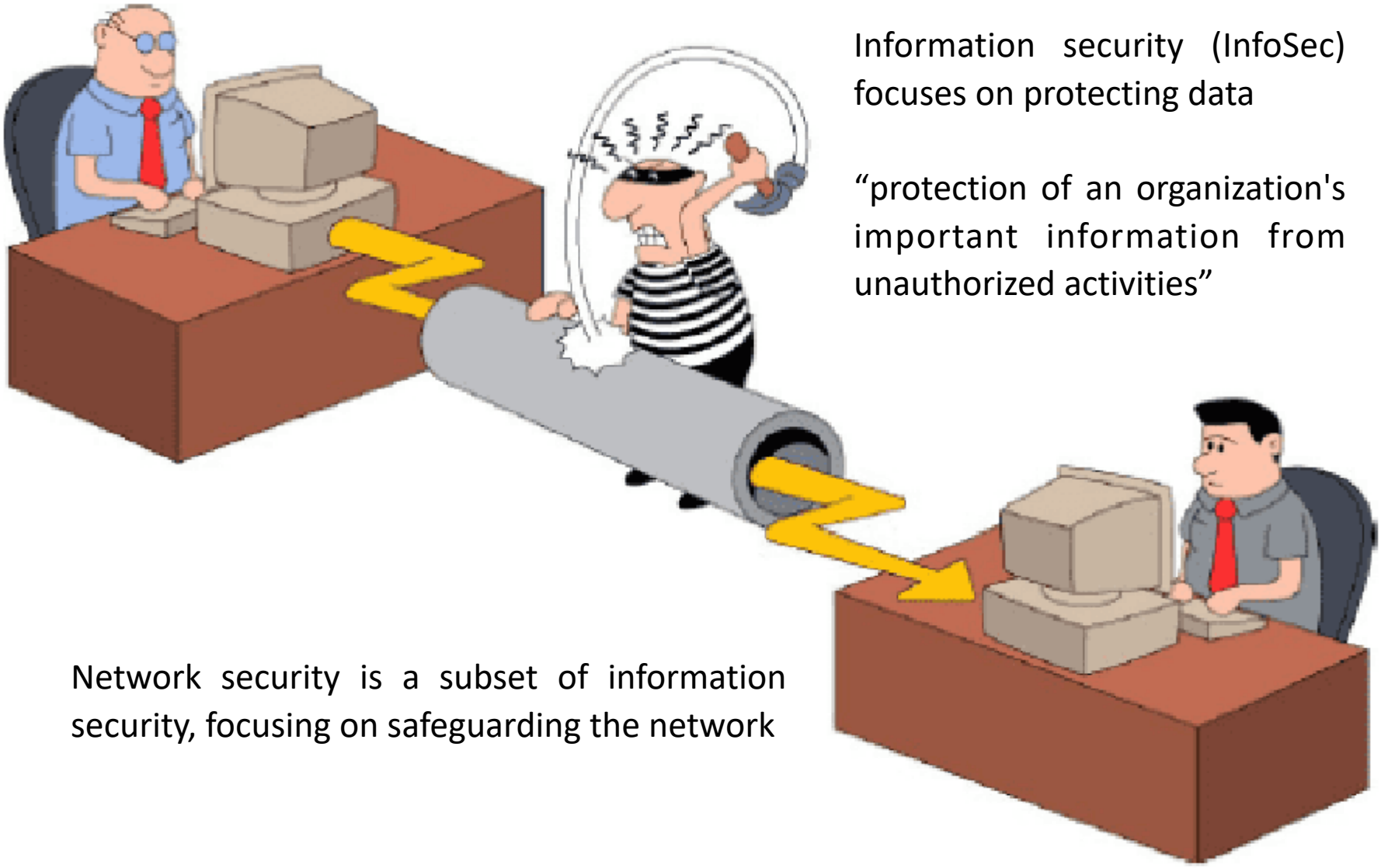
UNIT-1
Introduction

Outline

- OSI Security Architecture
- Security Attacks
- Security Services
- Security Mechanism
- Symmetric Cipher Model
- Cryptography
- Cryptanalysis and Attacks
- Substitution and Transposition Techniques

Introduction to Information & N/W Security



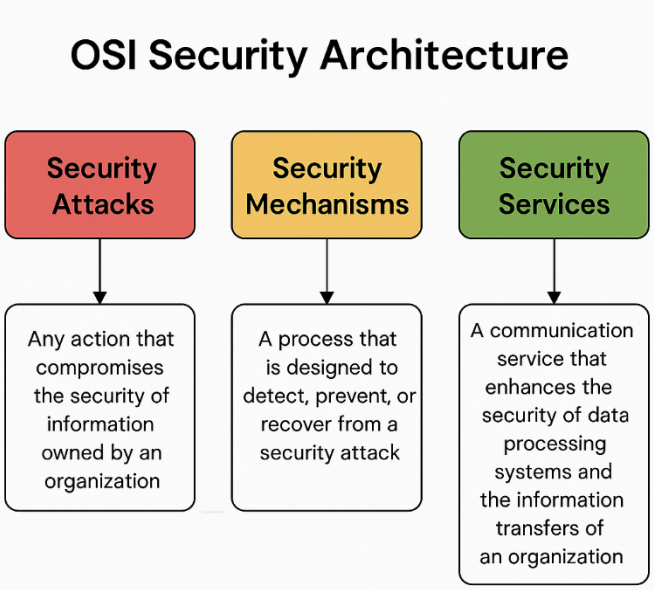
Information security (InfoSec) focuses on protecting data

“protection of an organization's important information from unauthorized activities”

Network security is a subset of information security, focusing on safeguarding the network

OSI Security Architecture

- The OSI (Open Systems Interconnection) security architecture focuses on Security Attacks, Mechanisms, and Services.
- **Security Attack:** Any action that compromises the security of information owned by an organization.
- **Security Mechanism:** A process that is designed to detect, prevent, or recover from a security attack.
- **Security Service:** A communication service that enhances the security of the data processing systems and the information transfers of an organization.



Security Mechanism Vs Security Service

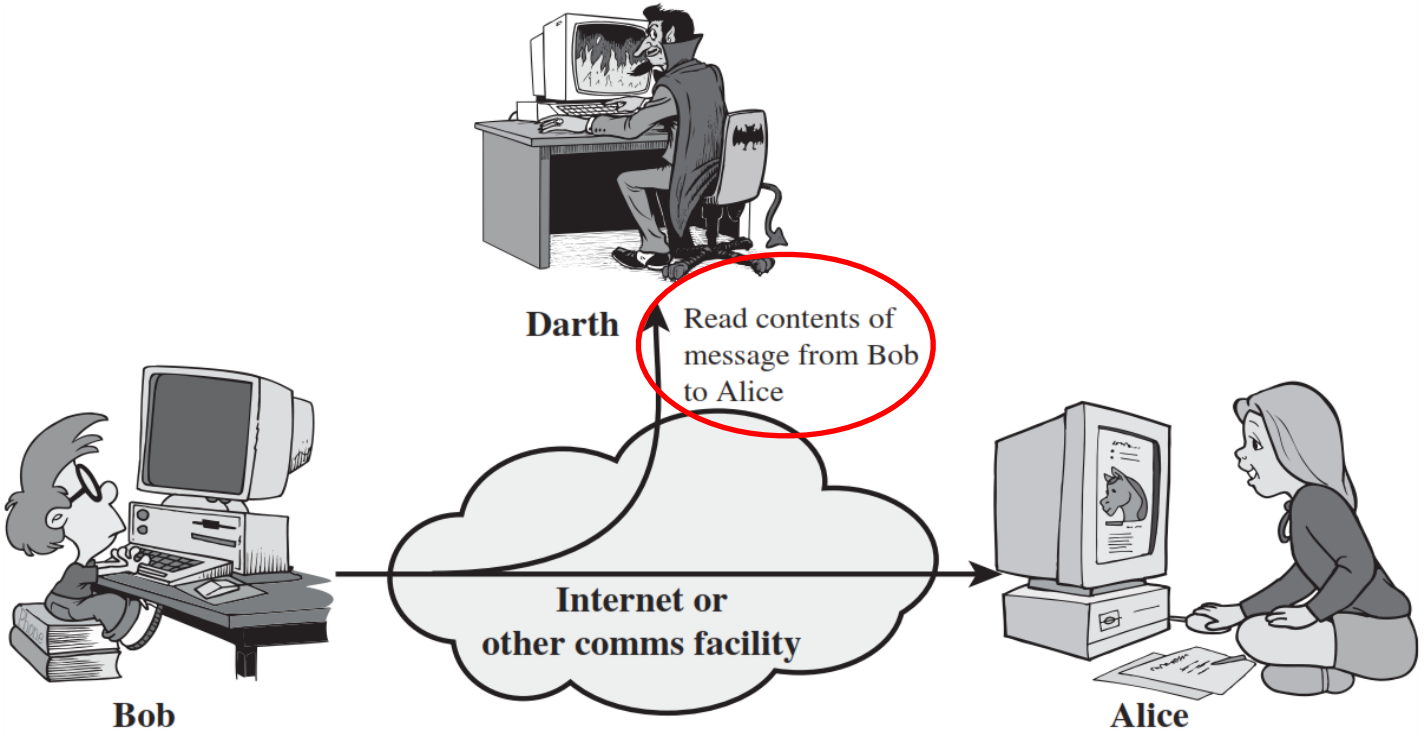
- **Scope and Function:**
  - **Security Mechanism:** The tools and techniques used to implement security.
  - **Security Service:** The overall security functions and objectives provided to implement security.
- **Implementation vs. Provision:**
  - **Security Mechanism:** The "how" of security (e.g., how encryption is performed, how access is controlled).
  - **Security Service:** The "what" of security (e.g., what is achieved with encryption, what is ensured by access control).
- Example: Encryption
  - Security mechanism: Describes the algorithm and method used (e.g., DES, AES)
  - Security Service: Ensures confidentiality of data

Security Attacks

- A **passive attack** attempts to learn or make use of information from the system but does not affect system resources.
  1. Eavesdropping
  2. Traffic analysis

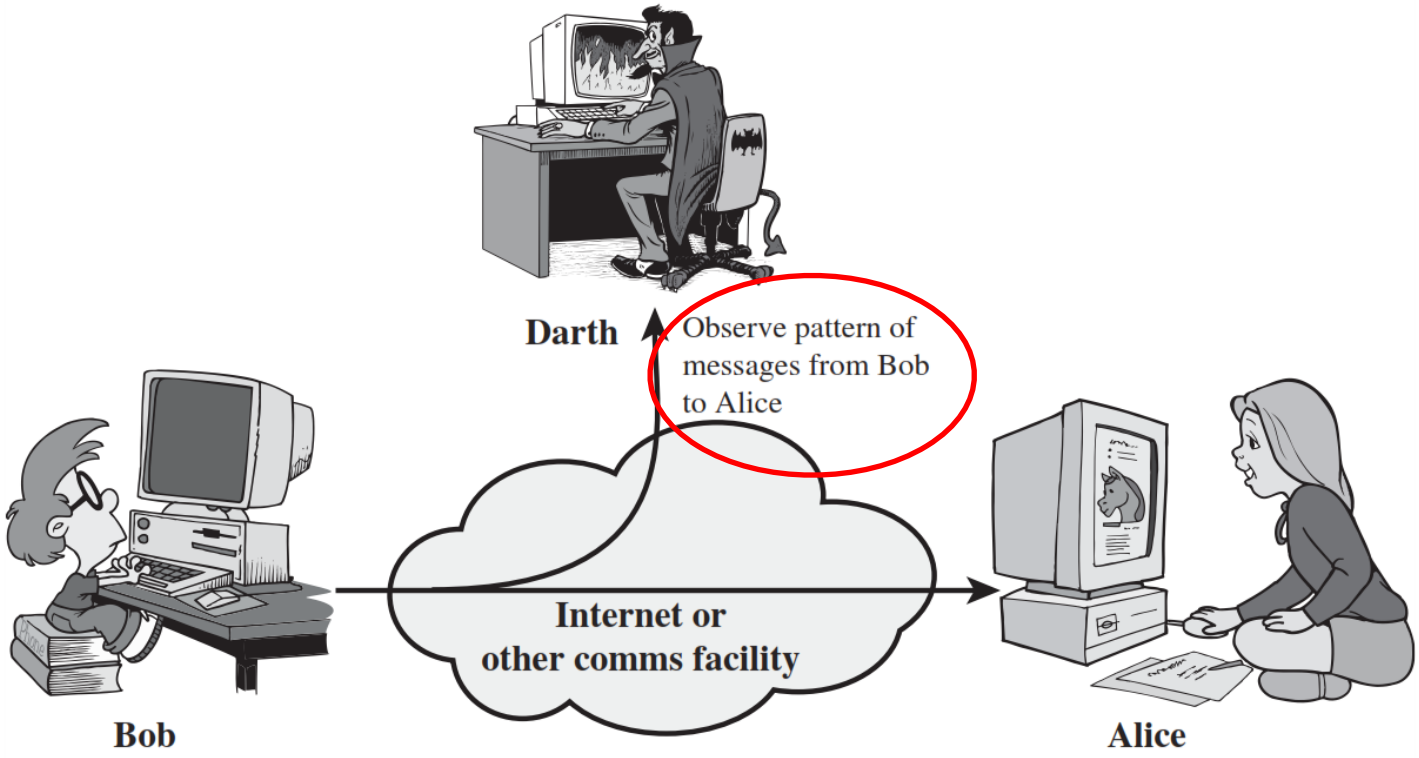
  (Port Scanning and Keylogging are also types of passive attack)
- An **active attack** attempts to alter system resources or affect their operation.
  1. Masquerade (impersonating a legitimate user)
  2. Replay (valid data transmission is maliciously repeated or delayed)
  3. Modification of messages
  4. Denial of service

1) Release of message contents (Passive Attack)



