. Alice writes the same plaintext, row by row, in a table of four columns.

m	e	e	t
m	e	a	t
t	h	e	p
a	r	k	

She then creates the ciphertext "MMTAEEHREAEKTTP".

KEYED TRANSPOSITION CIPHER

1. Divide the plaintext into groups of predetermined size, called blocks
2. A key is used t permute the character in each block separately

Plaintext: enemy attacks tonight

Sender and receiver has agreed to divide the text into group of 5 characters

Plaintext: enemy attac kston ightz

ENCRYPTION ↓

3	1	4	5	2
1	2	3	4	5

↑ **DECRYPTION**

The key used for encryption and decryption is a permutation key

Ciphertext: E E M Y N TAACT TKONS HITZG

COMBINING TWO APPROACHES

1. To achieve better scrambling
2. Encryption or Decryption is done in 3 steps

1.Text is written row by row
2. Use key for reordering
3. Read column by column

Plaintext: enemy attacks tonight

e	n	e	m	y
a	t	t	a	c
k	s	t	o	n
i	g	h	t	z

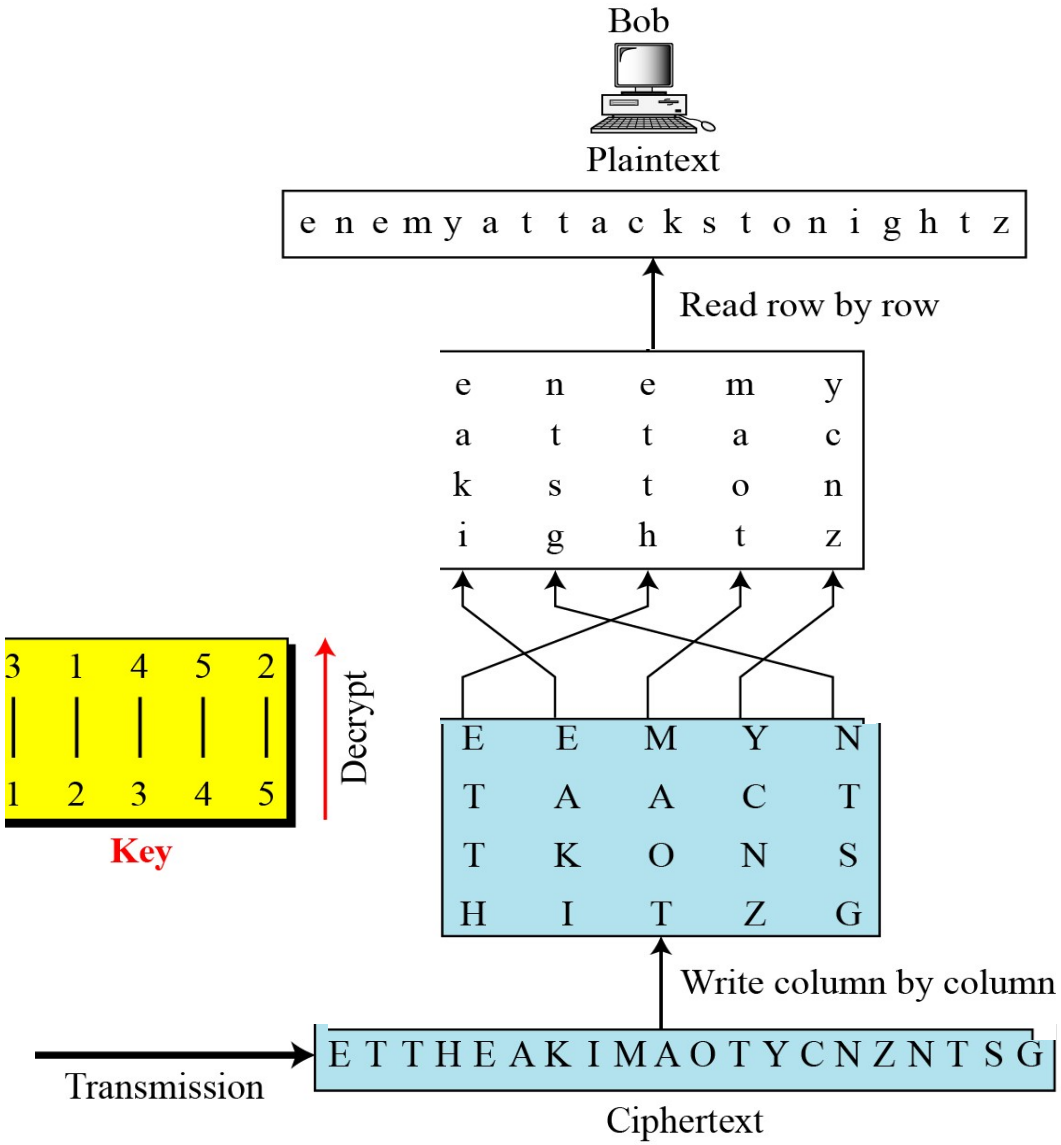
ENCRYPTION

3	1	4	5	2
1	2	3	4	5

E	E	M	Y	N
t	a	a	c	t
t	k	o	n	s
h	i	t	z	g

Read by column

Ciphertext: etth eaki maot ycnz ntsg


Bob
Plaintext
e n e m y a t t a c k s t o n i g h t z
Read row by row
e n e m y
a t t a c
k s t o n
i g h t z
3 1 4 5 2
1 2 3 4 5
Key
Decrypt
E E M Y N
T A A C T
T K O N S
H I T Z G
Write column by column
E T T H E A K I M A O T Y C N Z N T S G
Transmission
Ciphertext

CRYPTANALYSIS OF TRANSPOSITION CIPHER

1. These are vulnerable to several kinds of Cipher-text only attack

   A. Statistical Attack

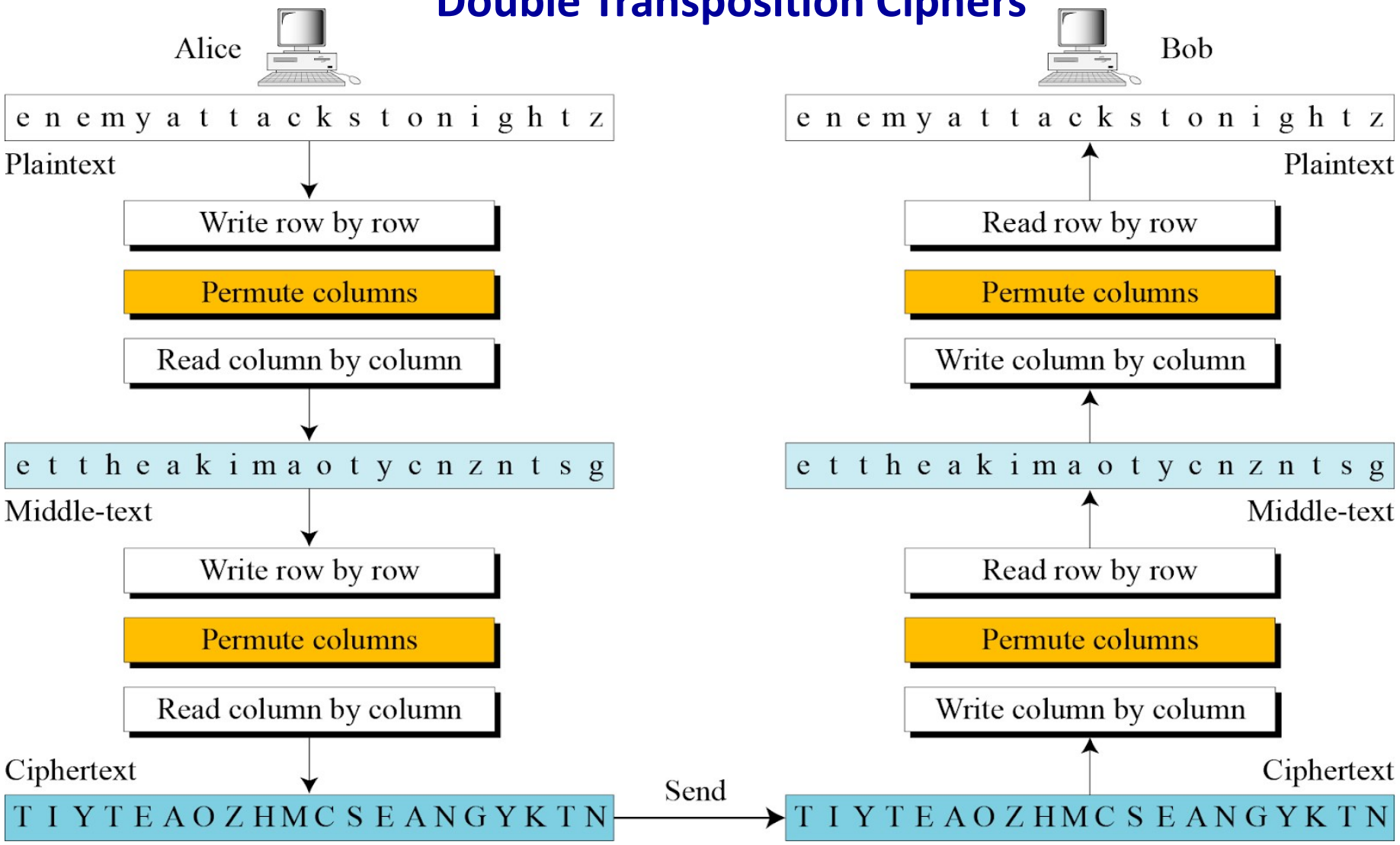
      The frequency of the letters is not changed. Thus, single-letter frequency analysis is the 1st attack

