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

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 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 that generates the requirement for actions of an entity to be traced uniquely to that entity.
   - This supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.

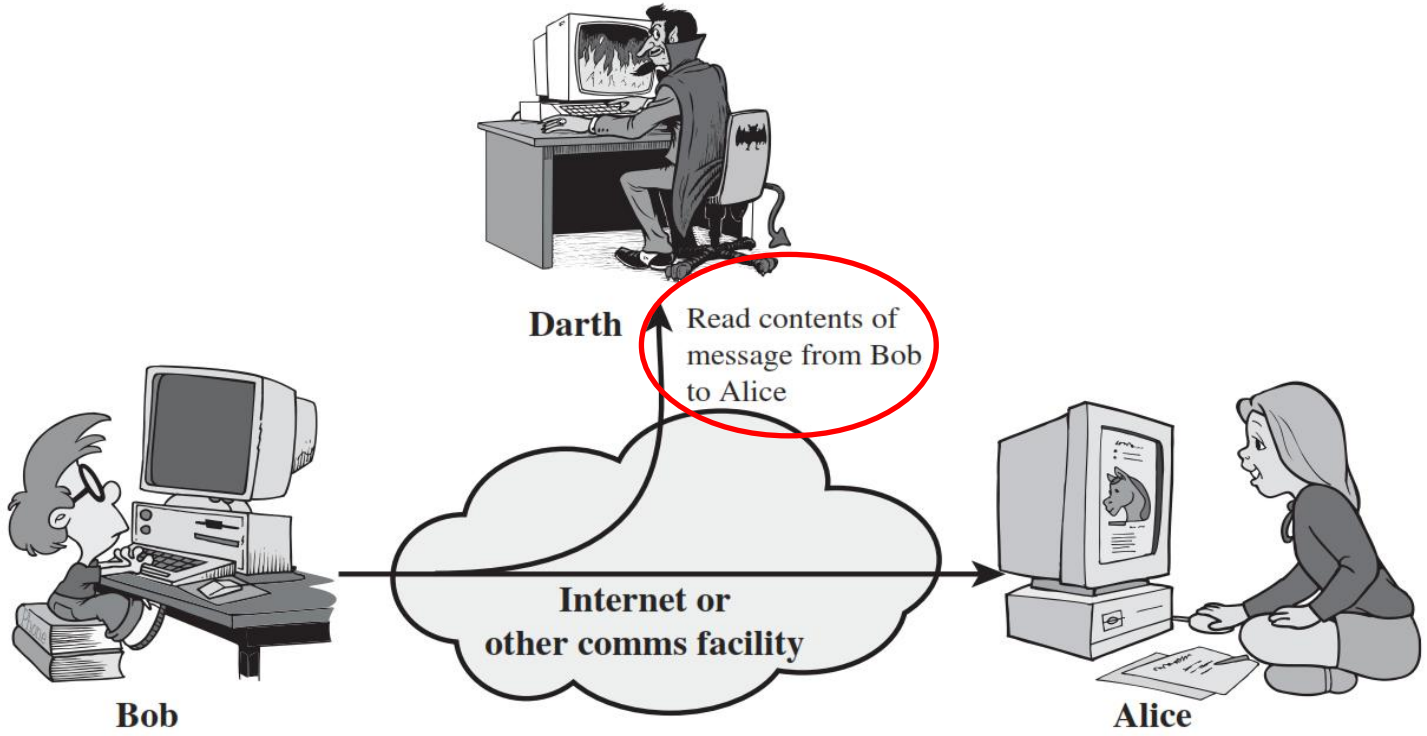
Threat and Attack

- **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.

Security Attacks

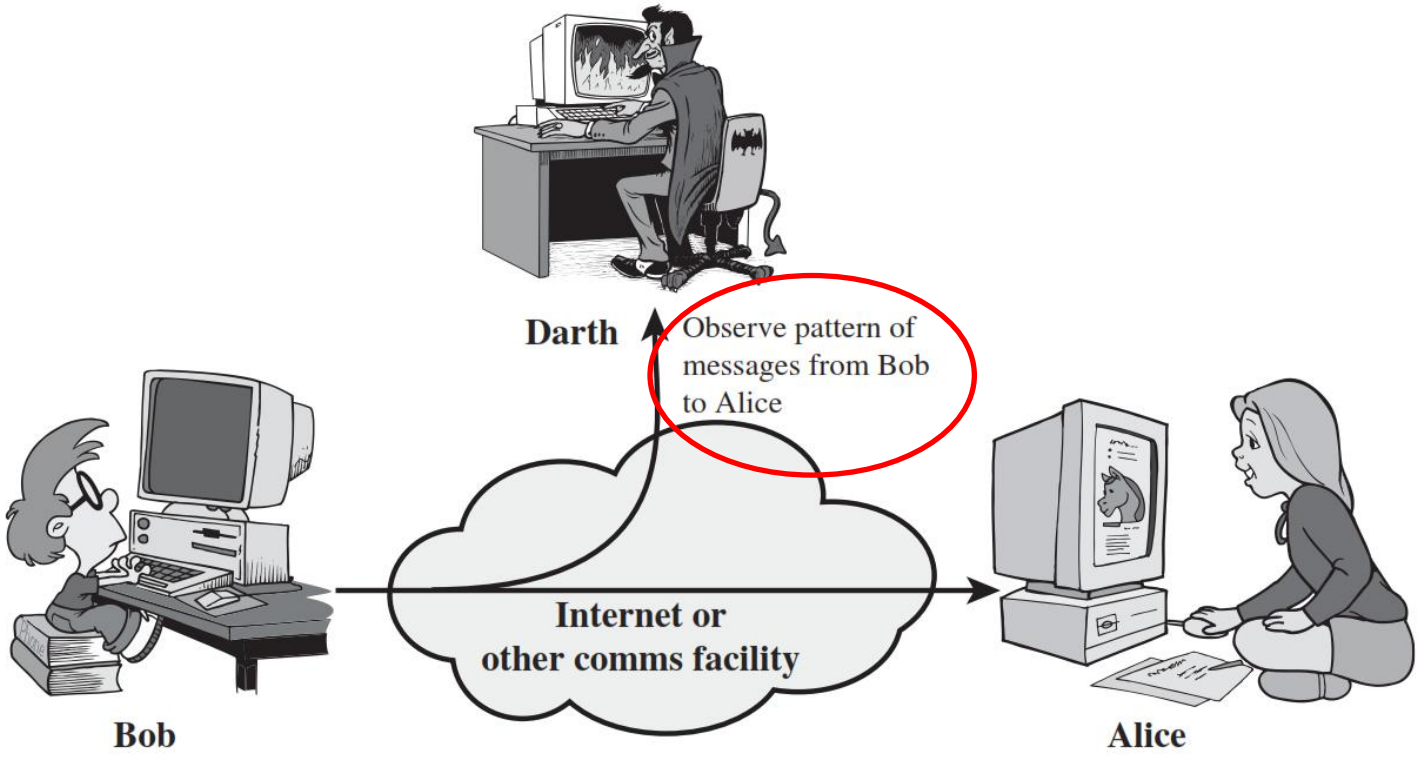
- A **passive attack** attempts to learn or make use of information from the system but does not affect system resources.
  1. Release of message contents
  2. Traffic analysis
- An **active attack** attempts to alter system resources or affect their operation.
  1. Masquerade
  2. Replay
  3. Modification of messages
  4. Denial of service.

1) Release of message contents (Passive Attack)



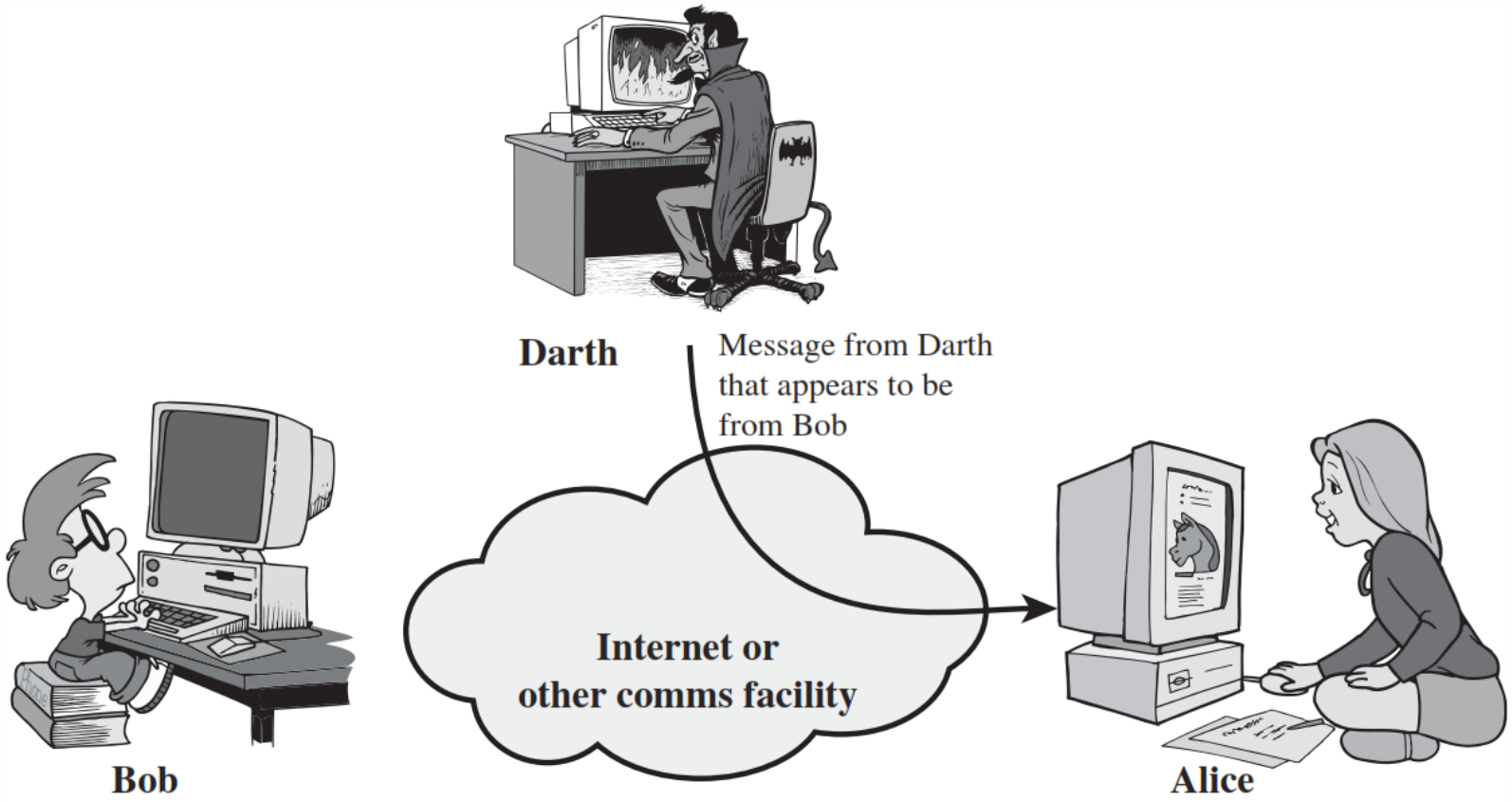
- A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information.
- We would like to prevent an opponent from learning the contents of these transmissions.