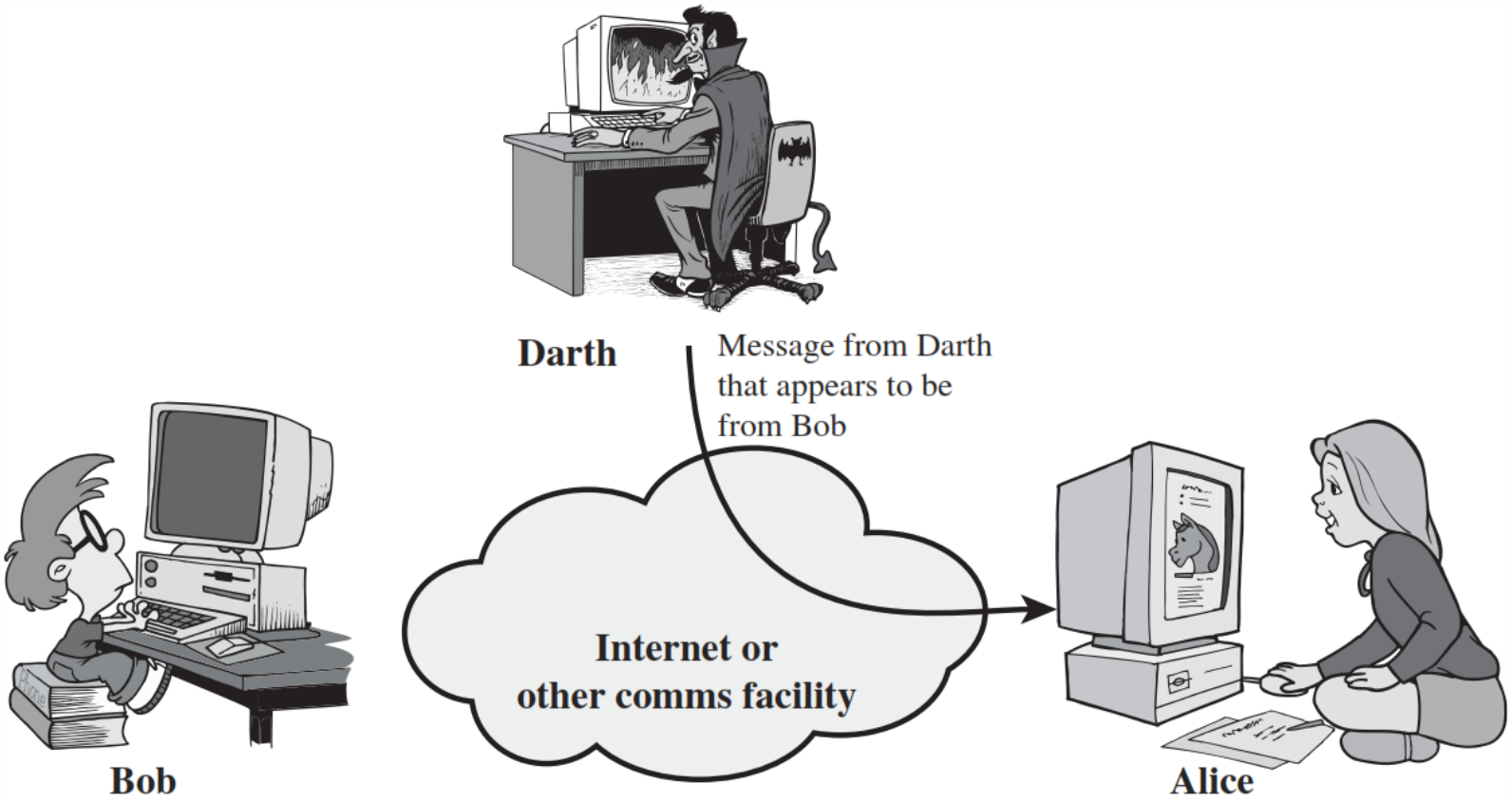
- A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information.
- We would like to prevent an opponent from learning the contents (Eavesdropping) of these transmissions.

2) Traffic Analysis (Passive Attack)



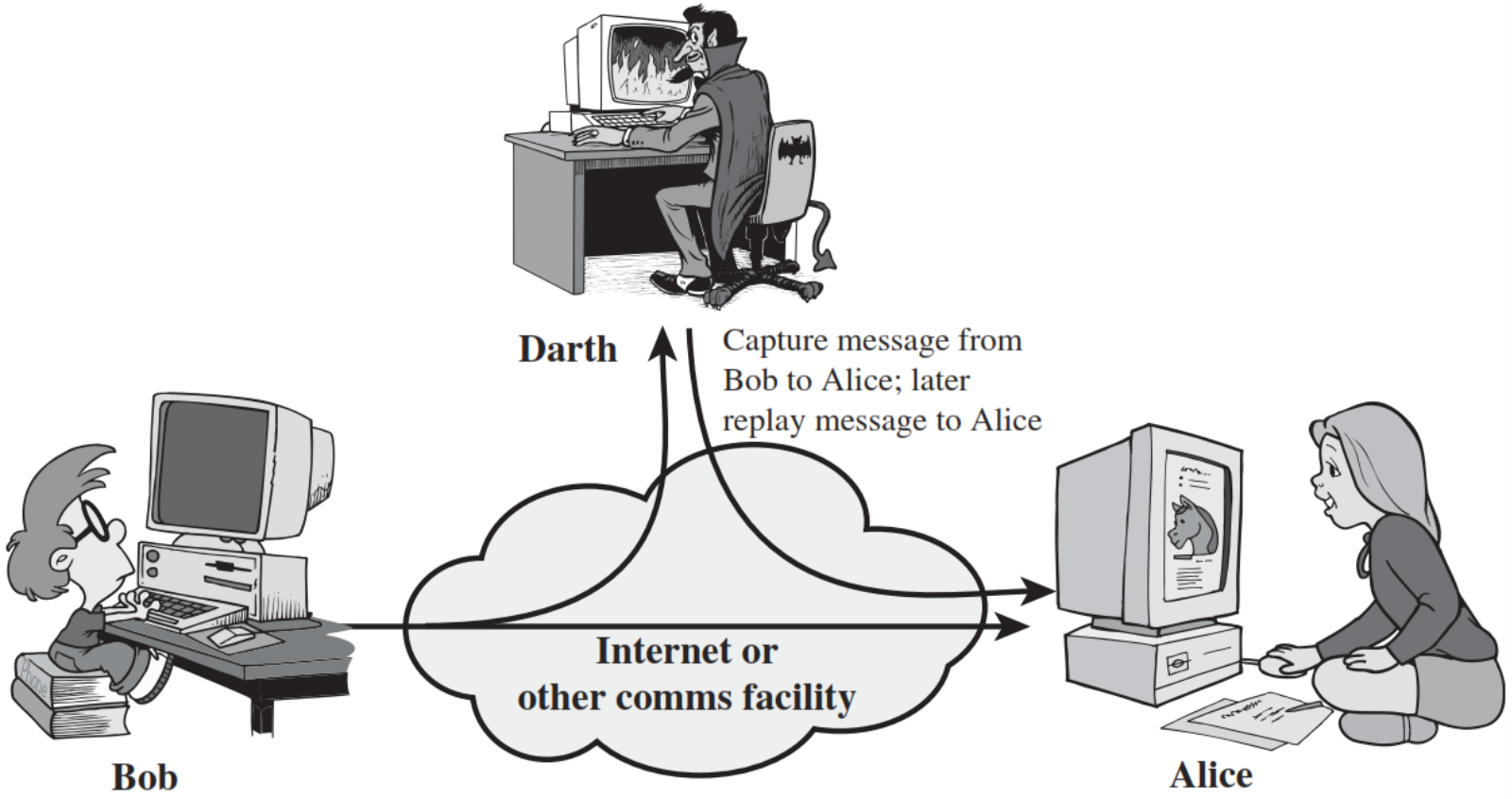
- In such attacks, an adversary capable of observing network traffic statistics in several different networks, correlates the traffic patterns in these networks.

1) Masquerade Attack (Active Attack)



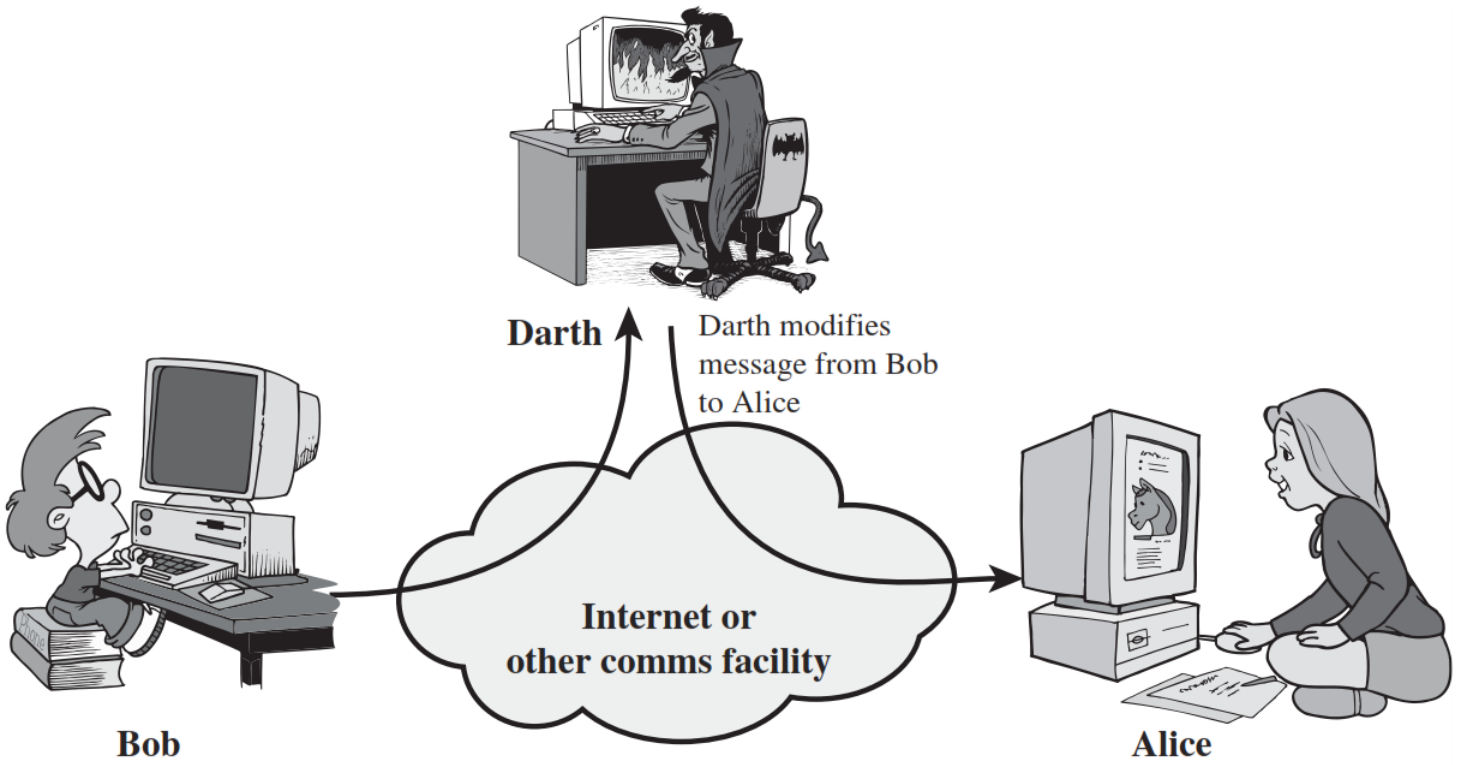
- A **masquerade** takes place when one entity pretends to be a different entity.

2) Replay Attack (Active Attack)



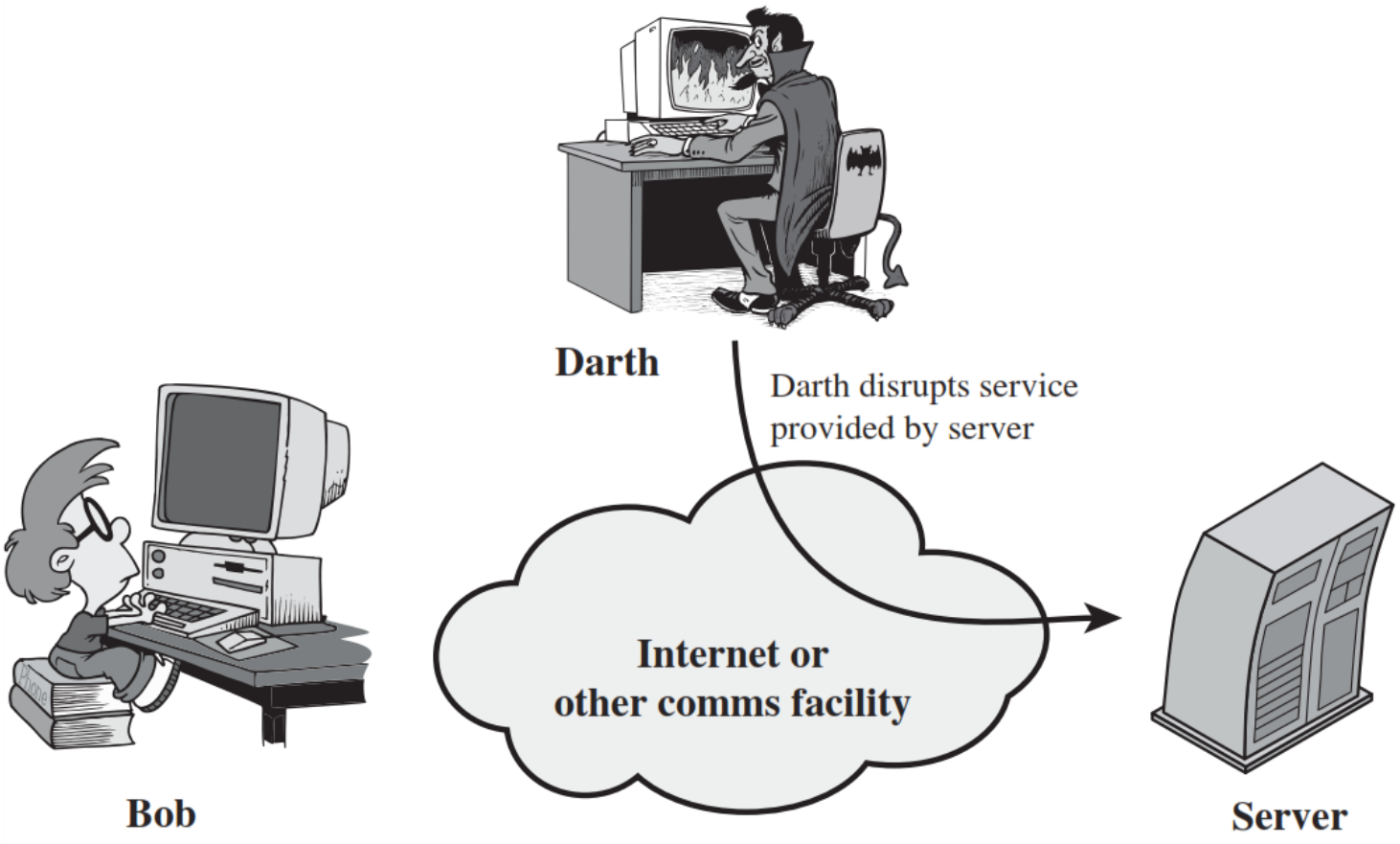
- **Replay attack** involves the passive capture of a data unit and its subsequent retransmission/delay to produce an unauthorized effect.