   B. Brute Force Attack

      • Attacker can use all possible keys to decrypt the message. Since the no. of keys is huge (1! + 2! + 3! + ... + L!)
      • A better approach is to guess the number of columns

   C. Pattern Attack

Double Transposition Ciphers



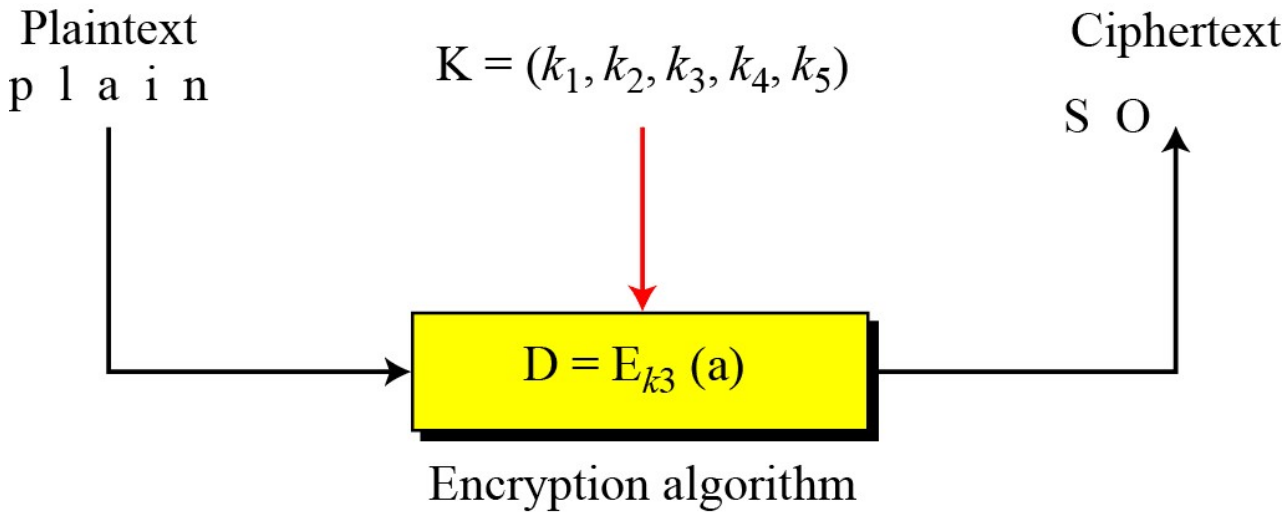
STREAM CIPHER

1. Encryption and decryption are done typically on one symbol at a time.

   Call the plaintext stream P, the ciphertext stream C, and the key stream K.

$$P = P_1P_2P_3, \ldots \qquad C = C_1C_2C_3, \ldots \qquad K = (k_1, k_2, k_3, \ldots)$$