2) Traffic Analysis (Passive Attack)



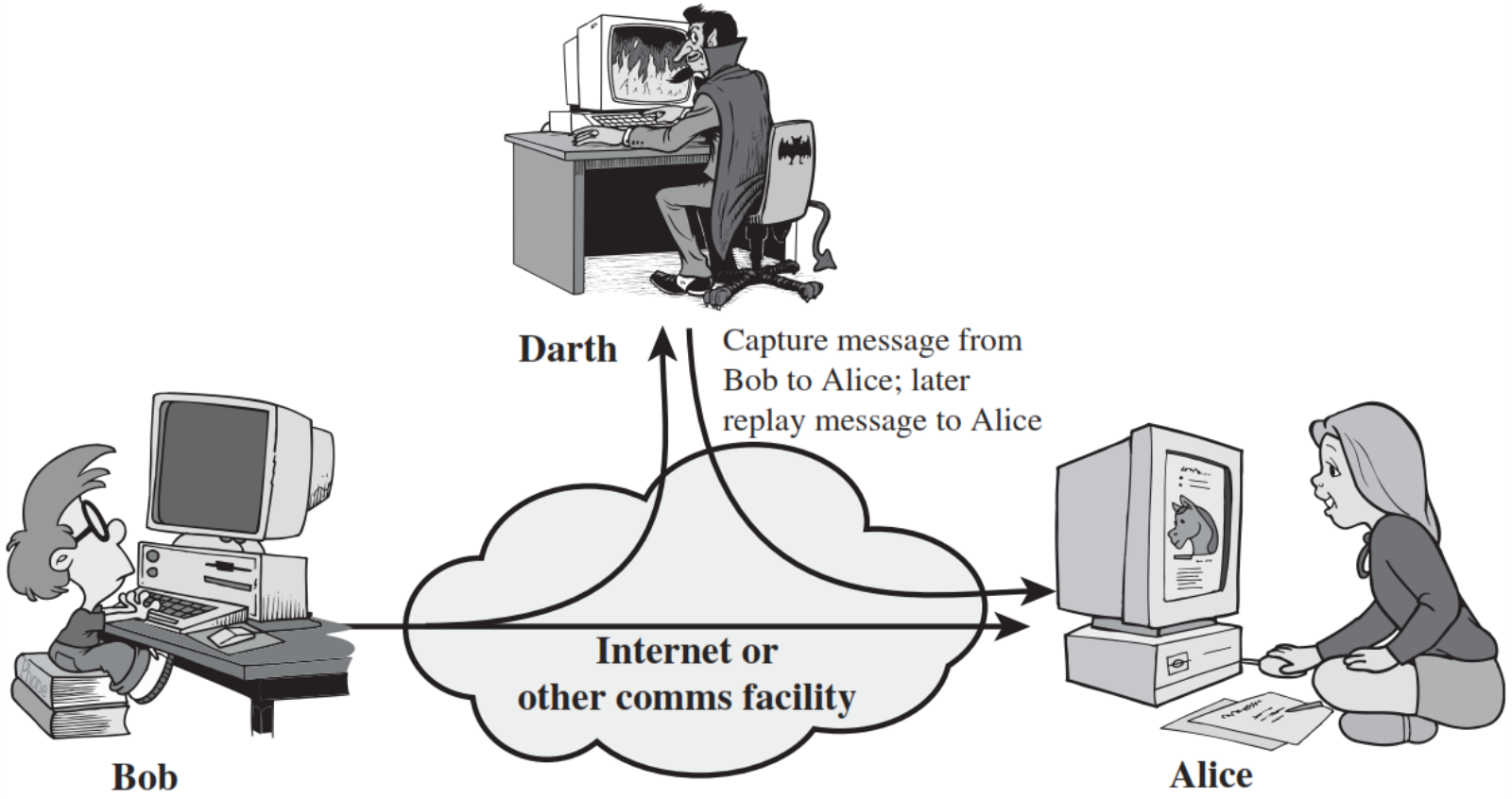
- In such attacks, an adversary, capable of observing network traffic statistics in several different networks, correlates the traffic patterns in these networks.

1) Masquerade Attack (Active Attack)



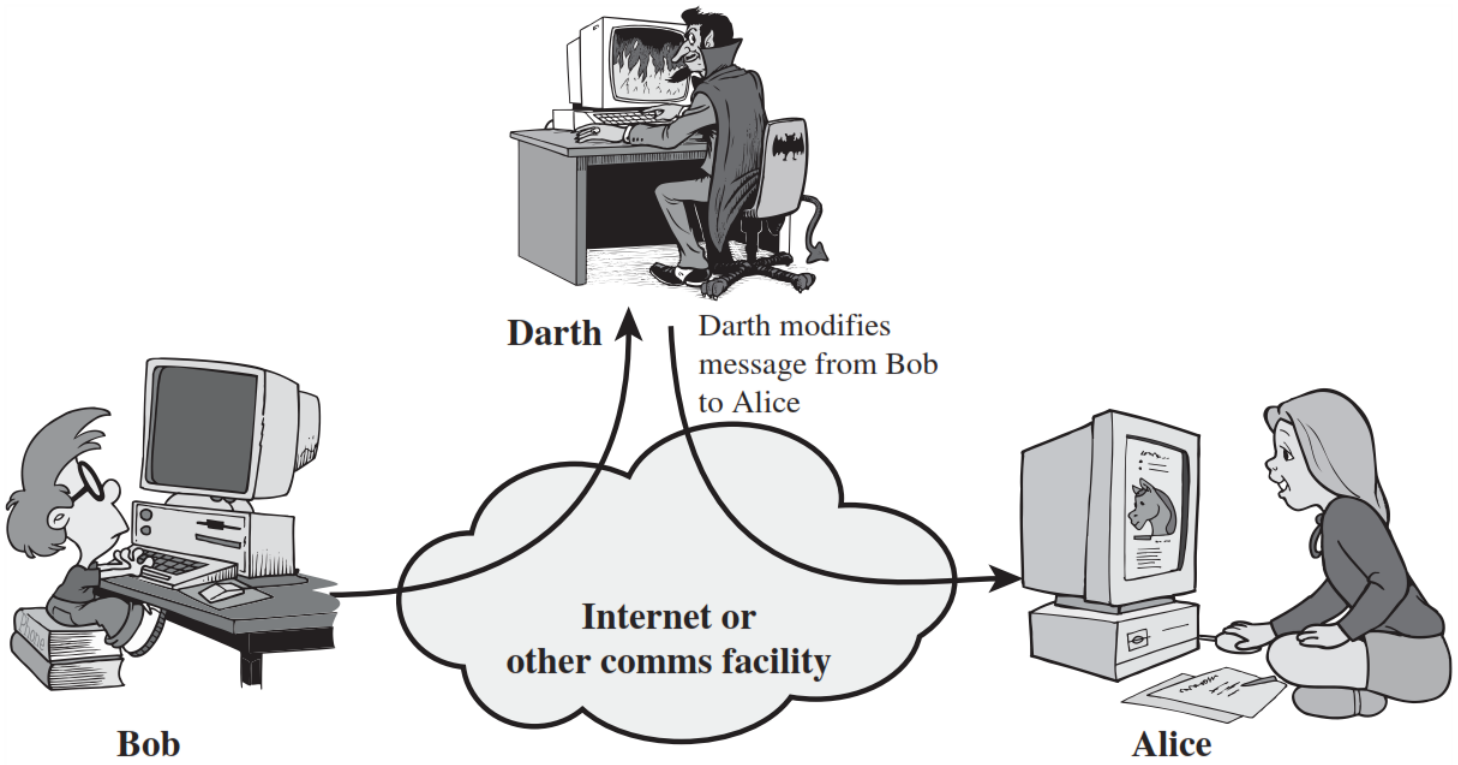
- A **masquerade** takes place when one entity pretends to be a different entity.

2) Replay Attack (Active Attack)



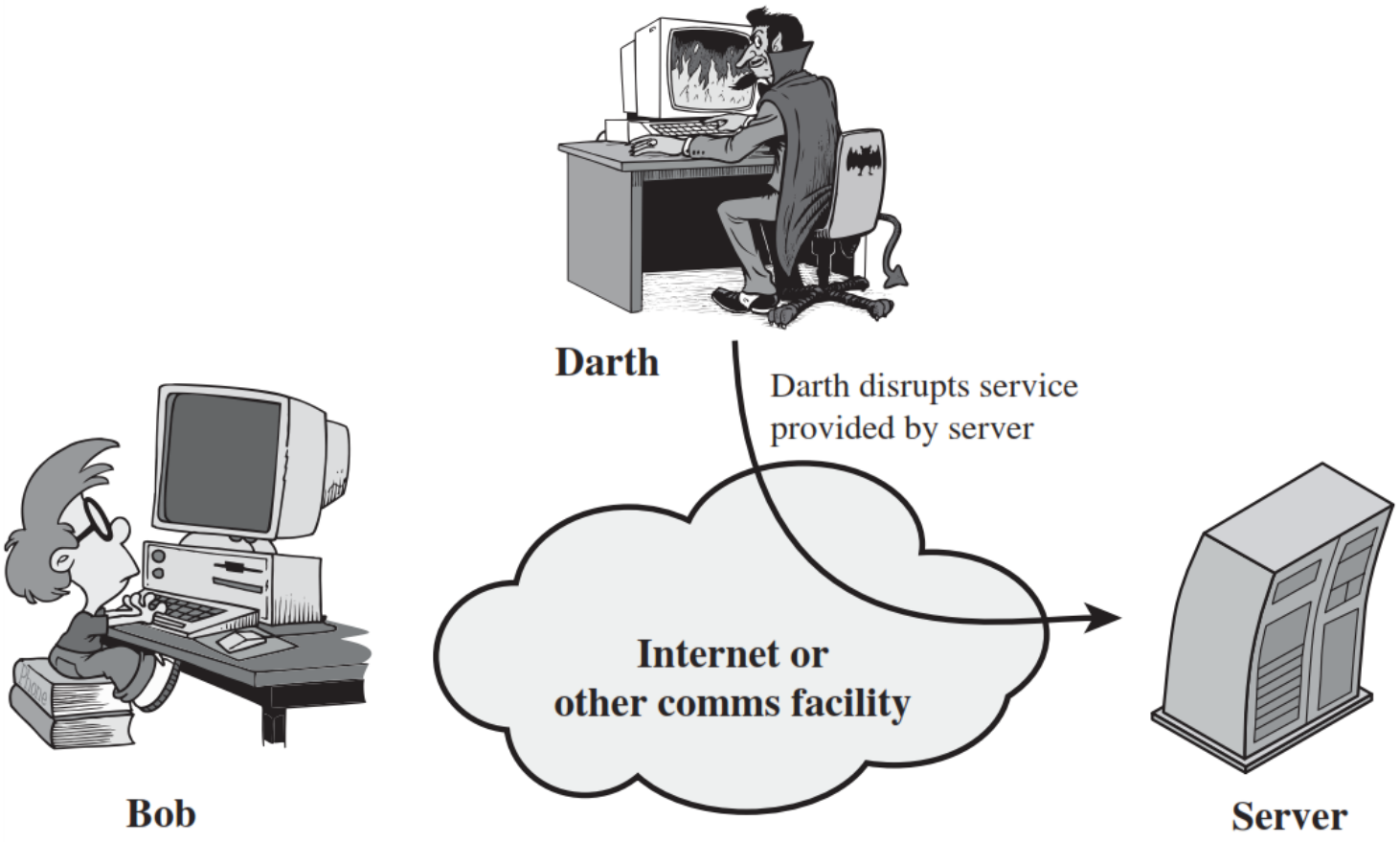
- **Replay attack** involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

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 delayed or reordered, to produce an unauthorized effect.