3) Modification of messages Attack (Active Attack)



- **Modification of messages** simply means that some portion of a legitimate message is altered, or that messages are reordered, to produce an unauthorized effect.

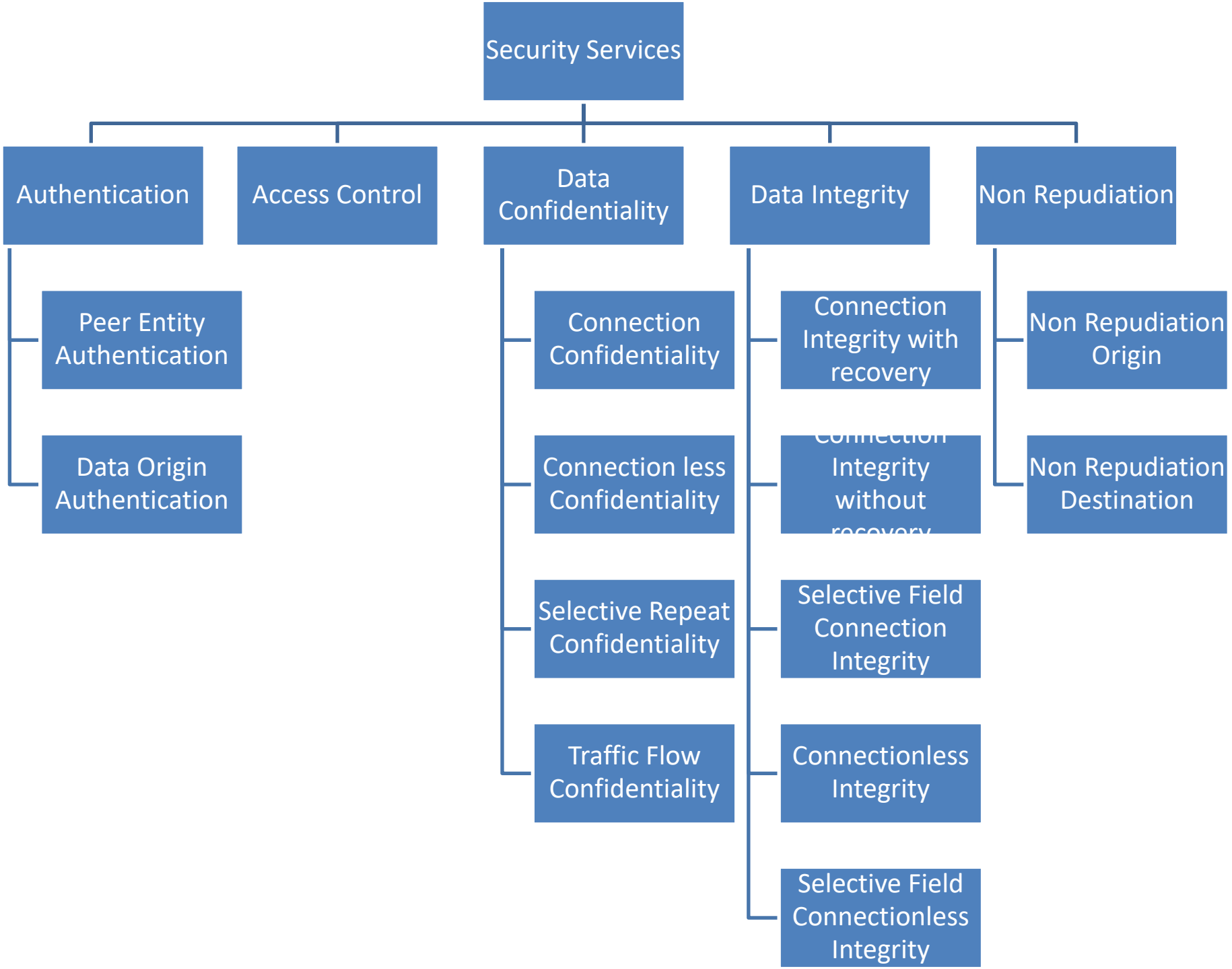
4) Denial of Service Attack (Active Attack)



- **The denial of service** attack prevents the normal use or management of communications facilities.

Security Services (X.800)

- X.800 standard defines a security service as a service provided by a protocol layer of communicating open systems that ensures the security of the systems themselves or the security of data transfers between them.


Security Services
Authentication
Access Control
Data Confidentiality
Data Integrity
Non Repudiation
Peer Entity Authentication
Data Origin Authentication
Connection Confidentiality
Connection less Confidentiality
Selective Repeat Confidentiality
Traffic Flow Confidentiality
Connection Integrity with recovery
Integrity without
Selective Field Connection Integrity
Connectionless Integrity
Selective Field Connectionless Integrity
Non Repudiation Origin
Non Repudiation Destination

Authentication

- **Authentication** is the assurance that the communicating entity is the one that it claims to be.

1. **Peer Entity Authentication:** Verifying the identity of entities (such as users, devices, or systems) involved in a communication session.
2. **Data-Origin Authentication:** In a connectionless transfer, providing assurance that the source of received data is as claimed.

Who you are ?
(biometrics)

Use of physical or behavioral characteristics

Physical authentication

Geolocation (GPS data)
where you are ?

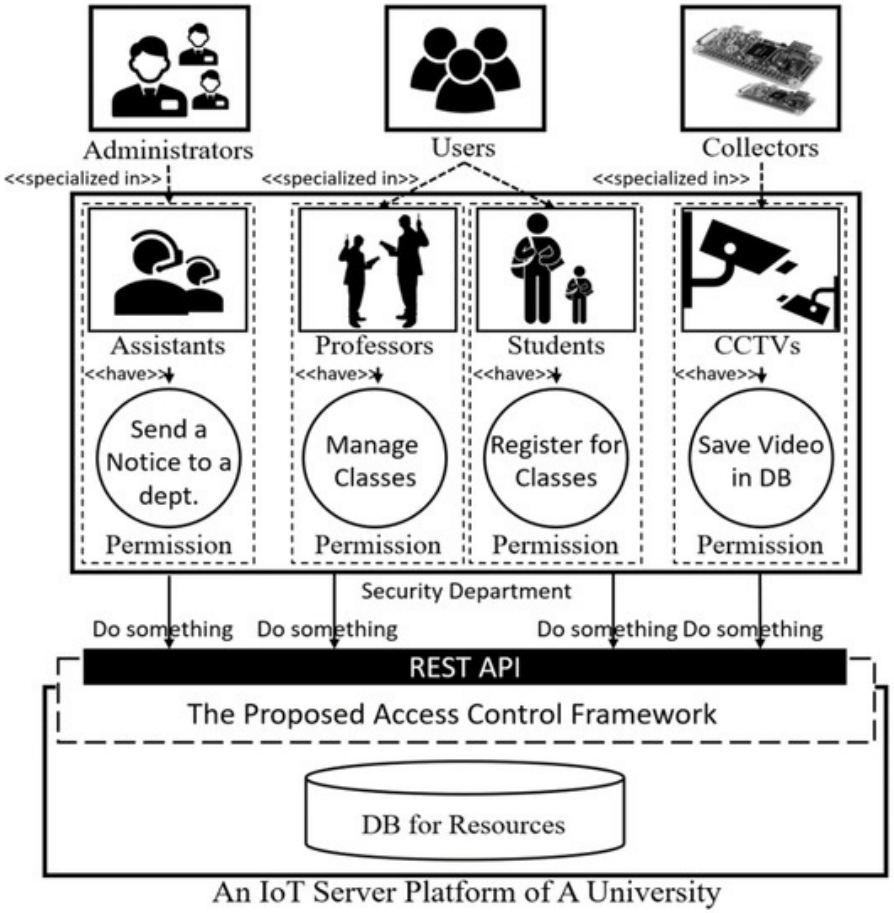
What you know ?

Knowledge-based Authentication

- Password
- One-time Passwords
- Network address

Access Control

- **Access control** is 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 the accessing resource is allowed to do).

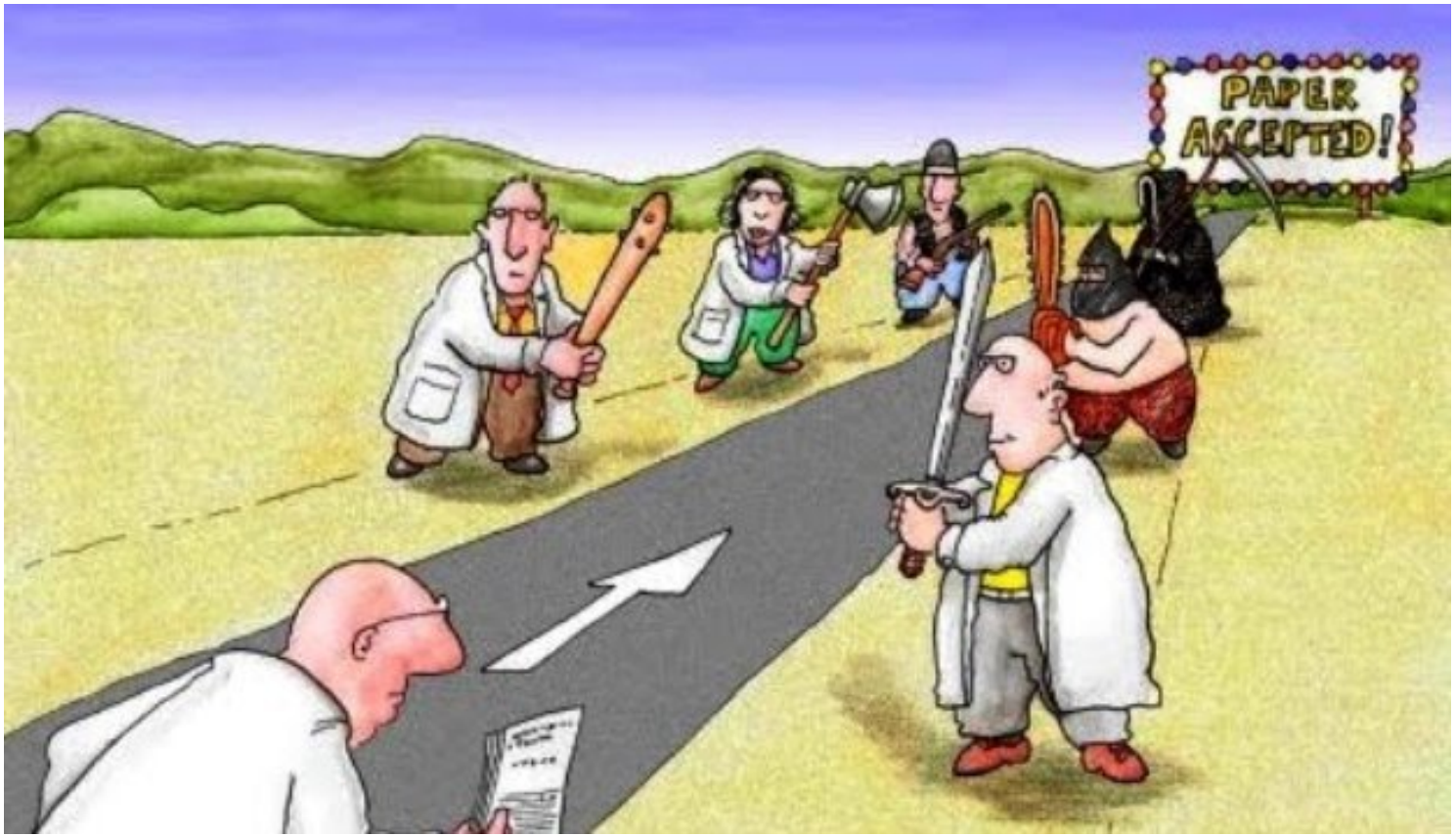


Data Confidentiality

- **Data confidentiality** is the protection of data from unauthorized disclosure.
  1. **Connection Confidentiality:** The protection of all user data during a continuous connection.
  2. **Connectionless Confidentiality:** The protection of all user data regardless of the absence of a continuous connection.
  3. **Selective-Field Confidentiality:** The confidentiality of selected fields within the user data on a connection or in a single data block.
  4. **Traffic-Flow Confidentiality:** The protection of the information that might be derived from observation of

Data Integrity

- Data integrity is the assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, or deletion).