$$C_1 = E_{k1}(P_1) \qquad C_2 = E_{k2}(P_2) \qquad C_3 = E_{k3}(P_3) \ldots$$

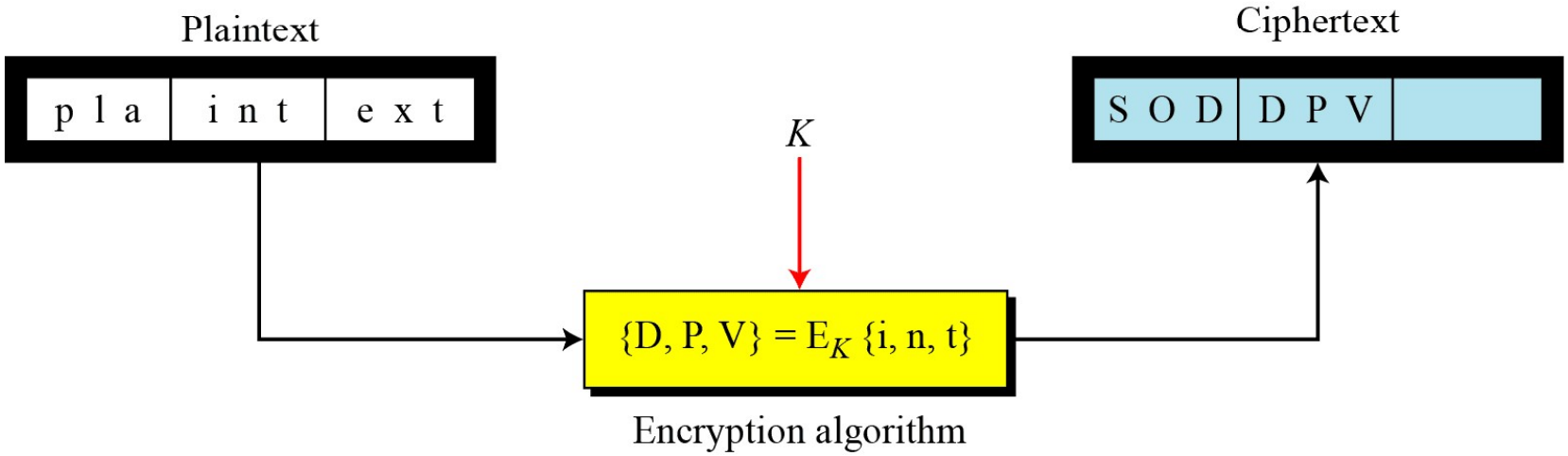


STREAM CIPHER

1. Additive ciphers can be categorized as stream ciphers in which the key stream is the repeated value of the key.
2. The monoalphabetic substitution ciphers discussed in this chapter are also stream ciphers.
3. Vigenere ciphers are also stream ciphers according to the definition.
4. a stream cipher is a monoalphabetic cipher if the value of k_i does not depend on the position of the plaintext character in the plaintext stream; otherwise, the cipher is polyalphabetic.

BLOCK CIPHER

In a block cipher, a group of plaintext symbols of size m ($m > 1$) are encrypted together creating a group of ciphertext of the same size. A single key is used to encrypt the whole block even if the key is made of multiple values. Figure 3.27 shows the concept of a block cipher.



BLOCK CIPHER

1. Playfair ciphers are block ciphers.
2. Hill ciphers are block ciphers.
3. From the definition of the block cipher, it is clear that every block cipher is a polyalphabetic cipher because each character in a ciphertext block depends on all characters in the plaintext block.

We add the bogus character, "z" to the end of the plaintext to make the number of characters multiple of 2. The plaintext matrix, the key matrix, and ciphertext matrix are shown below:

$$\underset{\mathbf{C}}{\begin{bmatrix} 8 & 20 \\ 21 & 0 \\ 5 & 18 \\ 11 & 3 \\ 13 & 13 \\ 11 & 3 \\ 22 & 12 \\ 2 & 14 \\ 19 & 10 \\ 6 & 12 \\ 2 & 7 \\ 4 & 25 \end{bmatrix}} = \underset{\mathbf{P}}{\begin{bmatrix} 22 & 4 \\ 11 & 8 \\ 21 & 4 \\ 8 & 13 \\ 0 & 13 \\ 8 & 13 \\ 18 & 4 \\ 2 & 20 \\ 17 & 4 \\ 22 & 14 \\ 17 & 11 \\ 3 & 25 \end{bmatrix}} \times \underset{\mathbf{K}}{\begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix}}$$

The ciphertext is then "IUVAFSLDNNLDWMCOTKGMCHEZ", in which the last character is a bogus character.