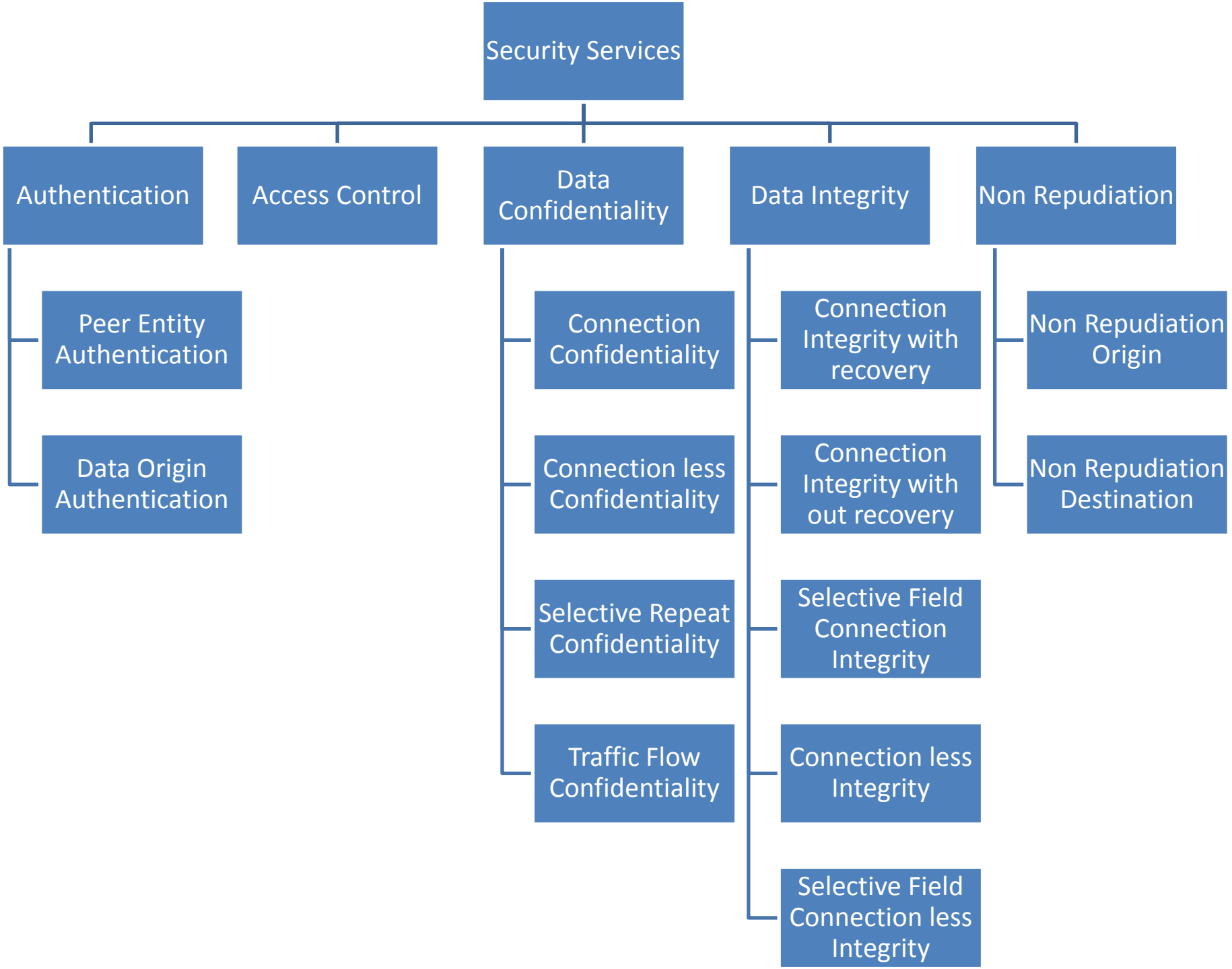
4) Denial of Service Attack (Active Attack)



- **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 that is provided by a protocol layer of communicating open systems and that ensures security of the systems or of data transfers.


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
Connection Integrity with out recovery
Selective Field Connection Integrity
Connection less Integrity
Selective Field Connection less 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:** Used in association with a logical connection to provide confidence in the identity of the entities connected.
2. **Data-Origin Authentication:** In a connectionless transfer, provides assurance that the source of received data is as claimed.

Who you are ?
(biometrics)

Physical authentication
where you are ?

What you know ?

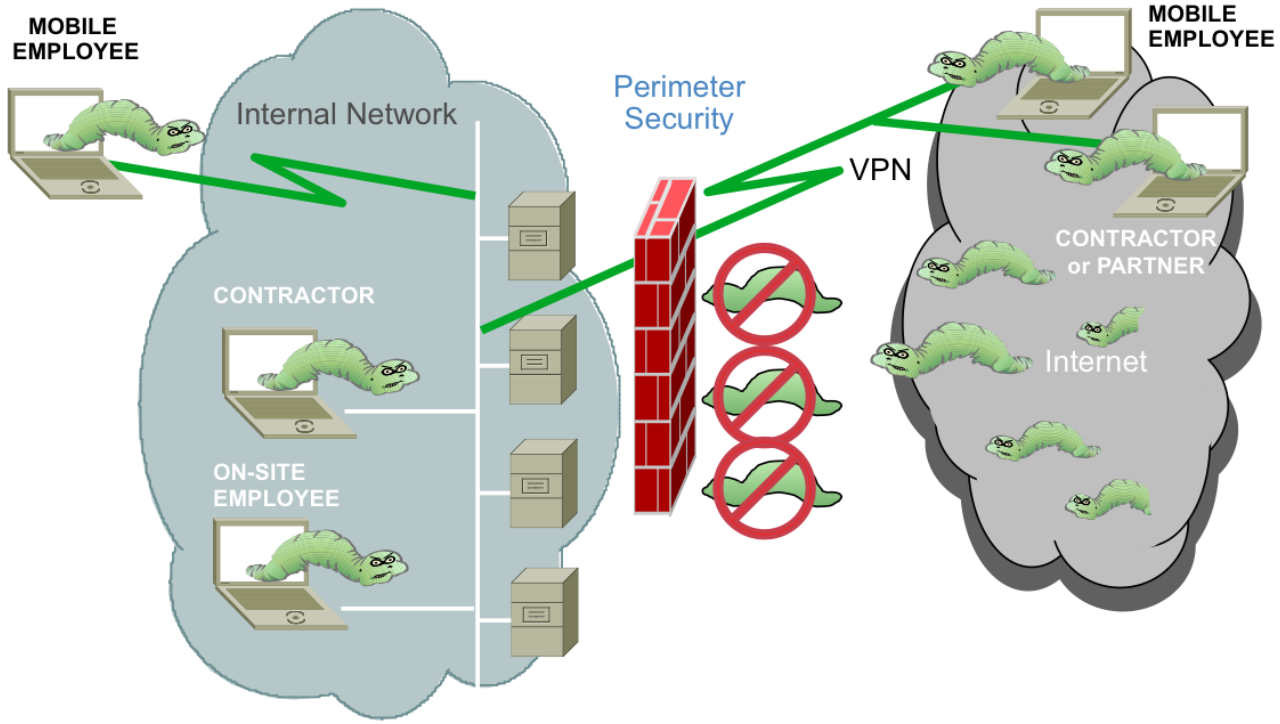
Password

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 those accessing the resource are allowed to do).



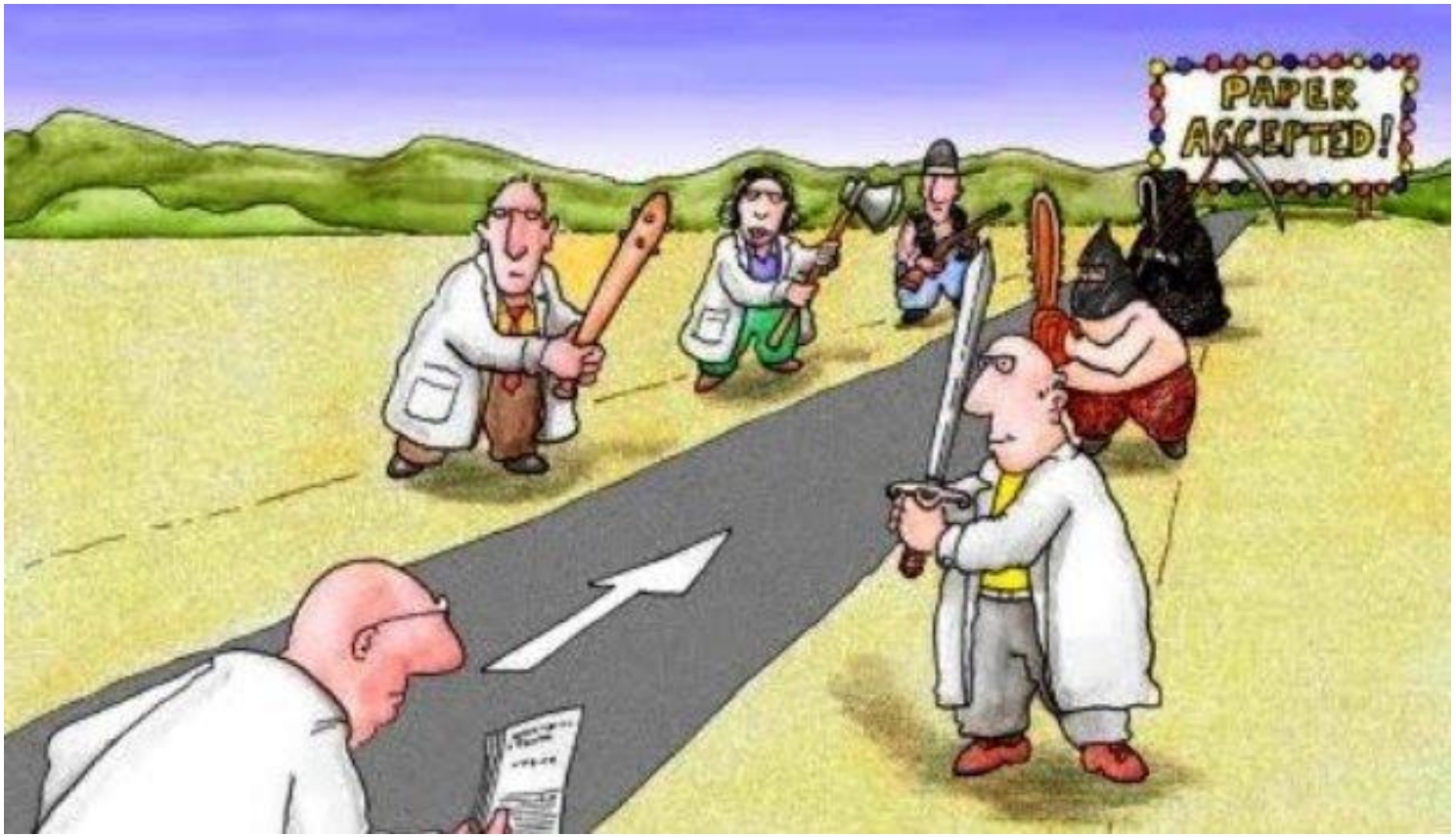
Data Confidentiality

- **Data confidentiality** is the protection of data from unauthorized disclosure.