Data Integrity (Cont…)

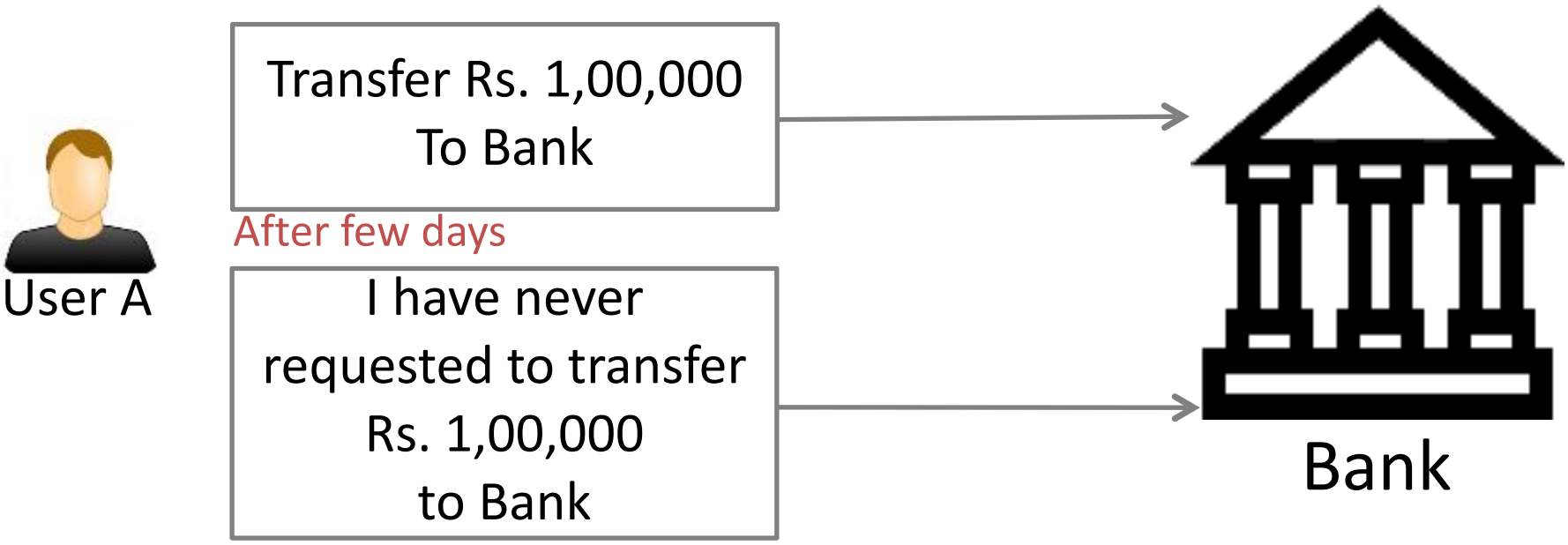
- **Connection Integrity with Recovery:** Provides integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data with recovery attempted.
- **Connection Integrity without Recovery:** As above, but provides only detection without recovery.
- **Selective-Field Connection Integrity:** Provides integrity of selected fields within the user data and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.

Data Integrity (Cont…)

- **Connectionless Integrity:** Provides integrity of a **single** connectionless data block and may detect data modification and replay.
- **Selective-Field Connectionless Integrity:** Provides integrity of selected fields within a **single** connectionless data block; Determines whether the selected fields have been modified.

Non Repudiation

- **Nonrepudiation** is the assurance that someone cannot deny something.
- Typically, nonrepudiation refers to the ability to ensure that a party in the communication cannot deny the authenticity of their signature on a document or message that he originated/received.



Non Repudiation (Cont…)

- **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 (X.800)

- X.800 provides a structured framework for security in the OSI environment
- Includes various security services and mechanisms needed to protect data communications.
- Security Services: defines specific security services such as authentication, access control, data confidentiality, data integrity, and non-repudiation.
- Security Mechanisms: specifies security mechanisms that implement the security services. These mechanisms include encryption, digital signatures, access control mechanisms, and data integrity checks.
  - **Specific security mechanisms:** Integrated into the appropriate protocol layer in order to provide some of the OSI security services.
  - **Pervasive security mechanisms:** Not integrated to any particular protocol layer

Security Mechanism (Specific Security)

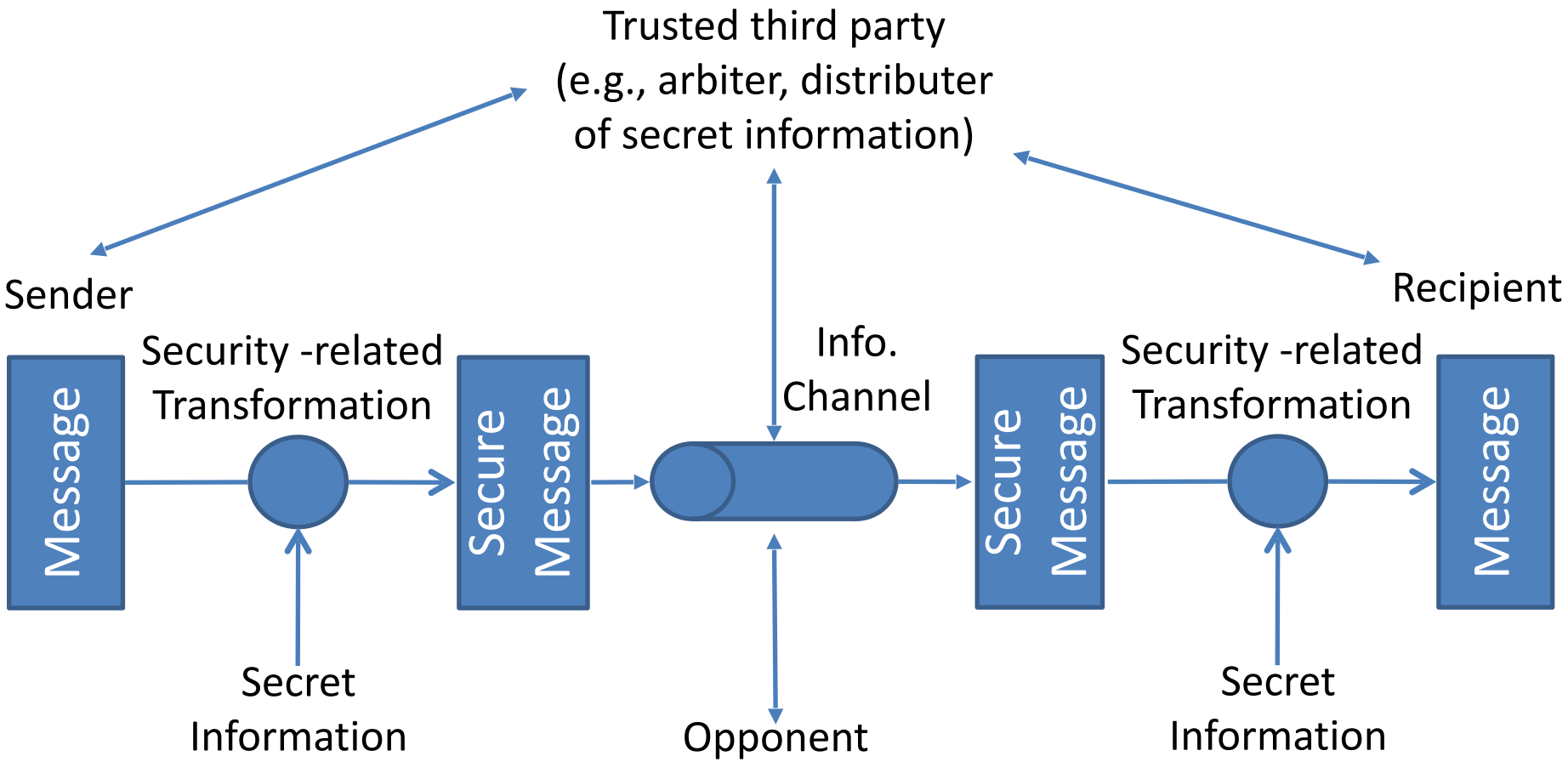
- **Encipherment:** Hiding or covering data using mathematical algorithms.
- **Digital Signature:** The sender can electronically sign the data and the receiver can electronically verify the signature.
- **Access Control:** A variety of mechanisms that enforce access rights to resources.
- **Data Integrity:** A variety of mechanisms used to assure the integrity of a data unit or stream of data units.
- **Authentication Exchange:** Two entities exchange some messages to prove their identity to each other.

…

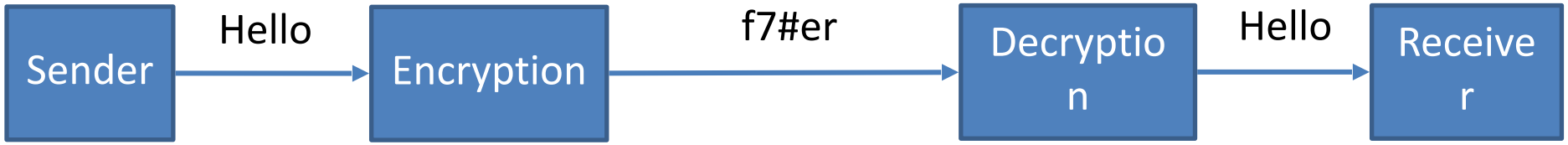
…Security Mechanism (Specific Security)

- **Traffic Padding:** The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.
- **Routing Control:** Selecting and continuously changing routes between sender and receiver to prevent opponent from eavesdropping.
- **Notarization:** The use of a trusted third party to assure and control the communication. It acts as a mediator between sender and receiver so that chance of conflict is reduced.

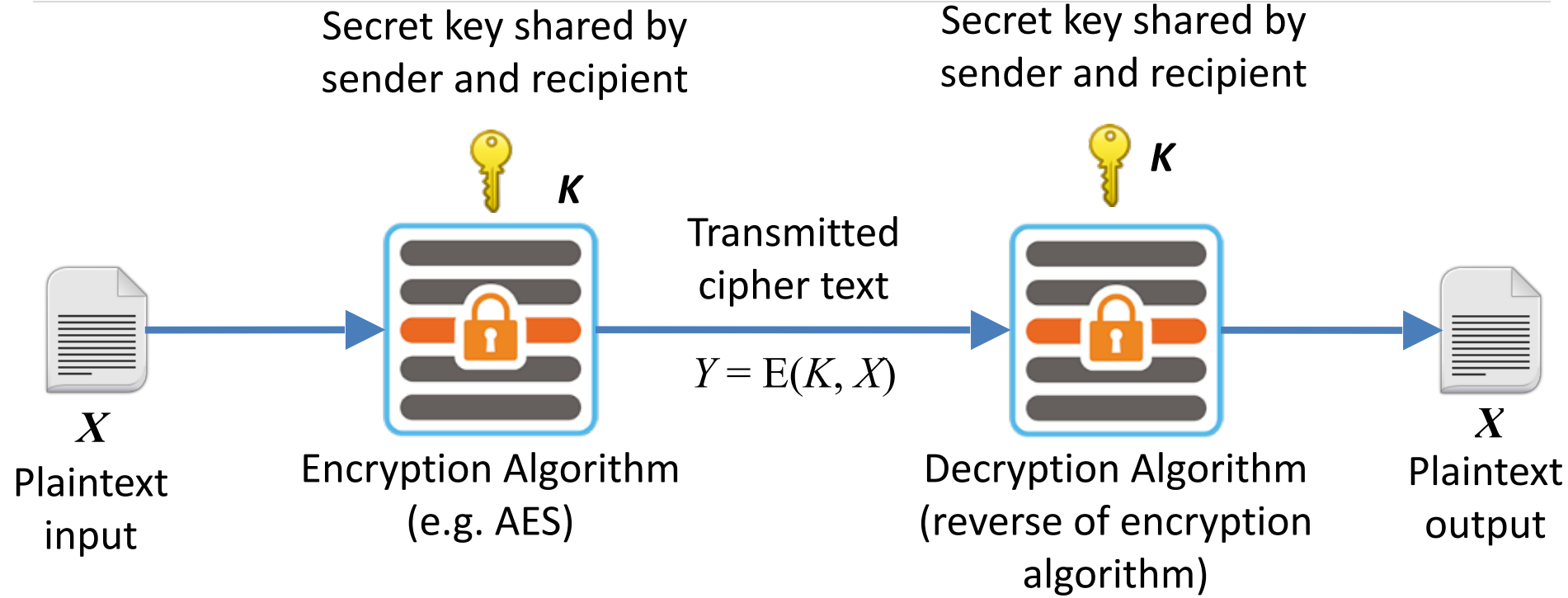
Model for Network Security



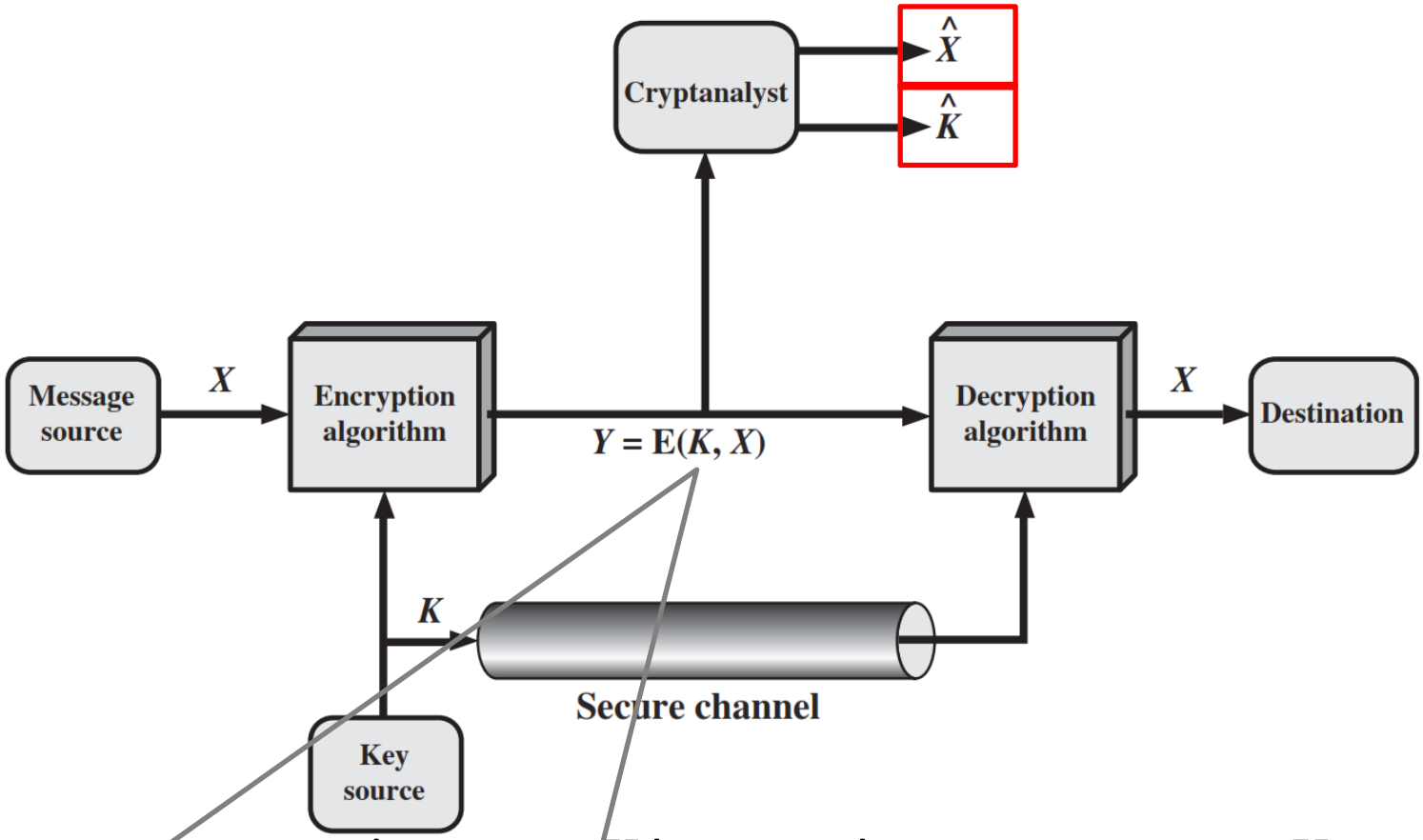
Encryption and Decryption



Symmetric Cipher Model (Conventional Encryption)