TEKOOHRACIRMNREATANFTETYTGHH", encrypted with a key of 4,

T						E				E
	-				-					
		-		-						
			-							

Modular Arithmetic and Number Theory

Euler's Phi-Function $\varphi(n)$

1. Is sometimes called as Euler's totient function.
2. It plays a very important role in cryptography
3. The function finds the number of integers that are both smaller than n and relatively prime to n
4. The function φ (n) calculates the number of elements in this set

Use the following to find the value of φ (n)

1. $\phi(1) = 0$.
2. $\phi(p) = p - 1$ if p is a prime.
3. $\phi(m \times n) = \phi(m) \times \phi(n)$ if m and n are relatively prime. **m ≠ n**
4. $\phi(p^e) = p^e - p^{e-1}$ if p is a prime.

Note

The difficulty of finding φ(n) depends on the difficulty of finding the factorization of *n*.

Euler's Phi-Function $\varphi(n)$ *- Examples*

Note

Interesting point: If $n > 2$, the value of $\varphi(n)$ is even.

1. What is the value of $\varphi(13)$?

Solution: Because 13 is a prime, $\varphi(13) = (13 - 1) = 12$.

2. What is the value of $\varphi(10)$?

Solution: $\phi(10) = \phi(2) \times \phi(5)$
$= 1 * 4$
$= 4$

What is the number of elements in Z_{14}^*?
Solution: 6

3. What is the value of $\varphi(240)$?

Solution: $240 = 2^4 \times 3^1 \times 5^1$

$\phi(240) = (2^4 - 2^3) \times (3^1 - 3^0) \times (5^1 - 5^0)$
$= 64$

4. Can we say that $\phi(49) = \phi(7) \times \phi(7) = 6 \times 6 = 36$?

Solution: No. The third rule applies when *m* and *n* are relatively prime. Here $49 = 7^2$.
We need to use the fourth rule: $\phi(49) = 7^2 - 7^1 = 42$.

n	$\varphi(n)$	numbers coprime to n
1	1	1
2	1	1
3	2	1, 2
4	2	1,3
5	4	1,2,3,4
6	2	1,5
7	6	1,2,3,4,5,6
8	4	1,3,5,7
9	6	1,2,4,5,7,8
10	4	1,3,7,9
11	10	1,2,3,4,5,6,7,8,9,10
12	4	1,5,7,11
13	12	1,2,3,4,5,6,7,8,9,10,11,12
14	6	1,3,5,9,11,13
15	8	1,2,4,7,8,11,13,14

Euler's Phi-Function $\varphi(n)$ – *Examples for practice*

Calculate

a) $\Phi(29)$
b) $\Phi(32)$
c) $\Phi(80)$
d) $\Phi(100)$
e) $\Phi(101)$

ANSWERS

a) 28
b) 16
c) 32
d) 40
e) 100

$$\Phi(80) = 2 * 2 * 2 * 2 * 5$$
$$= 2^4 * 5$$
$$= (2^4 - 2^3) * 4$$
$$= (16 - 8) * 4$$
$$= 8 * 4$$
$$= 32$$

Note

Interesting point: If $n > 2$, the value of $\varphi(n)$ is even.

Fermat's Little Theorem

First Version

If p is prime number

a is positive integer not divisible by p

a, p are co-prime

$$a^{p-1} \equiv 1 \bmod p$$

Find the result of 6^{10} mod 11.

Solution: p = 11, a = 6

$$6^{11-1} \equiv 1 \bmod 11$$

$$6^{10} \equiv 1 \bmod 11$$

$$6^{10} \bmod 11 \equiv 1$$

Fermat's Little Theorem

Second Version

If p is prime number

a is positive integer ~~not divisible by p~~

a, p are co-prime

$$a^p \equiv a \bmod p$$

Find the result of 3^{12} mod 11.

Solution: p = 11, a = 3

Now, 3^{12} mod 11 = (3^{11} * 3^1) mod 11

= **(3^{11} mod 11) * (3^1 mod 11)**

= 3* 3

= 9

Multiplicative Inverse

A very interesting application of Fermat's theorem is in finding some multiplicative inverses quickly if the modulus is prime

If *p is prime* and *a is an integer* such that ***p*** does not divide ***a*** then,

$$a^{-1} \bmod p = a^{p-2} \bmod p$$

a. $8^{-1} \bmod 17 = 8^{17-2} \bmod 17 = 8^{15} \bmod 17 = 15 \bmod 17$

b. $5^{-1} \bmod 23 = 5^{23-2} \bmod 23 = 5^{21} \bmod 23 = 14 \bmod 23$

c. $60^{-1} \bmod 101 = 60^{101-2} \bmod 101 = 60^{99} \bmod 101 = 32 \bmod 101$

d. $22^{-1} \bmod 211 = 22^{211-2} \bmod 211 = 22^{209} \bmod 211 = 48 \bmod 211$