1. **Connection Confidentiality:** The protection of all user data on a connection.
2. **Connectionless Confidentiality:** The protection of all user data in a single data block.
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 traffic flows.

Data Integrity

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



Data Integrity (Cont…)

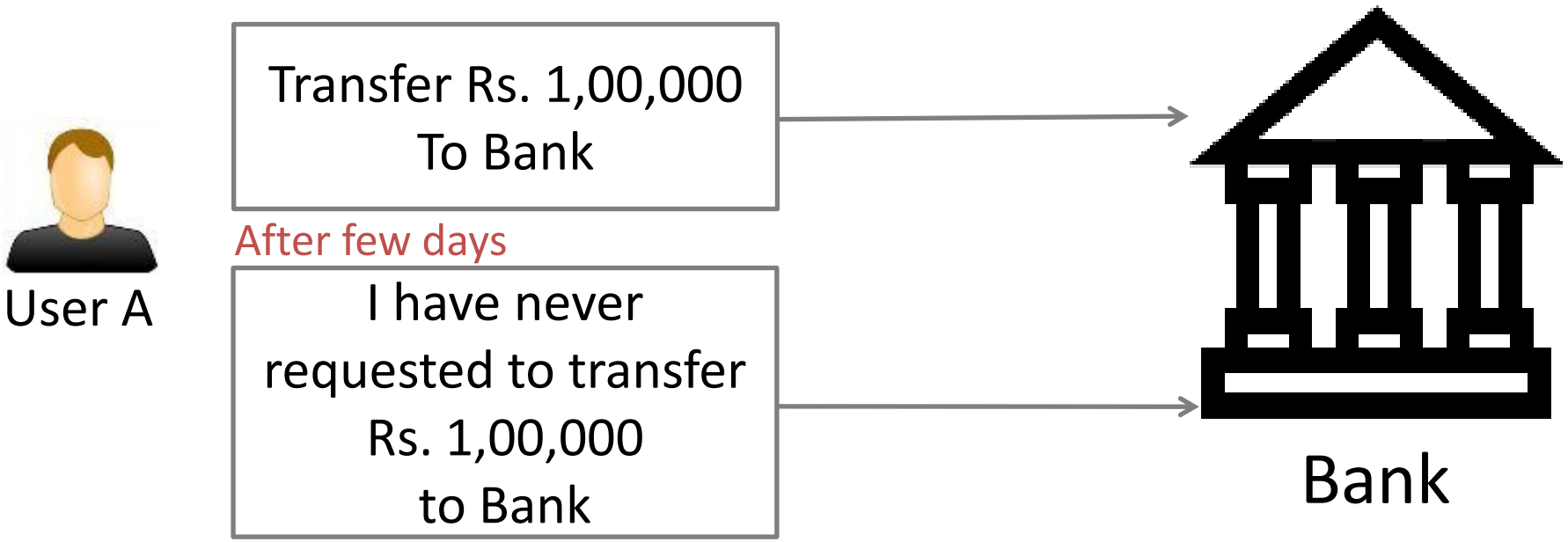
- **Connection Integrity with Recovery:** Provides integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data with recovery attempted.
- **Connection Integrity without Recovery:** As above, but provides only detection without recovery.
- **Selective-Field 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 take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.
- **Selective-Field Connectionless Integrity:** Provides integrity of selected fields within a single connectionless data block; takes the form of determination of 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 communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.



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)

- **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 OSI security service or protocol layer

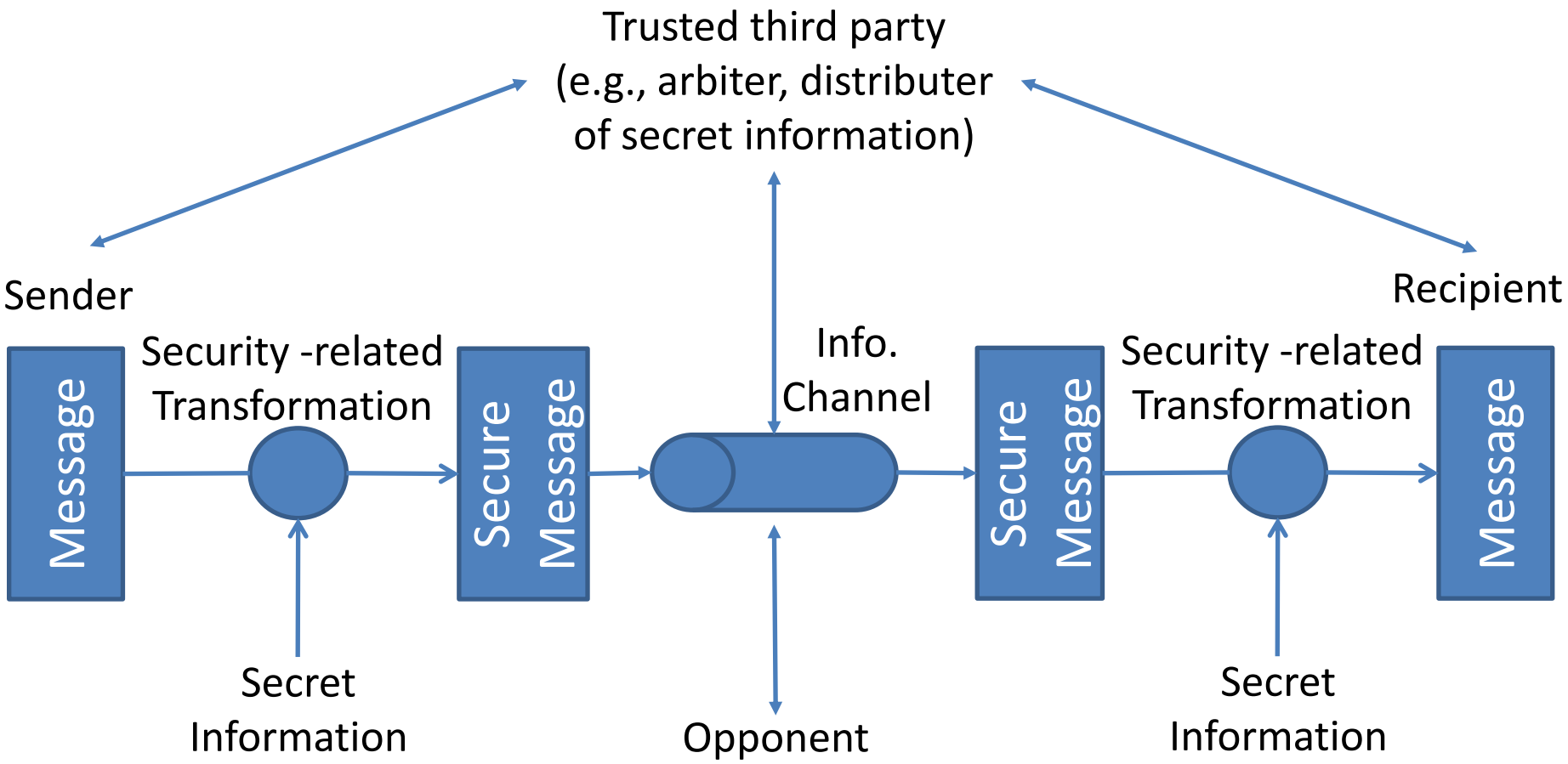
Security Mechanism (Specific Security)

- **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.

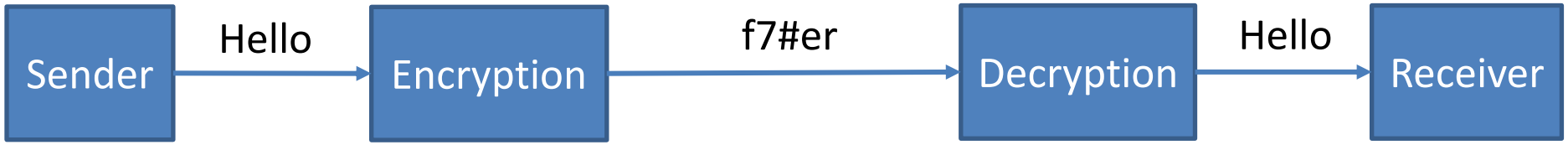
Security Mechanism (Specific security)

- **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.