- [illegible]
- [illegible]
- [illegible]
- [illegible]



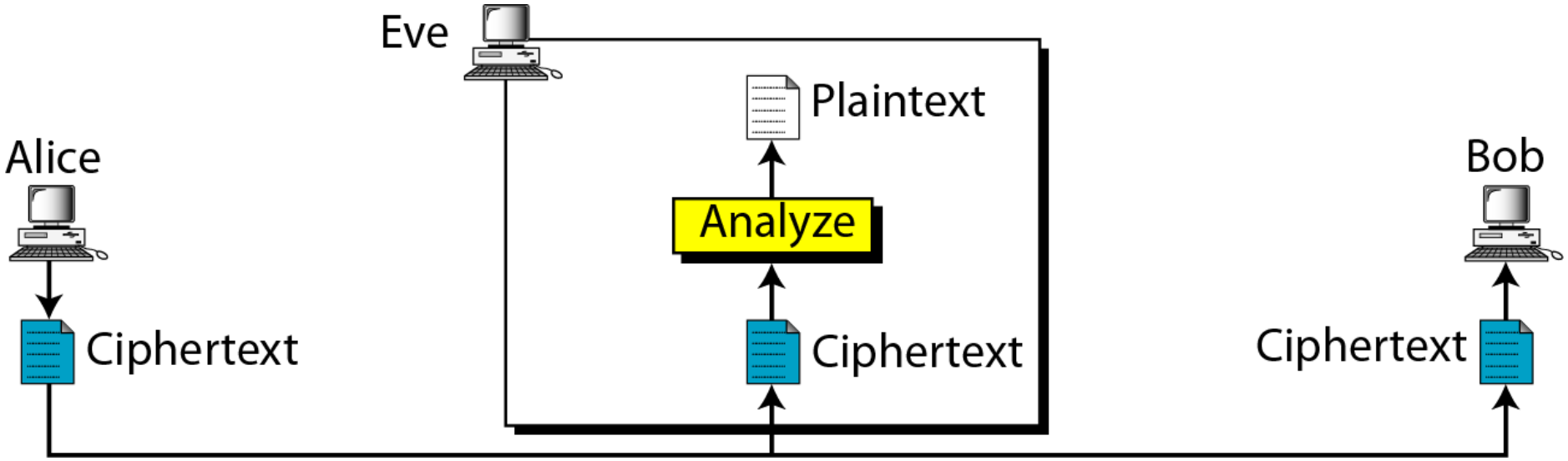
- An opponent, observing Y but not having access to K or X, may attempt to recover X or K or both X and K.
- If the opponent is interested in only this particular message, then he will focus to recover X by generating a plaintext estimate $\hat{X}$.
- Often, however, the opponent is interested in being able to read future messages as well, in which case an attempt is made to recover K by generating an estimate $\hat{K}$.

Cryptanalysis and Brute-Force Attack

- **Cryptanalysis** is the study and practice of analyzing and breaking cryptographic systems. The main goal of cryptanalysis is to uncover the underlying plaintext from ciphertext without knowing the secret key used for encryption.
- Cryptanalytic attacks rely on the nature of the algorithm and some knowledge of the general characteristics of the plaintext or even some sample plaintext–ciphertext pairs.
- This type of attack exploits the characteristics of the algorithm to attempt to derive a specific plaintext or to derive the key being used.
- **Brute-force attack:** The attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained.
- On an average, half of all possible keys must be tried to achieve success.

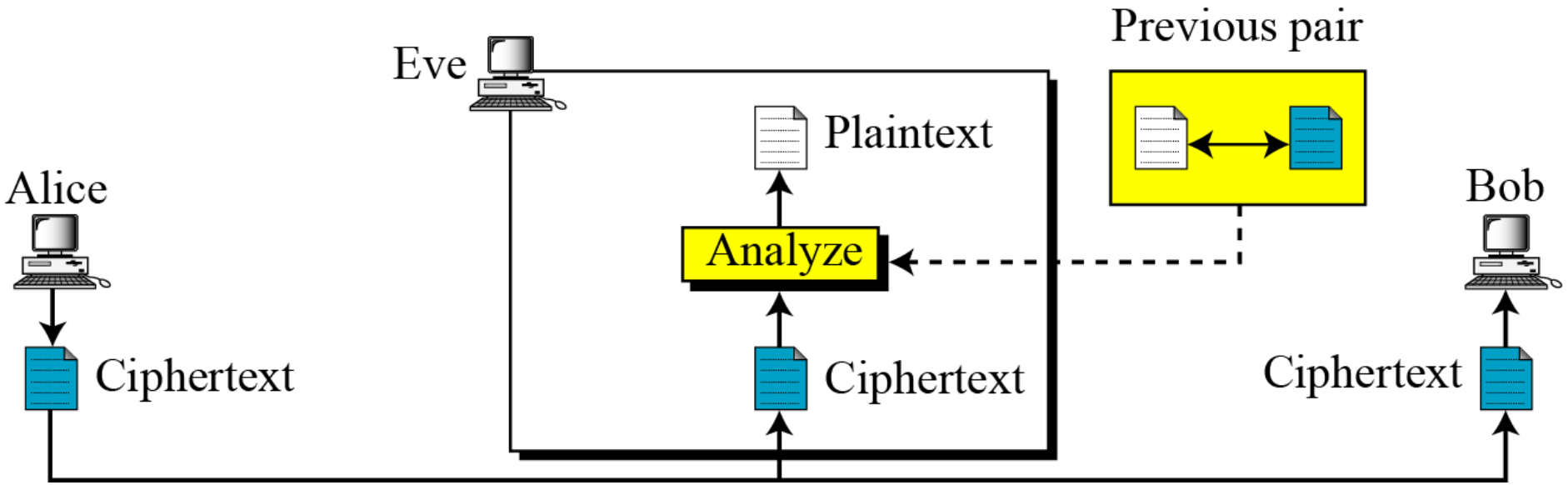
Attacks on Encrypted Messages

Type of Attack	Known to cryptanalyst
Ciphertext Only	Encryption algorithm, Ciphertext



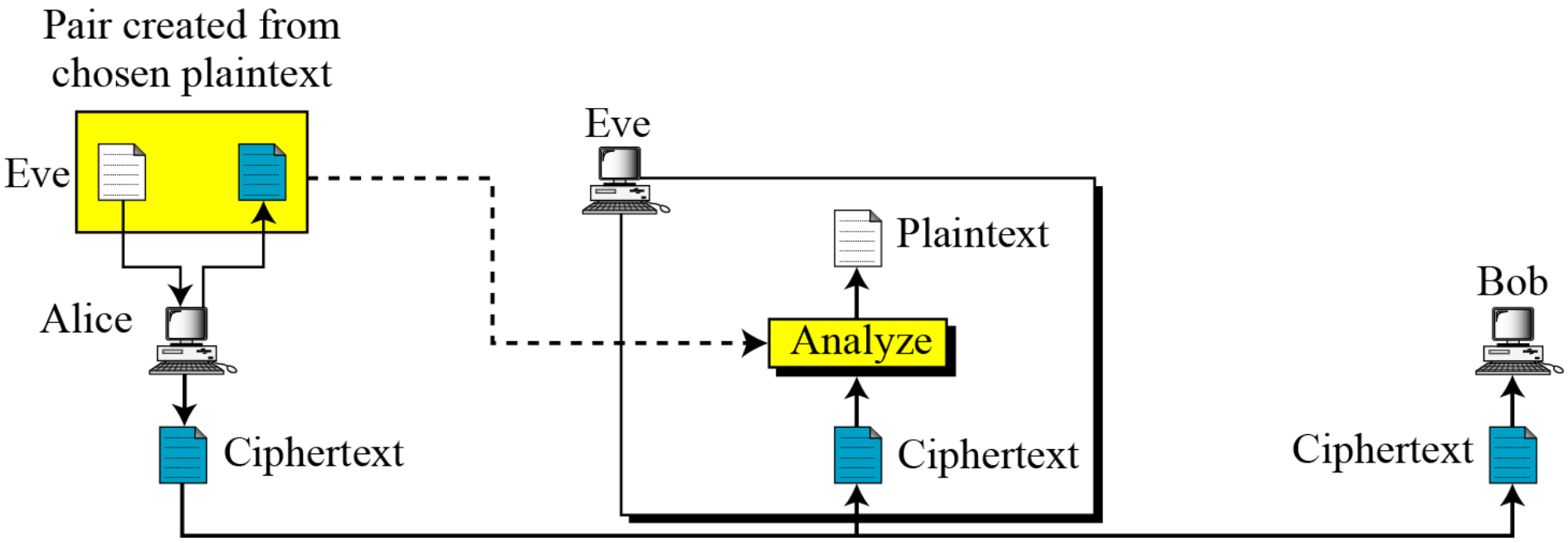
Attacks on Encrypted Messages

Type of Attack	Known to cryptanalyst
Known Plaintext	Encryption algorithm, Ciphertext, One or more plaintext-cipher text pairs formed with the secret key



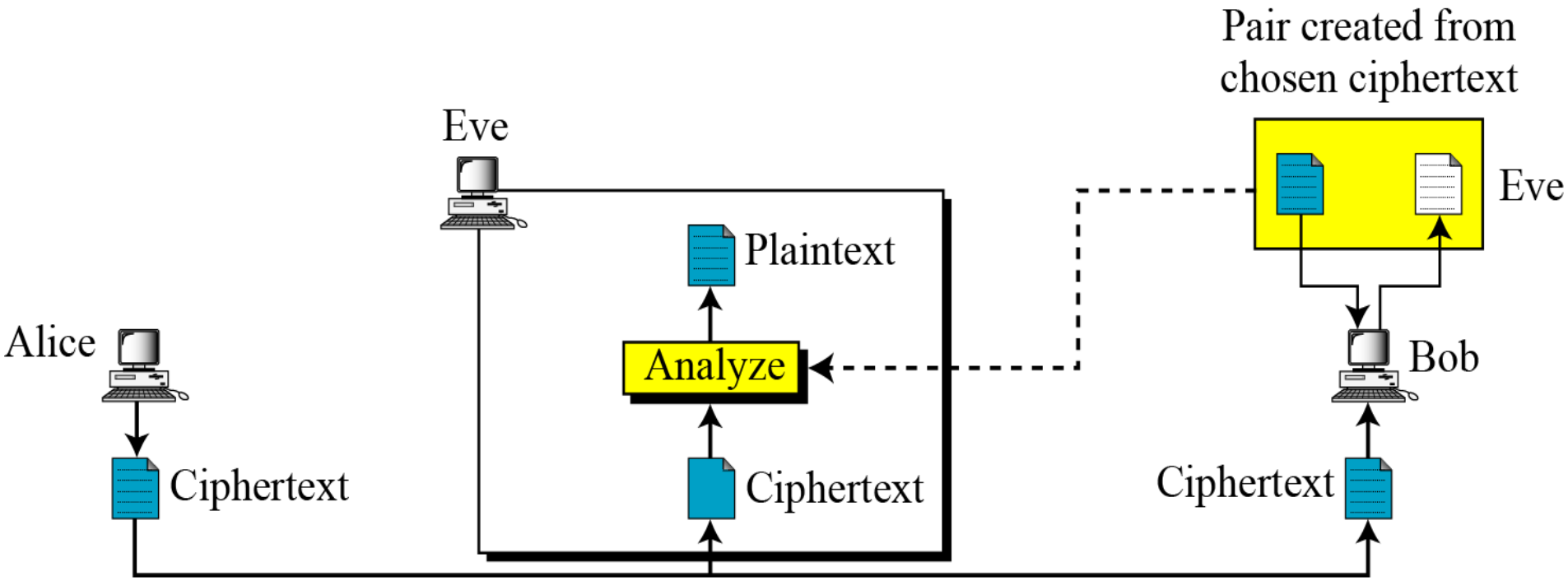
Attacks on Encrypted Messages

Type of Attack	Known to cryptanalyst
Chosen Plaintext	Encryption algorithm, Ciphertext, Plaintext message chosen by cryptanalyst with its corresponding ciphertext



Attacks on Encrypted Messages

Type of Attack	Known to cryptanalyst
Chosen Ciphertext	Encryption algorithm, Ciphertext, Ciphertext chosen by cryptanalyst, with its corresponding decrypted plaintext generated with the secret key



Attacks on Encrypted Messages

Type of Attack	Known to cryptanalyst
Chosen text	Encryption algorithm, Ciphertext, Plaintext chosen by cryptanalyst, with its corresponding ciphertext generated with the secret key , Ciphertext chosen by cryptanalyst, with its corresponding decrypted plaintext generated with the secret key

Substitution Ciphers

- A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols.
  1) Caesar Cipher
  2) Monoalphabetic Cipher
  3) Playfair Cipher
  4) Hill Cipher
  5) Polyalphabetic Ciphers
  6) One-Time Pad

1) Caesar Cipher

- The **Caesar cipher** involves replacing each letter of the alphabet with the letter standing *k* places further down the alphabet.
- In encryption each plaintext letter P, substitute the ciphertext letter C:

$$C = E(k, P) = (P + k) \bmod 26$$
$$C = E(3, P) = (P + 3) \bmod 26$$

- For decryption algorithm is:

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

Caesar Cipher (Cont…)

- 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

$$C = E(3, P) = (P + 3) \bmod 26$$

```
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
```

Example:

Plaintext: THE QUICK BROWN FOX

Ciphertext: WKH TXLFN EURZQ IRA

Brute force attack on Caesar Cipher

- The encryption and decryption algorithms are known.
- There are only 25 keys to try.
- The language of the plaintext is known and easily recognizable.