Euler's Theorem

1. Generalization of Fermat's Theorem
2. The modulus in the Fermat's theorem is prime, whereas the modulus in Euler's theorem is an integer.

$$a^{p-1} \equiv 1 \bmod p$$

First Version

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Second Version

$$a^{k \times \varphi(n) + 1} \equiv a \pmod{n}$$

Note

The second version of Euler's theorem is used in the RSA cryptosystem in Chapter 4.

Chinese Remainder theorem

1. Is used to solve a set of congruent equations with one variable but different moduli, which are relatively prime

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\dots$$
$$x \equiv a_k \pmod{m_k}$$

It states that the above equations have a unique solution if the moduli are relatively prime.

Chinese Remainder theorem

Solution To Chinese Remainder Theorem

1. Find $M = m_1 \times m_2 \times \ldots \times m_k$. This is the common modulus.
2. Find $M_1 = M/m_1$, $M_2 = M/m_2$, …, $M_k = M/m_k$.
3. Find the multiplicative inverse of M_1, M_2, …, M_k using the corresponding moduli $(m_1, m_2, \ldots, m_k)$. Call the inverses M_1^{-1}, M_2^{-1}, …, M_k^{-1}.
4. The solution to the simultaneous equations is

$$x = (a_1 \times M_1 \times M_1^{-1} + a_2 \times M_2 \times M_2^{-1} + \cdots + a_k \times M_k \times M_k^{-1}) \bmod M$$

Chinese Remainder theorem (Example)

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 2 \pmod 7$$

a1 =2, a2=3, a3=2

m1 =3, m2=5, m3=7

1. Find M = m1 * m2 * m3

   M = 3 * 5 * 7 = 105

2. Find M_1 = M/ m1

$$M_1 = \frac{m1 * m2 * m3}{m1}$$

$$M_1 = m2 * m3$$

= 35

M_2 = 21

M_3 = 15

Chinese Remainder theorem (Example)

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 2 \pmod 7$$

$M = 3 * 5 * 7 = 105$

$M_1 = 35$, $M_2 = 21$, $M_3 = 15$

3. Find the multiplicative inverse of $M_1, M_2, \ldots, M_k$ using the corresponding moduli $(m_1, m_2, \ldots, m_k)$. Call the inverses $M_1^{-1}, M_2^{-1}, \ldots, M_k^{-1}$.

$M_1^{-1} \mod 3$

$= 35^{-1} \mod 3$

$= 35^{3-2} \mod 3$

$= 35^{1} \mod 3$

$= 2$

$M_2^{-1} \mod 5$

$= 21^{-1} \mod 5$

$= 21^{5-2} \mod 5$

$= 21^{3} \mod 5$

$= 1$

Similarly $M_3^{-1} = 1$

Chinese Remainder theorem

Solution To Chinese Remainder Theorem

1. Find $M = m_1 \times m_2 \times \ldots \times m_k$. This is the common modulus.
2. Find $M_1 = M/m_1$, $M_2 = M/m_2$, …, $M_k = M/m_k$.
3. Find the multiplicative inverse of M_1, M_2, …, M_k using the corresponding moduli $(m_1, m_2, \ldots, m_k)$. Call the inverses M_1^{-1}, M_2^{-1}, …, M_k^{-1}.
4. The solution to the simultaneous equations is

$$x = (a_1 \times M_1 \times M_1^{-1} + a_2 \times M_2 \times M_2^{-1} + \cdots + a_k \times M_k \times M_k^{-1}) \bmod M$$

a1=2, a2=3, a3=2

$M_1 = 35$, $M_2 = 21$, $M_3 = 15$

$M_1^{-1} = 2$, $M_2^{-1} = 1$, $M_3^{-1} = 1$

x = 233 mod 105
= 23

Chinese Remainder theorem (example to practise)

$X \equiv 1 \bmod 5$

$X \equiv 1 \bmod 7$

$X \equiv 3 \bmod 11$

Find an integer that has remainder 3 when divided by 7 and 13 , but is divisible by 12.

$X \equiv 3 \bmod 7$

$X \equiv 3 \bmod 13$

$X \equiv 0 \bmod 12$