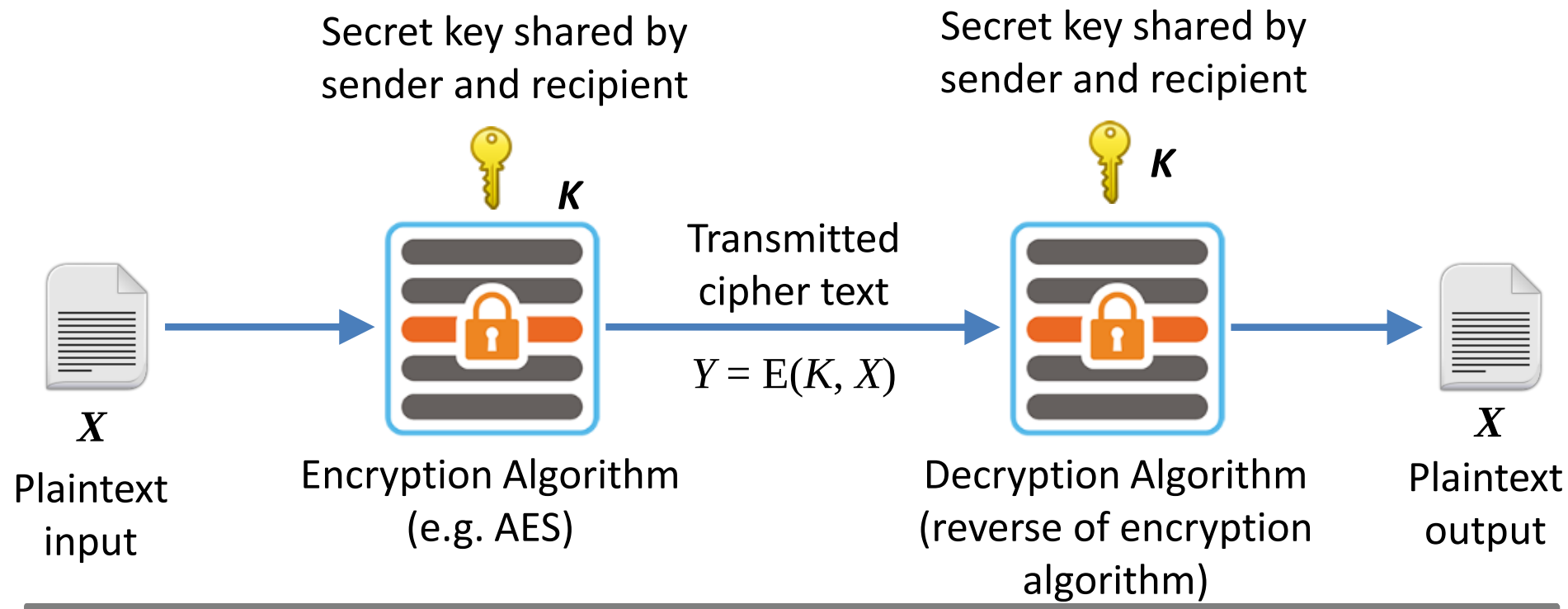
Model for Network Security



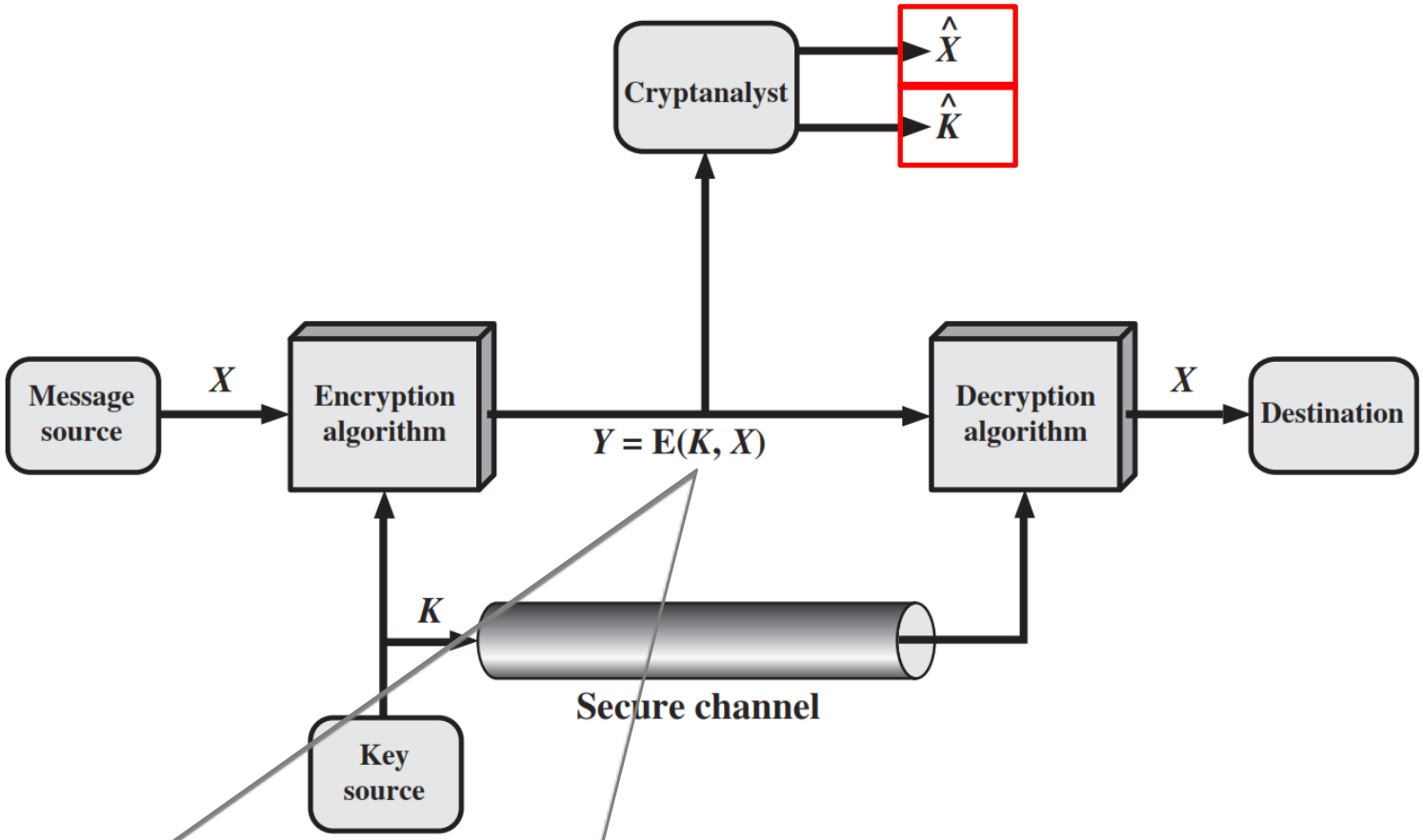
Encryption and Decryption



Symmetric Cipher Model (Conventional Encryption)



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



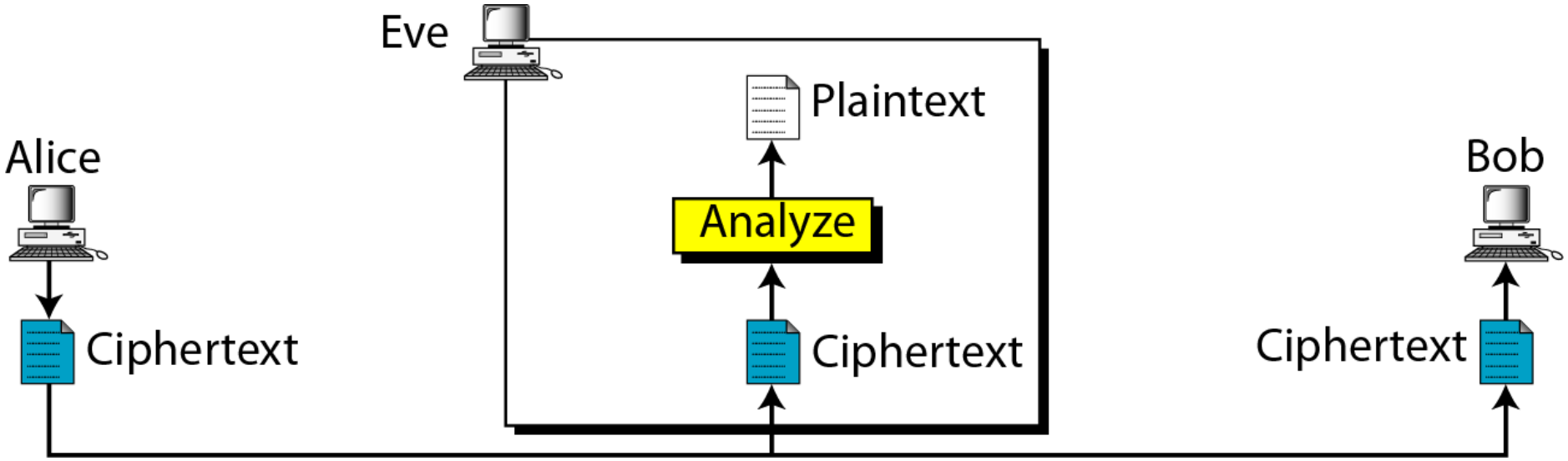
- An opponent, observing Y but not having access to K or X, may attempt to recover X or K or both X and K.
- If the opponent is interested in only this particular message, then he will focus to recover X by generating a plaintext estimate $\hat{X}$.
- Often, however, the opponent is interested in being 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:** 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 average, half of all possible keys must be tried to achieve success.