Brute force attack on Caesar Cipher

Ciphertext: `ZNK WAOIQ HXUCT LUD`

Key	Transformed text
1	YMJ VZNHP GWTBS KTC
2	XLI UYMGO FVSAR JSB
3	WKH TXLFN EURZQ IRA
4	VJG SWKEM DTQYP HQZ
5	UIF RVJDL CSPXOGPY
6	THE QUICK BROWN FOX
7	SGD PTHBJ AQNVM ENW
8	RFC OSGAI ZPMUL DMV
9	QEB NRFZH YOLTK CLU
10	PDA MQEYG XNKSJ BKT
11	OCZ LPDXF WMJRI AJS
12	NBY KOCWE VLIQH ZIR
13	MAX JNBVD UKHPG YHQ

Key	Transformed text
14	LZW IMAUC TJGOF XGP
15	KYV HLZTB SIFNE WFO
16	JXU GKYSA RHEMD VEN
17	IWT FJXRZ QGDLC UDM
18	HVS EIWQY PFCKB TCL
19	GUR DHVPX OEBJA SBK
20	FTQ CGUOW NDAIZ RAJ
21	ESP BFTNV MCZHY QZI
22	DRO AESMU LBYGX PYH
23	CQN ZDRLT KAXFW OXG
24	BPM YCQKS JZWEV NWF
25	AOL XBPJR IYVDU MVE

Substitution Techniques

1) Caesar Cipher
2) **Monoalphabetic Cipher**
3) Playfair Cipher
4) Hill Cipher
5) Polyalphabetic Ciphers
6) One-Time Pad

2) Monoalphabetic Cipher (Simple substitution)

- It is an improvement to the Caesar Cipher.
- Instead of shifting the alphabets by some number, this scheme uses some permutation of the letters in alphabet.
- The sender and the receiver decide on a randomly selected permutation of the letters of the alphabet.
- With 26 letters in alphabet, the possible permutations are 26! which is equal to 4x1026.

```
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: y n l k x b s h m i w d p j r o q v f e a u g t
z c
```

Attack on Monoalphabetic Cipher

Ciphertext:

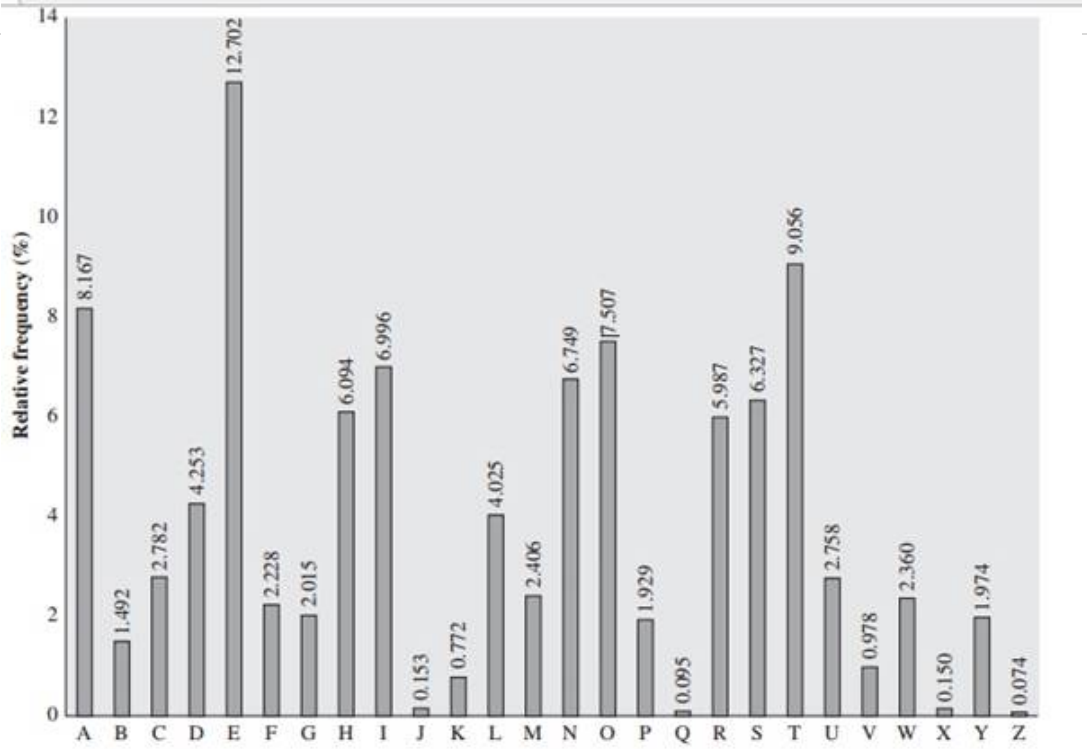
uzqsovuohxmopvgpozpevsg**zw**szopfpesxudbmetsxaizvu
ephzhmdzshzowsfpappdtsvpqu**zw**ymxuzuhsxepyepopdzs
zufpomb**zw**pfupzhmdjudtmohmq

- The relative frequencies of the letters in the ciphertext (in percentages) are

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

…Attack on Monoalphabetic Cipher

Standard Frequency Distribution chart for English



Matching ciphertext frequency in the standard distribution chart of English

Ciphertext Letter	Ciphertext letter Frequency	Related Plaintext Letter Frequency	Related Plaintext Letter
P	13.33	~12.02	e
Z	11.67	~9.06	t

- In our ciphertext, the most common digram is ZW, which appears three times. So equate Z with t, W with h and P with e.
- Now notice that the sequence ZWP appears in the ciphertext, and we can translate that sequence as “the.”

…Attack on Monoalphabetic Cipher

- If the cryptanalyst knows the nature of the plaintext, then the analyst can exploit the regularities of the language.
- The relative frequency of the letters can be determined and compared to the standard frequency distribution for English.
- If the message were long enough, this technique alone might be sufficient, but because in this example, message is relatively short, we cannot expect an exact match.

Substitution Techniques

1) Caesar Cipher
2) Monoalphabetic Cipher
3) **Playfair Cipher**
4) Hill Cipher
5) Polyalphabetic Ciphers
6) One-Time Pad

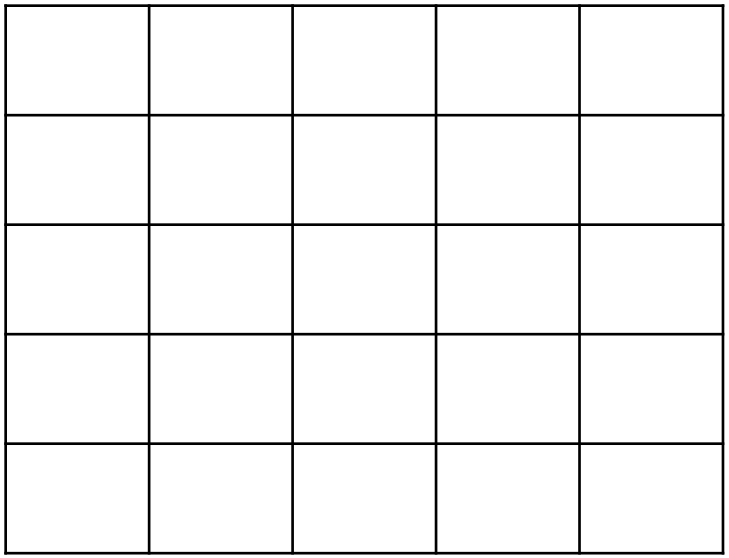
3) Playfair Cipher

- The Playfair algorithm is based on a 5 × 5 matrix (**key**) of letters.
- The matrix is constructed by filling in the letters of the **keyword** (minus duplicates) from left to right and from top to bottom, and then filling in the remainder of the matrix with the remaining letters in alphabetic order. **The letters I and J count as one letter**.

Example:

Keyword= OCCURRENCE

Plaintext= TALL TREES



Playfair Cipher - Encrypt Plaintext

- Playfair, treats digrams (two letters) in the plaintext as single units and translates these units into ciphertext digrams.
- Make Pairs of letters add filler letter "**X**" if same letter appears in a pair.

  Plaintext= `TALL TREES`

  Plaintext= `TA LX LT RE ES`
- If there is an odd number of letters, then add uncommon letter to complete digram, a X/Z may be added to the last letter.

Playfair Cipher - Encrypt Plaintext

- Map each pair in key matrix

Plaintext= `TA LX LT RE`

Ciphertext= `PF IZ TZ EO RT`

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

- If the letters appear on the same row, replace them with the letters to their immediate right respectively (with wrap around to the left side of the row if necessary).
- The order is important - the first letter of the pair should be replaced first.
- For example, using the table above, the letter pair **TA** would be encoded as **PF**.
- If both the letters are in the same column: Take the letter below each one (going back to the top if at the bottom).
- If both the letters are in the same row: Take the letter to the right of each one (going back to the leftmost if at the rightmost position).

Playfair Cipher Examples

1. Key= “ engineering ” Plaintext=” test this process ”
2. Key= “ keyword ” Plaintext=” come to the window ”
3. Key= “ moonmission ” Plaintext=” greet ”

E N G I R A B C D F H K L M O P Q S T U V W X Y Z	Encrypted Message: pi tu pm gt ue lf gp xg

K E Y W O R D A B C F G H I L M N P Q S T U V X Z	Encrypted Message: lc nk zk vf yo gq ce bw

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

Substitution Techniques

1) Caesar Cipher
2) Monoalphabetic Cipher
3) Playfair Cipher
4) **Hill Cipher**
5) Polyalphabetic Ciphers
6) One-Time Pad

4) Hill Cipher

- Hill cipher is based on linear algebra
- Each letter is represented by numbers from 0 to 25 and calculations are done modulo 26.
- Encryption and decryption can be given by the following formula:

Encryption: $C=KP \bmod 26$

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

$$\begin{pmatrix} c_1 & c_2 & c_3 \end{pmatrix} = \begin{pmatrix} k11 & k12 & k13 \\ k21 & k22 & k23 \\ k31 & k32 & k33 \end{pmatrix} \begin{pmatrix} p_1 & p_2 & p_3 \end{pmatrix} \bmod 26$$

Hill Cipher Encryption

- To encrypt a message using the Hill Cipher we must first turn our keyword and plaintext into a matrix (a 2 x 2 matrix or a 3 x 3 matrix, etc).

Example: Key = "HILL", Plaintext = "EXAM"

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

$$\text{Key Matrix} \begin{pmatrix} \text{H} & \text{I} \\ \text{L} & \text{L} \end{pmatrix} = \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}$$

$$\text{Plaintext} \begin{pmatrix} \text{E} \\ \text{X} \end{pmatrix} \begin{pmatrix} \text{A} \\ \text{M} \end{pmatrix} = \begin{pmatrix} 4 \\ 23 \end{pmatrix} \begin{pmatrix} 0 \\ 12 \end{pmatrix}$$

Hill Cipher Encryption (Cont…)

$$\text{Key Matrix} = \begin{pmatrix} H & I \\ L & L \end{pmatrix} = \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \qquad \text{Plaintext} \begin{pmatrix} E \\ X \end{pmatrix} \begin{pmatrix} A \\ M \end{pmatrix} = \begin{pmatrix} 4 \\ 23 \end{pmatrix} \begin{pmatrix} 0 \\ 12 \end{pmatrix}$$

C=KP mod 26

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 4 \\ 23 \end{pmatrix}$$

$7 \times 4 + 8 \times 23 = 212$

$11 \times 4 + 11 \times 23 = 297$

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 4 \\ 23 \end{pmatrix} = \begin{pmatrix} 212 \\ 297 \end{pmatrix}$$

$$\begin{pmatrix} 212 \\ 297 \end{pmatrix} = \begin{pmatrix} 4 \\ 11 \end{pmatrix} \bmod 26 = \begin{pmatrix} E \\ L \end{pmatrix}$$

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 0 \\ 12 \end{pmatrix}$$

$7 \times 0 + 8 \times 12 = 96$

$11 \times 0 + 11 \times 12 = 132$

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 0 \\ 12 \end{pmatrix} = \begin{pmatrix} 96 \\ 132 \end{pmatrix}$$

$$\begin{pmatrix} 96 \\ 132 \end{pmatrix} = \begin{pmatrix} 18 \\ 2 \end{pmatrix} \bmod 26 = \begin{pmatrix} S \\ C \end{pmatrix}$$

Ciphertext = "ELSC"

Hill Cipher Decryption

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

Step:1 Find Inverse of key matrix

Step:2 Multiply the Multiplicative Inverse of the Determinant by the Adjoin Matrix

Step:3 Multiply inverse key matrix with ciphertext matrix to obtain plaintext matrix

Step: 1 Inverse of key matrix

2 X 2 inverse of matrix

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad - cb} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

3 X 3 inverse of matrix

$$A^{-1} = \frac{1}{\text{determinant}(A)} \bullet \text{adjoin}(A)$$

Step: 1 Inverse of key matrix

$$\text{Inverse Key Matrix} = \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}^{-1} = \frac{1}{77-88}\begin{pmatrix} 11 & -8 \\ -11 & 7 \end{pmatrix}$$

$$= \frac{1}{-11}\begin{pmatrix} 11 & -8 \\ -11 & 7 \end{pmatrix}$$

$$= \frac{1}{15}\begin{pmatrix} 11 & 18 \\ 15 & 7 \end{pmatrix} \bmod 26$$

- -11 mod 26 = 15
- Because, modulo for negative number is = N- (B%N)
  = 26 – (11%26)

Step: 2 Modular (Multiplicative) inverse

- The inverse of a number A is 1/A since A * 1/A = 1

  e.g. the inverse of 5 is 1/5
- In modular arithmetic we do not have a division operation.
- The modular inverse of A (mod C) is A^{-1}
- **$(A * A^{-1}) \equiv 1 \pmod{C}$**

Example:

- The modular inverse of A mod C is the A^{-1} value that makes

  $A * A^{-1} \bmod C = 1$

  A = 3, C = 11

  Since (3*4) mod 11 = 1, **4** is modulo inverse of **3**

  A = 10, C = 17 , A^{-1} = **12**

Step 2: Modular (Multiplicative) inverse

Determinants' multiplicative inverse Modulo 26												
Determinant	1	3	5	7	9	11	15	17	19	21	23	25
Inverse Modulo 26	1	9	21	15	3	19	7	23	11	5	17	25

$$= \frac{1}{15}\begin{pmatrix} 11 & 18 \\ 15 & 7 \end{pmatrix} \bmod 26$$

- Multiplicative inverse of $\frac{1}{15}$ is 7

Step 2: Multiply with adjoin of matrix

$$= 7\begin{pmatrix} 11 & 18 \\ 15 & 7 \end{pmatrix} = \begin{pmatrix} 77 & 126 \\ 105 & 49 \end{pmatrix} = \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix} \bmod 26$$

$$= \text{thus, if } K = \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \text{ then } K^{-1} = \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix}$$

Hill Cipher Decryption

Inverse Key Matrix = $\begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix}$ Ciphertext $\begin{pmatrix} E \\ L \end{pmatrix}\begin{pmatrix} S \\ C \end{pmatrix} = \begin{pmatrix} 4 \\ 11 \end{pmatrix}\begin{pmatrix} 18 \\ 2 \end{pmatrix}$

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

$\begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix}\begin{pmatrix} 4 \\ 11 \end{pmatrix}$

$25 \times 4 + 22 \times 11 = 342$

$1 \times 4 + 23 \times 11 = 257$

$\begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix}\begin{pmatrix} 4 \\ 11 \end{pmatrix} = \begin{pmatrix} 342 \\ 257 \end{pmatrix}$

$\begin{pmatrix} 342 \\ 257 \end{pmatrix} = \begin{pmatrix} 4 \\ 23 \end{pmatrix} \bmod 26 = \begin{pmatrix} E \\ X \end{pmatrix}$

$\begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix}\begin{pmatrix} 18 \\ 2 \end{pmatrix}$

$25 \times 18 + 22 \times 2 = 494$

$1 \times 18 + 23 \times 2 = 64$

$\begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix}\begin{pmatrix} 18 \\ 2 \end{pmatrix} = \begin{pmatrix} 494 \\ 64 \end{pmatrix}$

$\begin{pmatrix} 494 \\ 64 \end{pmatrix} = \begin{pmatrix} 0 \\ 12 \end{pmatrix} \bmod 26 = \begin{pmatrix} A \\ M \end{pmatrix}$

Plaintext = “EXAM”

Substitution Techniques

1) Caesar Cipher
2) Monoalphabetic Cipher
3) Playfair Cipher
4) Hill Cipher
5) **Polyalphabetic Ciphers**
6) One-Time Pad

5) Polyalphabetic Cipher

- Monoalphabetic cipher encoded using only one fixed alphabet
- **Polyalphabetic cipher** is a substitution cipher in which the cipher alphabet for the plain alphabet may be different at different places during the encryption process.
  1. **Vigenere cipher**
  2. **Vernam cipher**

Vigenere Cipher

Keyword : **DECEPTIVE**

Key : **DECEPTIVE**

Plaintext : **WEAREDISCOVEREDSAVEYOURSELF**

Ciphertext : **ZICVTWQNGRZGVTWAVZHCQYGLMGJ**

$$C = (P_1 + K_1, P_2 + K_2, \ldots P_m + K_m) \bmod 26$$

$$P = (C_1 - K_1, C_2 - K_2, \ldots C_m - K_m) \bmod 26$$

An analyst looking at only the ciphertext would detect the repeated sequences VTW at a displacement of 9 and make the assumption that the keyword is either three or nine letters in length.

Keyword : **DECEPTIVE**

Key : **DECEPTIVE**

Plaintext : **WEAREDISCOVEREDSAVEYOURSELF**

This system is referred as an **autokey system**

Plaintext

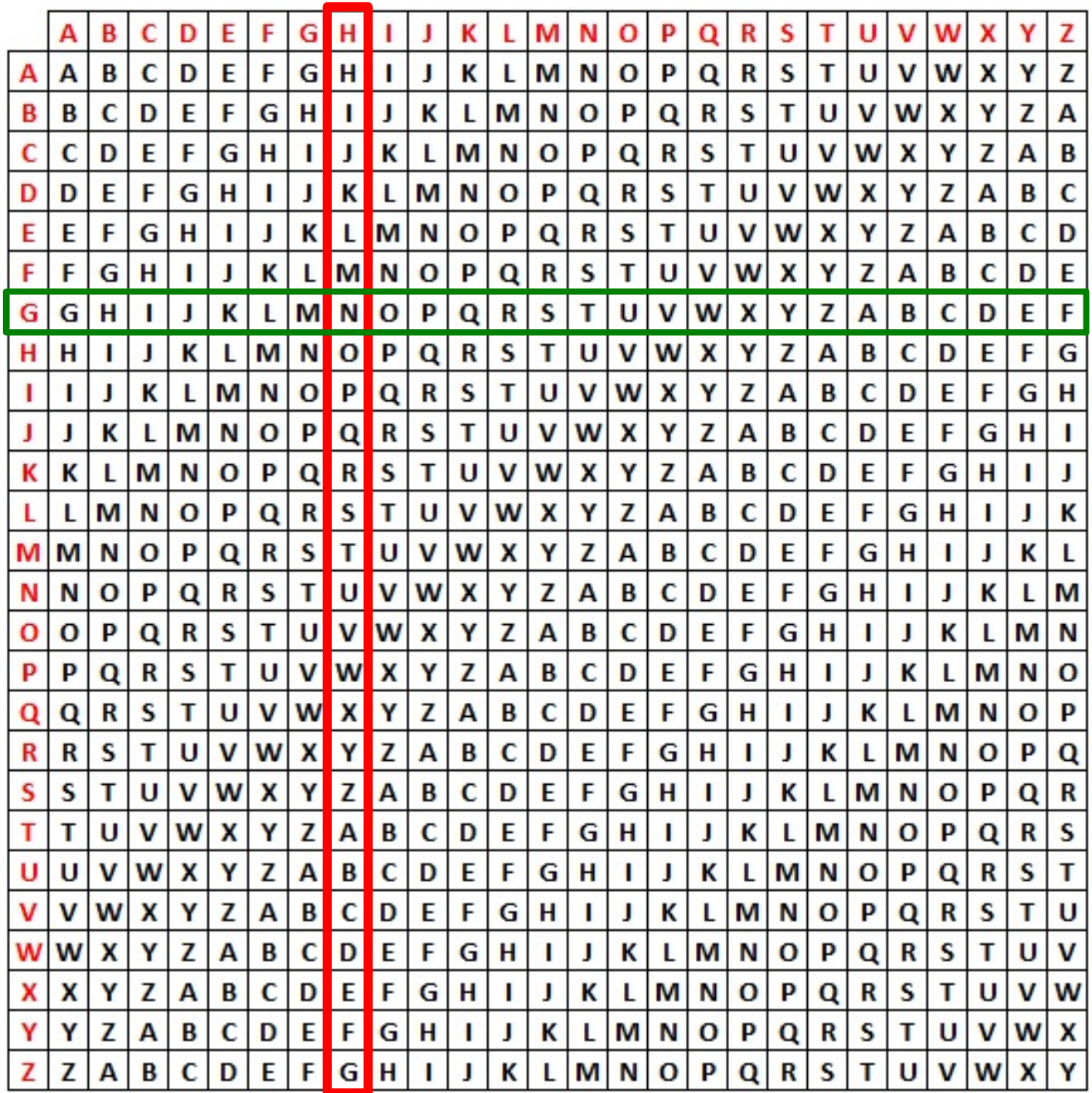
Key

KEY = **GM**

PT = **HELLO**

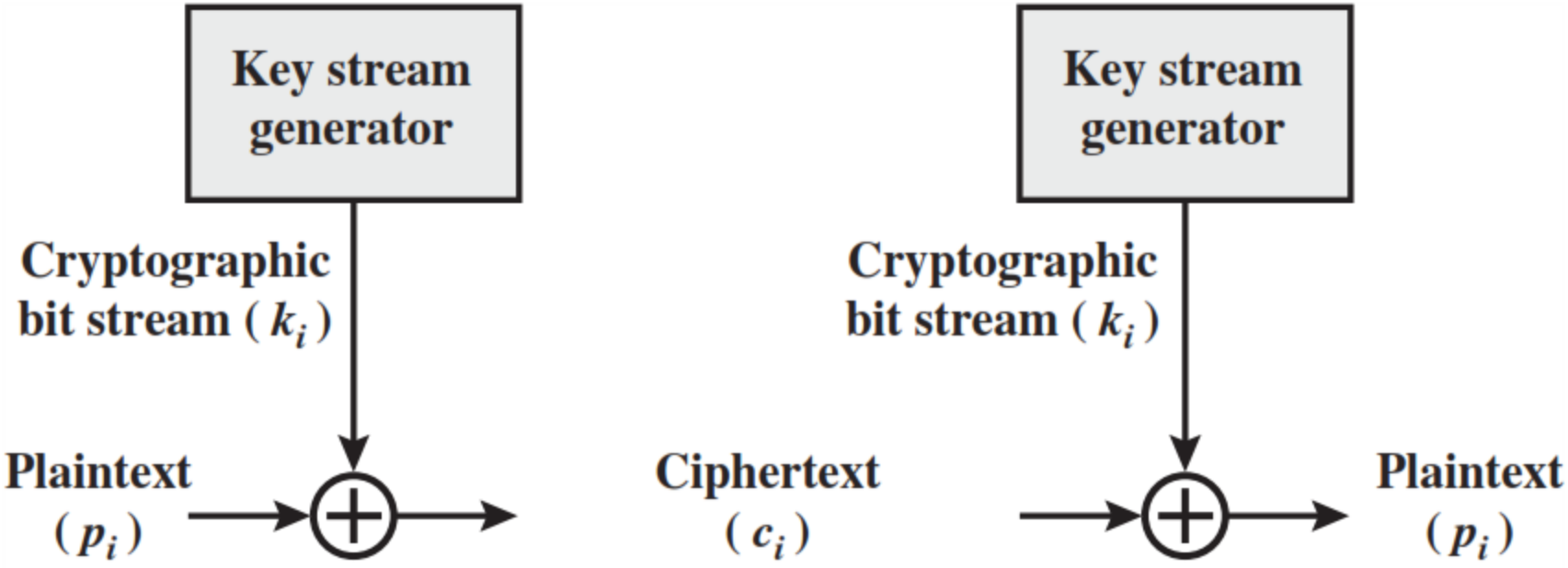
Autokey= GMGMG

CT = **NQRXU**



Vernam Cipher

- The ciphertext is generated by applying the logical XOR operation to the individual bits of plaintext and the key stream.
- The key can be shorter than the message and repeated, which makes it vulnerable to certain types of attacks.



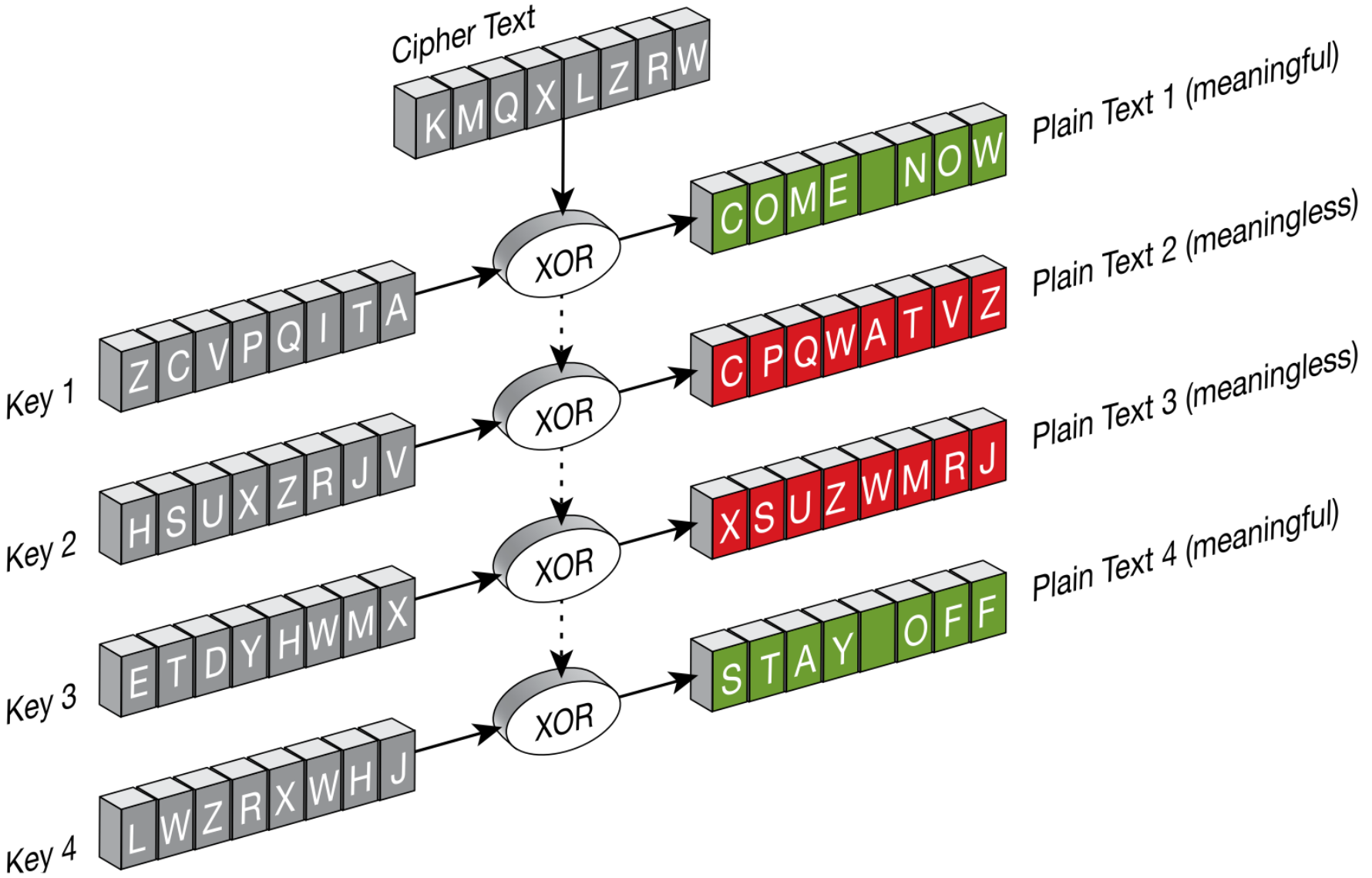
Substitution Techniques

1) Caesar Cipher
2) Monoalphabetic Cipher
3) Playfair Cipher
4) Hill Cipher
5) Polyalphabetic Ciphers
6) **One-Time Pad**