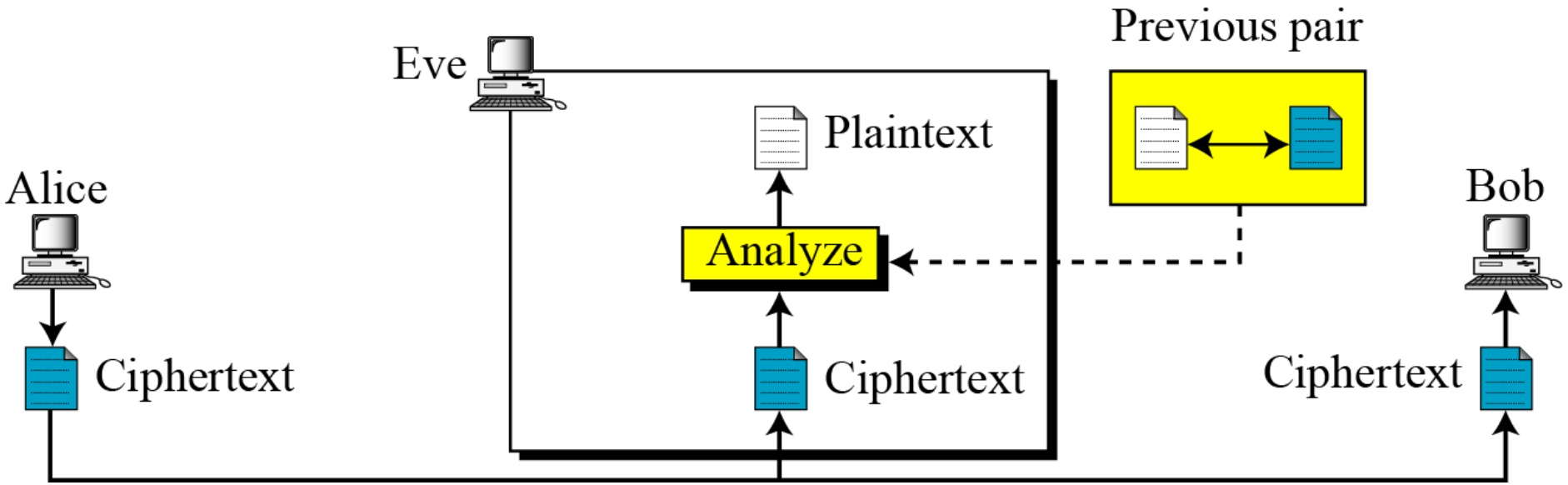
Attacks on Encrypted Messages

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



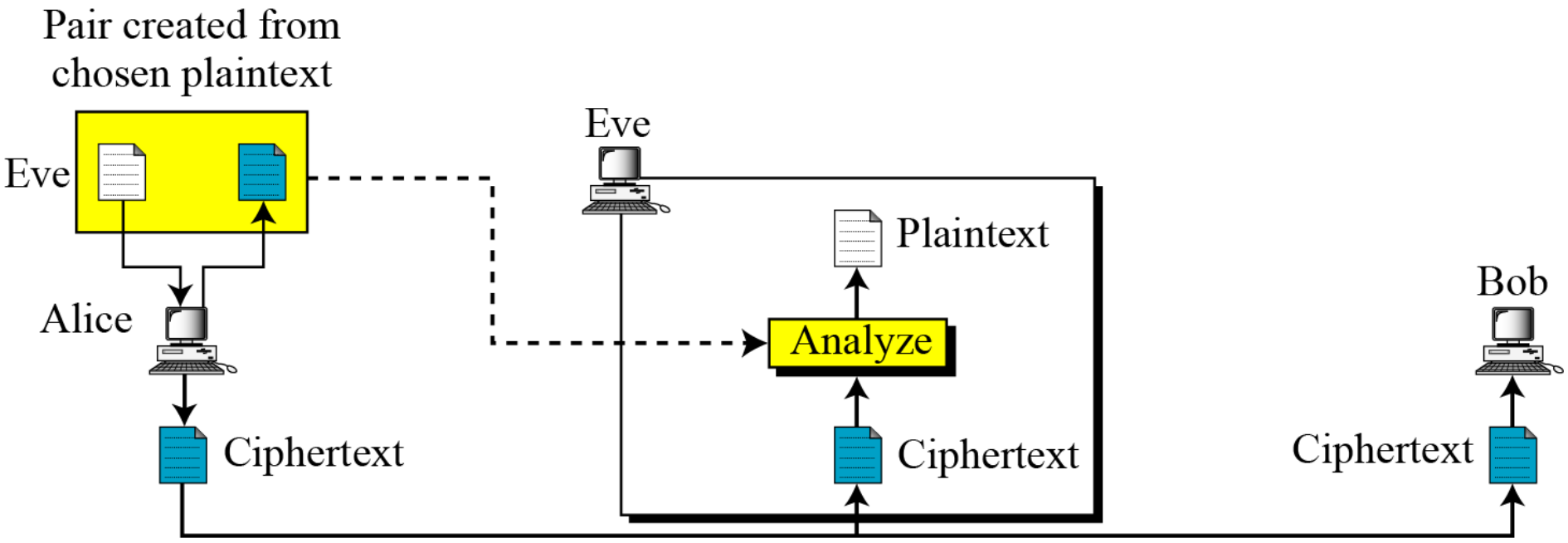
Attacks on Encrypted Messages

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



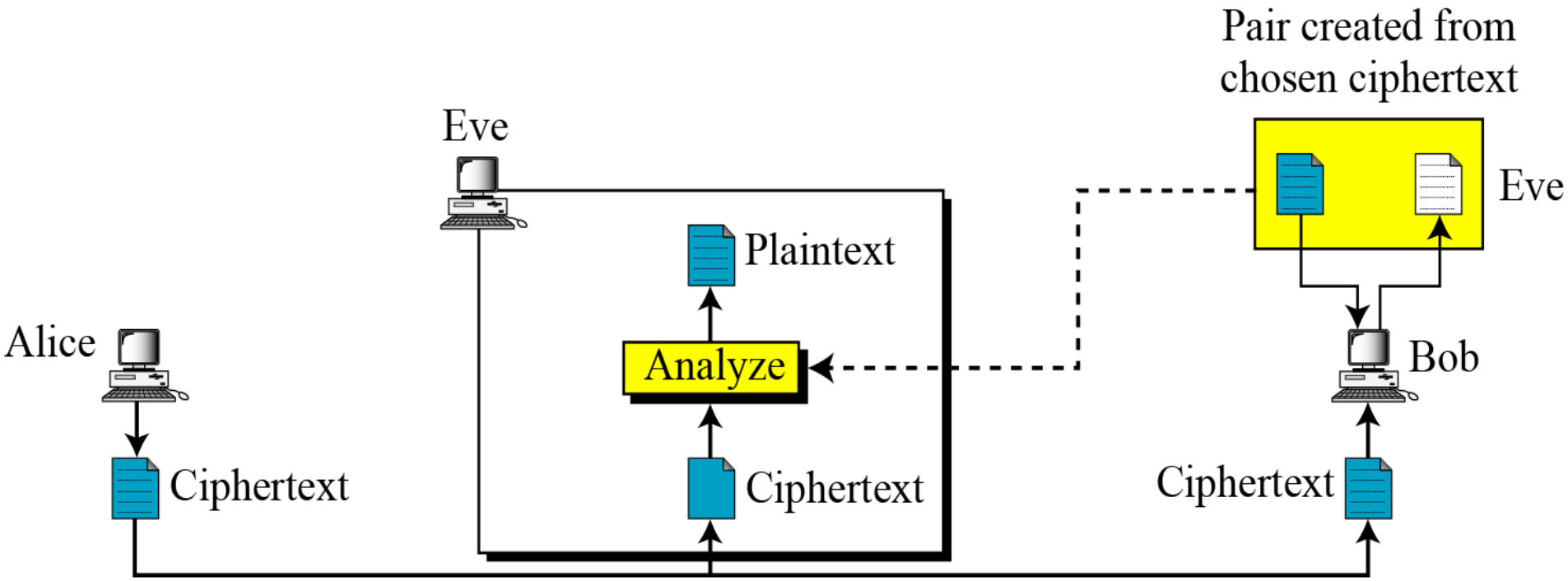
Attacks on Encrypted Messages

Type of Attack	Known to cryptanalyst
Chosen Plaintext	Encryption algorithm, Ciphertext, Plaintext message chosen by cryptanalyst



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 Techniques

- 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 three 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

- 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				

Ciphertext:

uzqsovuohxmopvgpozpevsg**zw**szopfpesxudbmetsxaizvuephzhmdzshzowsf
pappdtsvpqu**zw**ymxuzuhsxepyepopdzszufpomb**zw**pfupzhmdjudtmohmq

- 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 (Cont…)

- 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 a standard frequency distribution for English.
- If the message were long enough, this technique alone might be sufficient, but because this is a relatively short message, 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 ES

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 in the same row, replace them with the letters to their immediate right respectively, wrapping around to the left side of the row if necessary.
- If the letters appear in the same column, replace them with the letters immediately below respectively, wrapping around to the top if necessary.
- Otherwise, each letter of the pair should be replaced by the letter in the same row but in the column of the other letter of the pair.
- For example, using the table above, the letter pair **RE** would be encoded as **EO**.
- For example, using the table above, the letter pair **TA** would be encoded as **PF**.

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: $C=PK \bmod 26$

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

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

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…)

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

$$P=CK^{-1} \bmod 26$$

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

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

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

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

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

Hill Cipher Decryption

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

$P=CK^{-1} \bmod 26$

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

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

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

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

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

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

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

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

$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 0 \\ 12 \end{pmatrix} = \begin{pmatrix} 494 \\ 64 \end{pmatrix}$