One time pad

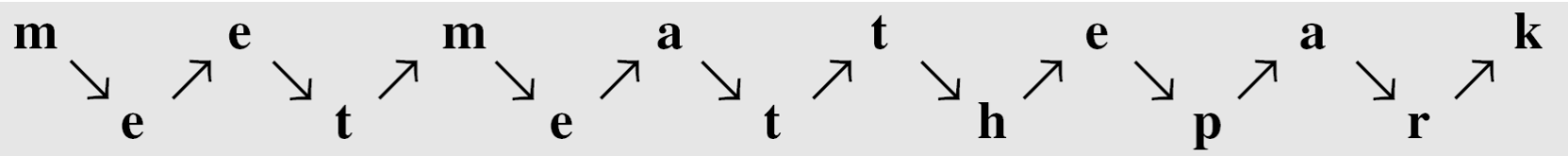
- The one-time pad is an extension of the Vernam cipher, which is a provably secure cryptosystem, was developed by Gilbert Vernam in 1918.
- The message is represented as a binary string (a sequence of 0's and 1's using a coding mechanism such as ASCII coding.
- Uses a key that is as long as the message, completely random, and used only once. It is considered unbreakable if these conditions are met.
- **The key is a truly random sequence of 0's and 1's of the same length as the message.**

- message ='IF'
- then its ASCII code =(1001001 1000110)
- key = (1010110 0110001)
- *Encryption:*
  - 1001001 1000110 plaintext
  - 1010110 0110001 key
  - 0011111 1110110 ciphertext


Cipher Text
K M Q X L Z R W
Key 1
Z C V P Q I T A
Key 2
H S U X Z R J V
Key 3
E T D Y H W M X
Key 4
L W Z R X W H J
XOR
XOR
XOR
XOR
C O M E N O W
C P Q W A T V Z
X S U Z W M R J
S T A Y O F F
Plain Text 1 (meaningful)
Plain Text 2 (meaningless)
Plain Text 3 (meaningless)
Plain Text 4 (meaningful)

Transposition Techniques

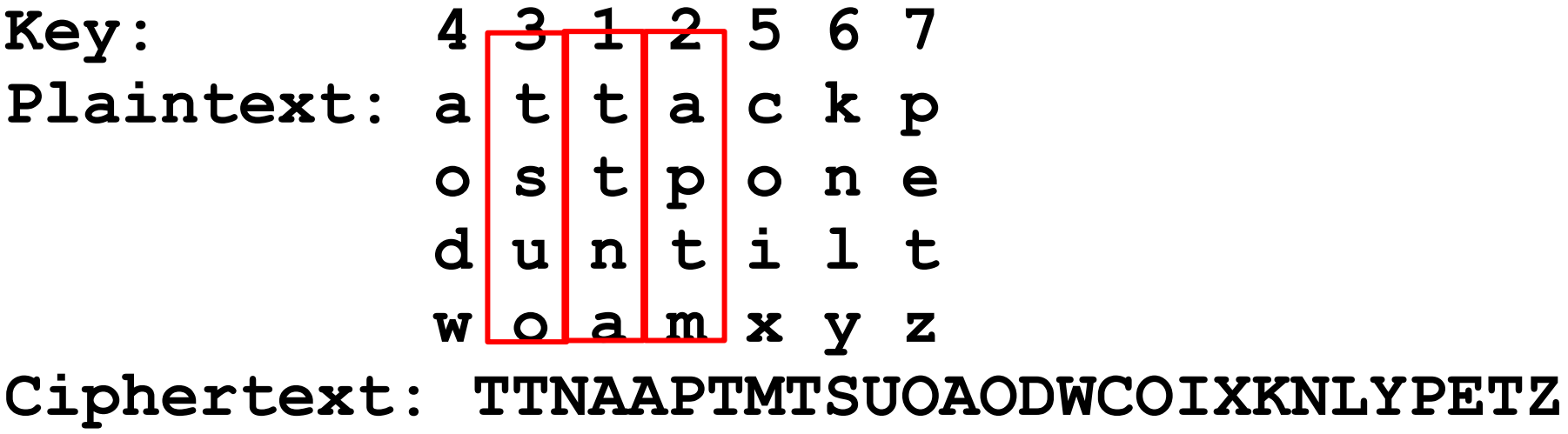
- A transposition cipher does not substitute one symbol for another, instead it changes the location of the symbols.
- The simplest such cipher is the **rail fence technique**, in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.
- For example, to send the message **"Meet me at the park"** to Bob, Alice writes



- She then creates the ciphertext "MEMATEAKETETHPR".

...Transposition Techniques

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

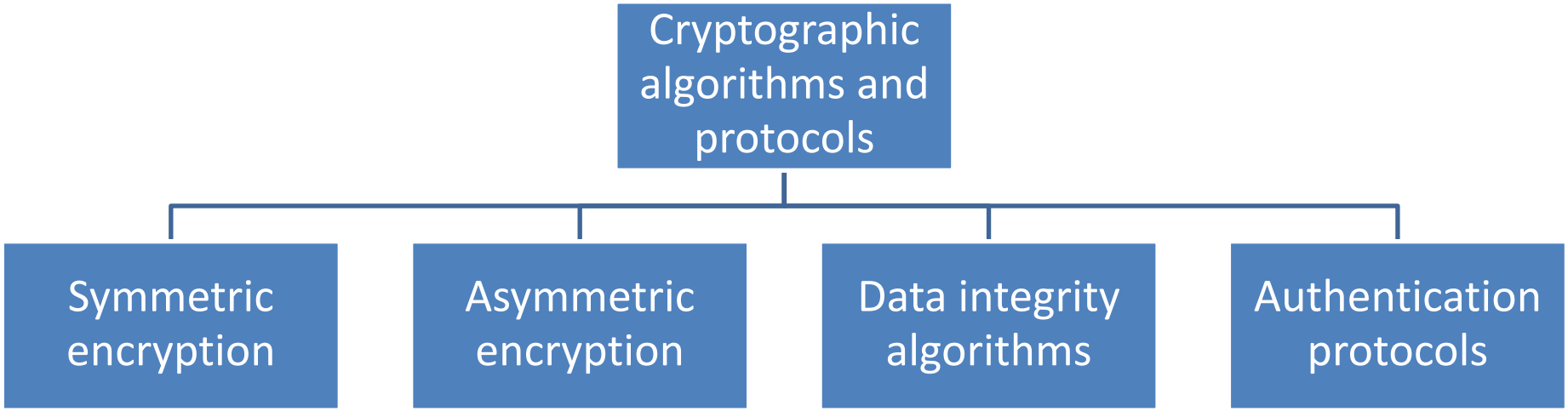


Cryptography and Cryptanalysis

- **Cryptography and Cryptanalysis**
  - **Cryptography** is the study of the design of techniques for ensuring the secrecy and/or authenticity of information
  - **Cryptanalysis** deals with the defeating such techniques to recover information, or forging information that will be accepted as authentic

Cryptographic Algorithms

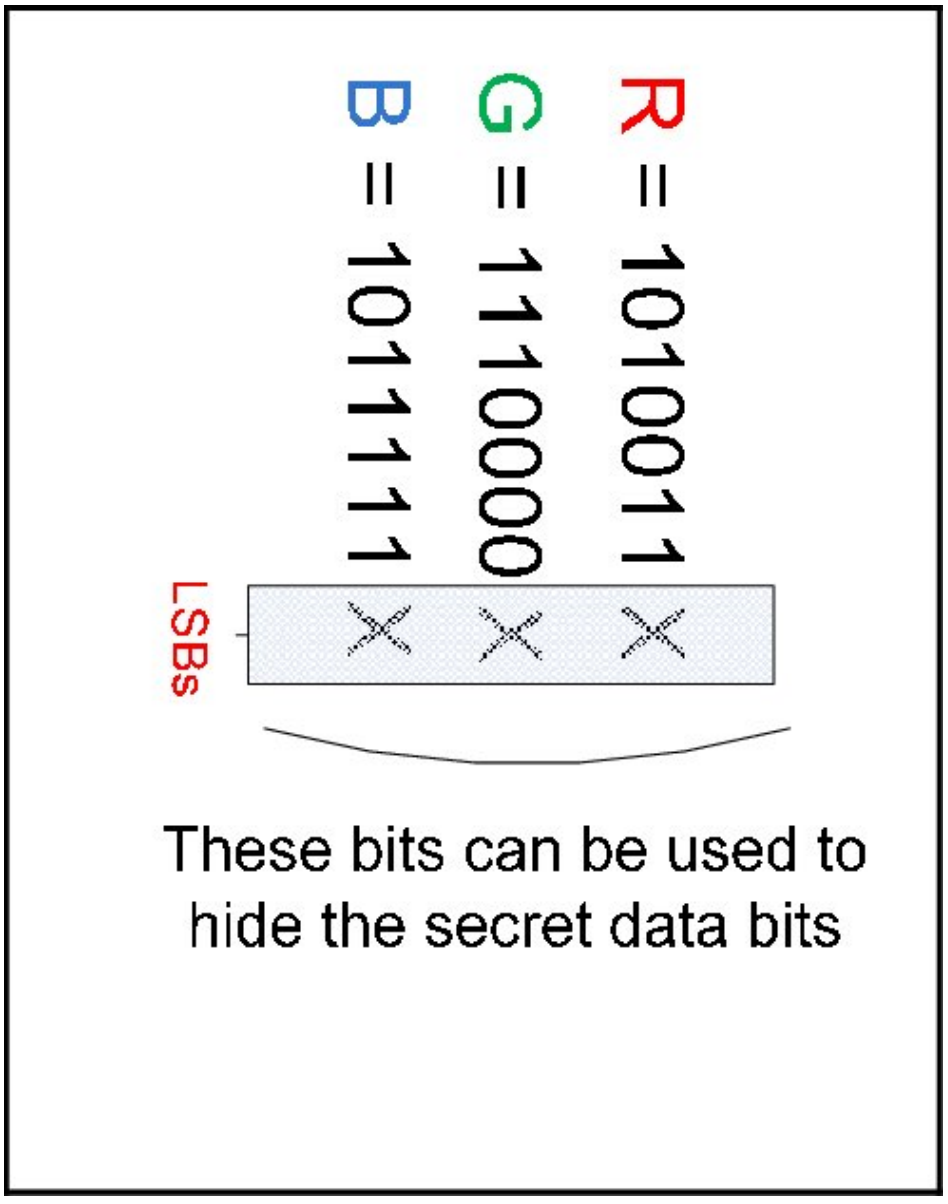
- Cryptographic algorithms and protocols can be grouped into four main areas



- Symmetric encryption algorithms are used to encrypt the bulk of data, such as stream ciphers and block ciphers
- Asymmetric encryption algorithms are used for digital signatures, key exchange, and encryption of small blocks of data, such as secret keys and passwords
- Data integrity algorithms are used to protect the integrity of data, such as message authentication codes and hash functions
- Authentication protocols are used to prove the identity of entities, such as users or devices

Steganography

- an alternative to encryption
- hides existence of message
  - using only a subset of letters/words in a longer message marked in some way
  - using invisible ink
  - hiding in LSB in graphic image or sound file
- Drawback: high overhead to hide relatively few info bits
- Advantage: can obscure encryption use


R = 10100111
G = 11100000
B = 10111111
LSBs
These bits can be used to hide the secret data bits

Demo

- https://stylesuxx.github.io/steganography/

Security Objectives

- Security objectives for information and computing services are Confidentiality, Integrity, Availability, Authenticity, Accountability.

1) Confidentiality:

- **Data confidentiality:** Assures that private or confidential information is not made available or disclosed to unauthorized individuals.
- **Privacy:** Assures that individuals control what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

Security Objectives (Cont…)

2) **Integrity:**
   - **Data integrity:** Assures that information and programs are changed only in a specified and authorized manner.
   - **System integrity:** Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.
3) **Availability:** Assures that systems work promptly and service is not denied to authorized users.

Security Objectives (Cont…)

4) **Authenticity:**

- The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator.
- This means verifying that each input arriving at the system came from a trusted source.

5) **Accountability:**

- The security goal is to make sure that any actions taken by a person or system can be tracked back to that specific person or system.
- This supports nonrepudiation, restriction, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.

Threat and Attack

- **Threat:** A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could crack security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.
- **Attack:** An violation on system security that derives from an intelligent threat; that is, an intelligent act that is a calculated attempt to avoid security services and violate the security policy of a system.