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

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**

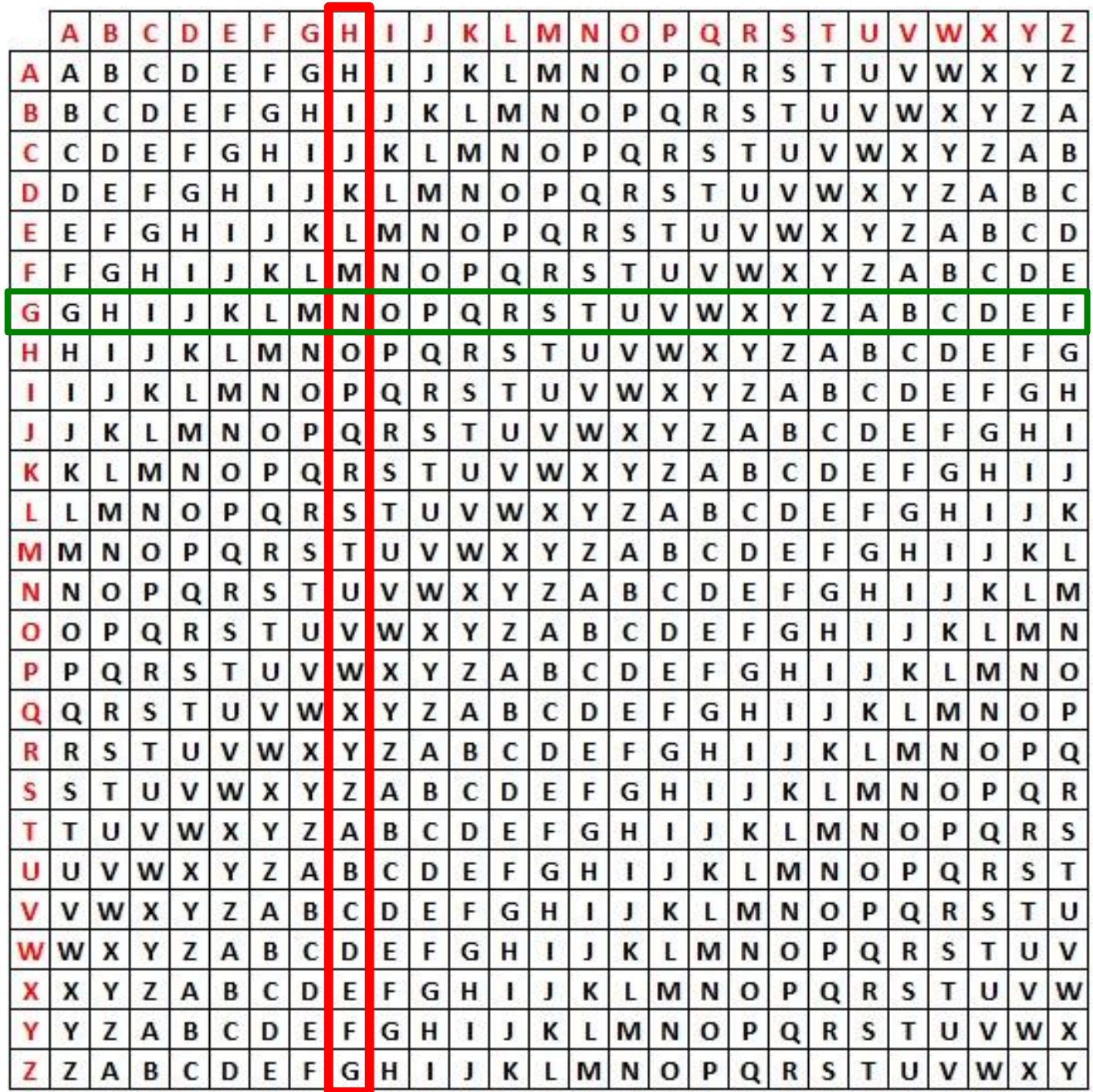
Plaintext

Key

PT = **HELLO**

KEY = **GM**

CT = **NQRXU**



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**

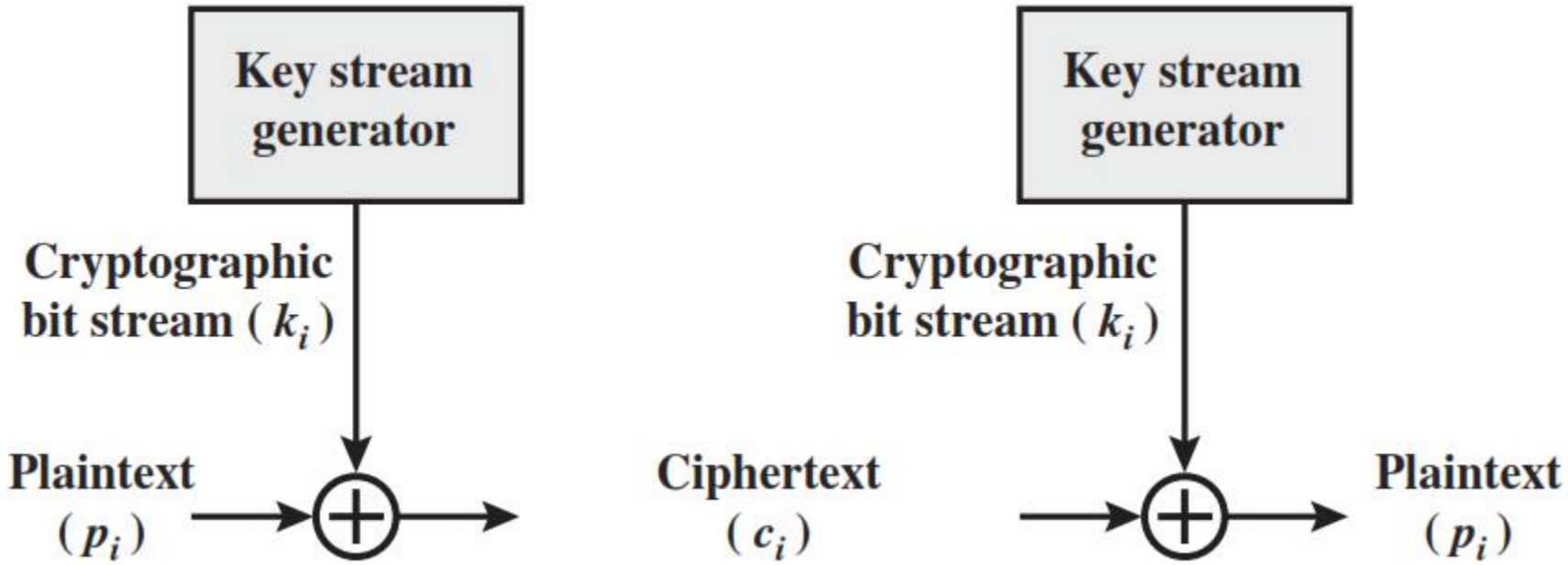
Key : **DECEPTIVE**

Plaintext : **WEAREDISCOVEREDSAVEYOURSELF**

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

Vernam Cipher

- The ciphertext is generated by applying the logical XOR operation to the individual bits of plaintext and the key stream.



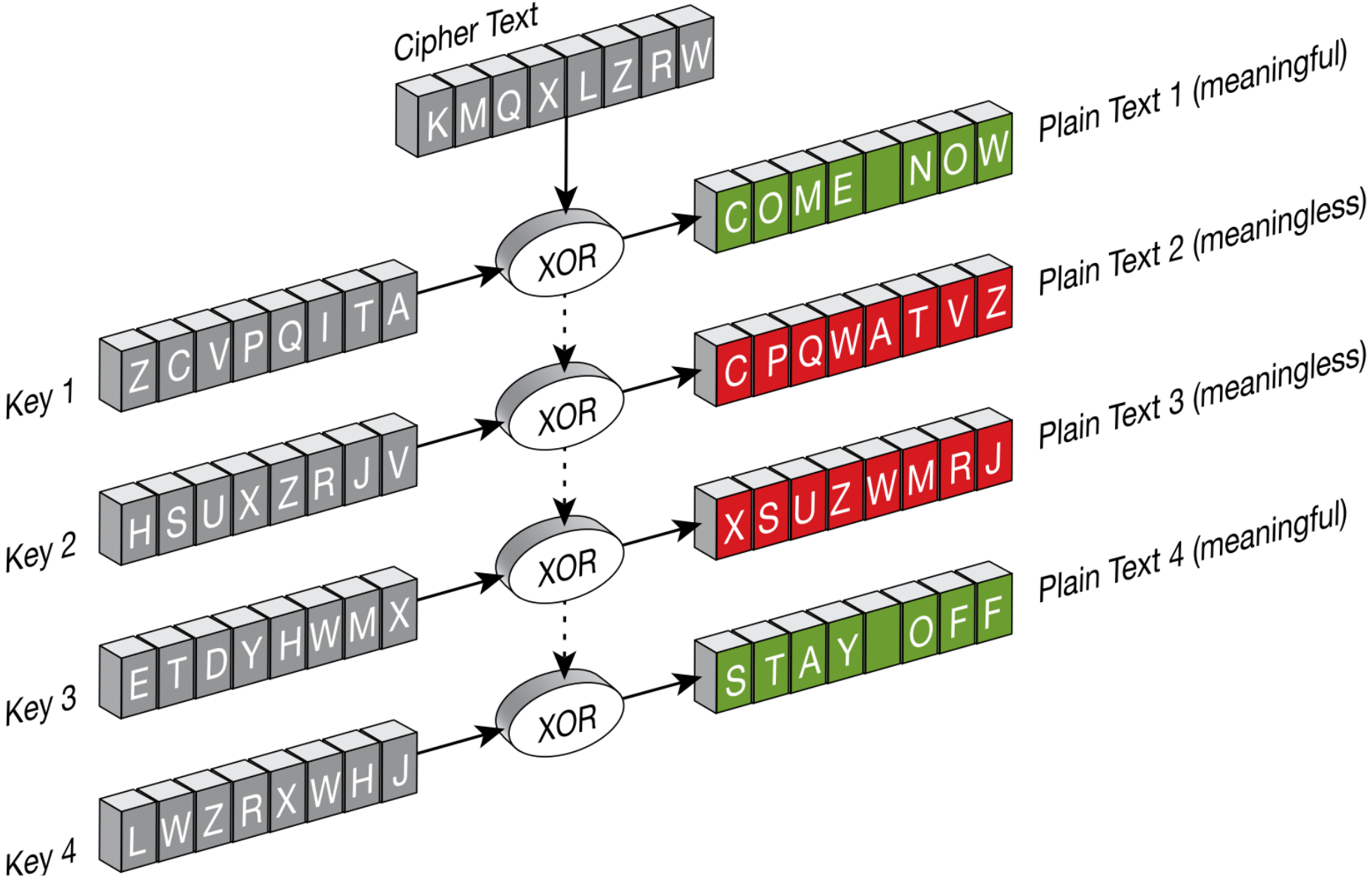
Substitution Techniques

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

One time pad

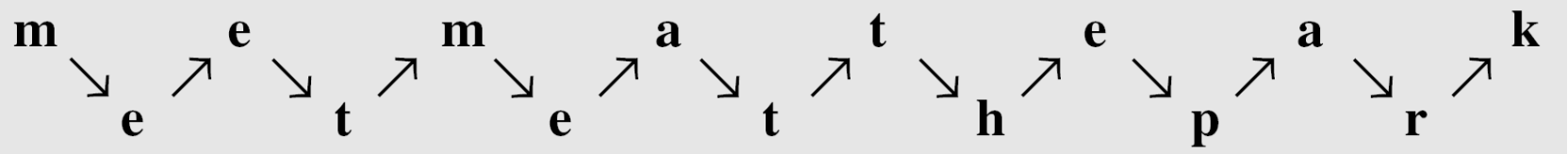
- The one-time pad, which is a provably secure cryptosystem, was developed by Gilbert Vernam in 1918.
- The message is represented as a binary string (a sequence of 0's and 1's using a coding mechanism such as ASCII coding.
- **The key is a truly random sequence of 0's and 1's of the same length as the 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

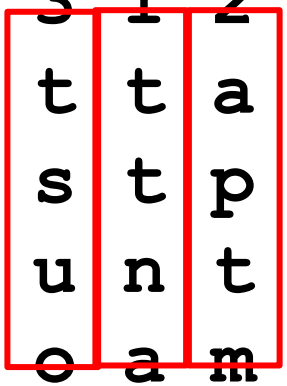
- A transposition cipher does not substitute one symbol for another, instead it changes the location of the symbols.
- The simplest such cipher is the **rail fence technique**, in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.
- For example, to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



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

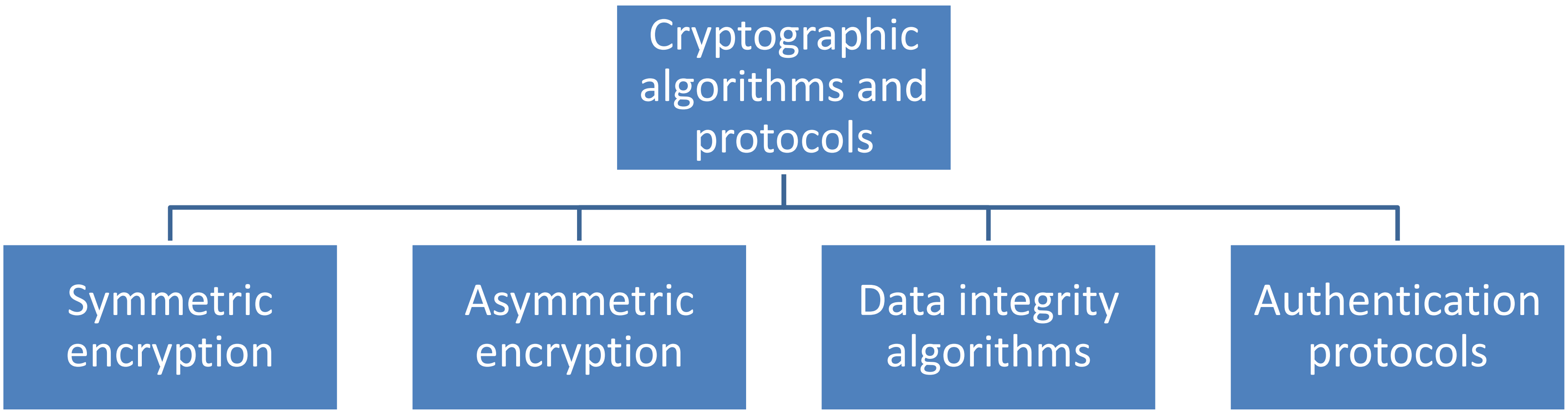
Ciphertext: TTNAAPTMTSUOAODWCOIXKNLYPETZ

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



- [illegible]

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
- has drawbacks
  - high overhead to hide relatively few info bits
- advantage is can obscure encryption use

3rd March

Dear George,

Greetings to all at Oxford. Many thanks for your letter and for the Summer examination package. All Entry Forms and Fees Forms should be ready for final despatch to the Syndicate by Friday 20th or at the very latest, I'm told, by the 21st. Admin has improved here, though there's room for improvement still; just give us all two or three more years and we'll really show you! Please don't let these wretched 16+ proposals destroy your basic O and A pattern. Certainly this sort of change, if implemented immediately, would bring chaos.

Sincerely yours.

Demo

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

THANK YOU FOR LISTENING ANY QUESTION ?

UNIT-1
Number Theory

Prime Numbers

- Prime numbers are central to number theory
- Prime numbers only have divisors of 1 and self
  - They cannot be written as a product of other numbers
  - e.g. 2,3,5,7 are prime, 4,6,8,9,10 are not

Relatively Prime Numbers

- Determining the GCD of two positive integers is easy
  - if they are expressed each - as the product of primes
  - e.g. if $300 = 2^2 \times 3^1 \times 5^2$ and $18 = 2^1 \times 3^2$ then the gcd(300, 18) is given as $2^1 \times 3^1 \times 5^0 = 6$
- Two numbers a and b are relatively prime if they have no common divisors apart from 1
  - e.g. 8 & 15 are relatively prime (even though none of them is prime) since factors of 8 are 1,2,4,8 and of 15 are 1,3,5,15 and 1 is the only common factor
  - e.g. check whether 6 and 8 are relative prime or not?
  - e.g. check whether 14 and 9 are relative prime or not?

Euclidean Algorithm

- Efficient way to find the GCD(a,b)
- Euclidean Algorithm to compute GCD(a,b) is:

```
EUCLID(a,b)
1. A = a; B = b
2. if B = 0 return  A (= gcd(a, b) )
3. R = A mod B
4. A = B
5. B = R
6. goto 2
```

  - e.g. check whether 6 and 8 are relative prime or not?
  - e.g. check whether 14 and 9 are relative prime or not?

Applications: Key Generation, Extended Euclidean Algorithm, Diffie-Hellman Key Exchange, Elliptic Curve Cryptography and more

Example GCD(1970,1066)

```
1970 = 1 x 1066 + 904     gcd(1066, 904)
1066 = 1 x 904 + 162      gcd(904, 162)
904 = 5 x 162 + 94              gcd(162, 94)
162 = 1 x 94 + 68               gcd(94, 68)
94 = 1 x 68 + 26          gcd(68, 26)
68 = 2 x 26 + 16          gcd(26, 16)
26 = 1 x 16 + 10          gcd(16, 10)
16 = 1 x 10 + 6           gcd(10, 6)
10 = 1 x 6 + 4            gcd(6, 4)
6 = 1 x 4 + 2                   gcd(4, 2)
4 = 2 x 2 + 0                   gcd(2, 0)
```

Therefore, gcd(1970, 1066) = 2

GCD(270,192) ??

Modular Arithmetic

- Two integers "a" and "b" are said to be congruent modulo "n" if their difference "a - b" is divisible by "n."
- This is denoted as "a ≡ b (mod n)." In other words, "a" and "b" leave the same remainder when divided by "n." e.g. 100 ≡ 34 mod 11 (where 100 and 34 leave same remainder when divided by 11)
- Modular addition rule
  - `e.g. (a+b)mod n = (a mod n + b mod n) mod n`
- Process of **modulo reduction:**
  - `E.g. -12 mod 7 ≡ -5 mod 7 ≡ 2 mod 7`
  - `E.g. 17 mod 5 ≡ 2 mod 5`

Abstract Algebra

- Number theory has increasing importance in cryptography
  - AES, Elliptic Curve, IDEA, Public Key
- Abstract algebra is a branch of mathematics that deals with algebraic structures, such as groups, rings, and fields, in a more abstract and general way than elementary algebra. It is called "abstract" because it focuses on the study of algebraic systems and their properties without necessarily specifying the nature of the elements involved.

Group

- A set of elements or “numbers”
- With some operation whose result is also in the set
- Obeys:
  - Closure: For any two elements "a" and "b" in the group, the result of the operation "a * b" is also in the group.
  - Associative law: $(a.b).c = a.(b.c)$
  - Has identity e: $e.a = a.e = a$
  - Has inverses a^{-1}: $a.a^{-1} = e$
- E.g. the set of integers "Z" under addition "+" forms a group.
- If commutative $a.b = b.a$
  - Then forms an **Abelian Group**

Cyclic Group

- A group is cyclic if every element is a power of some fixed element
- It is a group that can be generated by a single element, which is often referred to as the generator of the group.
- In a cyclic group, repeated applications of the group operation to the generator produce all the elements of the group.
- E.g. Cyclic Group of Integers Modulo 5: The set of integers modulo 5 is {0, 1, 2, 3, 4}, and the group operation is addition modulo 5

...Cyclic Group

Here are the key properties of this cyclic group:

- **Generator:** The integer 1 is a generator for this group. This means that by repeatedly adding 1 (modulo 5), we can generate all the elements of the group:
  - $1 + 1 \equiv 2 \pmod 5$
  - $2 + 1 \equiv 3 \pmod 5$
  - $3 + 1 \equiv 4 \pmod 5$
  - $4 + 1 \equiv 0 \pmod 5$
  - $0 + 1 \equiv 1 \pmod 5$
- **Closure:** When we add two integers modulo 5, the result remains within the set {0, 1, 2, 3, 4}, so the group is closed under addition modulo 5.
- **Associativity:** Addition modulo 5 is associative, as the order in which we add elements doesn't affect the result.
- **Identity Element:** The identity element in this group is 0 because adding 0 to any element doesn't change it.
- **Inverse Element:** Each element has an inverse within the group:
  - The inverse of 1 is 4 because $1 + 4 \equiv 0 \pmod 5$.
  - The inverse of 2 is 3 because $2 + 3 \equiv 0 \pmod 5$.
  - The inverse of 3 is 2 because $3 + 2 \equiv 0 \pmod 5$.
  - The inverse of 4 is 1 because $4 + 1 \equiv 0 \pmod 5$.
  - The inverse of 0 is itself ($0 + 0 \equiv 0 \pmod 5$).

Ring

- A set of “numbers”
- With two binary operations (addition and multiplication) which form
  - An Abelian Group with addition operation
- And multiplication:
  - Has closure
  - Is associative
  - Distributive over addition: `a(b+c) = ab + ac`
- If multiplication operation is commutative, it forms a **commutative ring**

Field

- A set of numbers with two operations which form:
  - Abelian Group for addition
  - Abelian Group for multiplication (ignoring 0)
  - Ring
- E.g. The field of real numbers (denoted as "R") with ordinary addition and multiplication.
- Hierarchy
  - Group -> Ring -> Field

Summary: Group, Ring and Field

- A group focuses on a single binary operation and is characterized by closure, associativity, identity, and inverses.
- A ring adds the concept of two operations (addition and multiplication) and maintains closure, associativity, and additional properties specific to rings. It may or may not have a multiplicative inverses for all elements.
- A field builds upon the ring structure but adds multiplicative inverses and a multiplicative identity, making it the most versatile and fundamental of the three structures.
- Fields are particularly important because they encompass both addition and multiplication, and they play a crucial role in various mathematical and scientific applications, including number theory, linear algebra, and cryptography.

Galois Fields

- Galois Fields (Finite fields) play a key role in cryptography
- It contains a finite number of elements. As with any field, a finite field is a set on which the operations of multiplication, addition, subtraction and division are defined and satisfy certain basic rules.
- The number of elements of a finite field is called its order or, sometimes, its size.
- A Galois field consists of a finite number of elements, denoted as "GF(p)," where “p" is a prime number (forms a Prime Field) or a power of a prime number (forms an Extension Field).
- Extension fields are constructed by defining irreducible polynomials over the prime field
- An irreducible polynomial is a polynomial that cannot be factored into two lower-degree polynomials with coefficients in the base field

Galois Fields GF(p)

- In particular often use the fields
  - GF(p)
  - GF(2^n)
- GF(p) is the set of integers Z_p ={0,1, … , p-1} with arithmetic operations modulo prime p
  - E.g. GF(7)={0,1,2,3,4,5,6}
- The arithmetic in GF is “well-behaved”
  - i.e. can do addition, subtraction, multiplication, and division without leaving the field GF(p)

GF(7) Addition/Multiplication Example

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

(a) Addition modulo 7

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

(b) Multiplication modulo 7

w	$-w$	w^{-1}
0	0	—
1	6	1
2	5	4
3	4	5
4	3	2
5	2	3
6	1	6

(c) Additive and multiplicative inverses modulo 7

Polynomial Arithmetic

- can compute using polynomials

  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = \sum a_i x^i$

  - nb. not interested in any specific value of x
  - which is known as the indeterminate

- several alternatives available
  - ordinary polynomial arithmetic
  - poly arithmetic with coords mod p
  - poly arithmetic with coords mod p and polynomials mod m(x)

Ordinary Polynomial Arithmetic

- add or subtract corresponding coefficients
- multiply all terms by each other
- eg

  let $f(x) = x^3 + x^2 + 2$ and $g(x) = x^2 - x + 1$

  $f(x) + g(x) = x^3 + 2x^2 - x + 3$

  $f(x) - g(x) = x^3 + x + 1$

  $f(x) \times g(x) = x^5 + 3x^2 - 2x + 2$

Polynomial Arithmetic with Modulo Coefficients

- We are most interested in mod 2
  - i.e. all coefficients are 0 or 1
  - eg. let $f(x) = x^3 + x^2$ and $g(x) = x^2 + x + 1$

    $f(x) + g(x) = x^3 + x + 1$

    $f(x) \times g(x) = x^5 + x^2$

Polynomial Division

- If $g(x)$ has no divisors other than itself & 1 say it is **irreducible** (or prime) polynomial
- Arithmetic modulo an irreducible polynomial forms a field (As discussed earlier)
    - x13+x11+x9+x8+x6+x5+x4+x3+1 modulo x8+x4+x3+x+1 (11B)
    - x7+x6+1=C1

Modular Polynomial Arithmetic

- can compute in field GF(2^n)
  - polynomials with coefficients modulo 2
  - whose degree is less than n
  - hence must reduce modulo an irreducible poly of degree n (for multiplication only)
- form a finite field
- can always find an inverse
  - can extend Euclid's Inverse algorithm to find

Example GF(2^3)

Table 4.6 Polynomial Arithmetic Modulo $(x^3 + x + 1)$

	+	000 0	001 1	010 x	011 $x+1$	100 x^2	101 x^2+1	110 x^2+x	111 x^2+x+1
000	0	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
001	1	1	0	$x+1$	x	x^2+1	x^2	x^2+x+1	x^2+x
010	x	x	$x+1$	0	1	x^2+x	x^2+x+1	x^2	x^2+1
011	$x+1$	$x+1$	x	1	0	x^2+x+1	x^2+x	x^2+1	x^2
100	x^2	x^2	x^2+1	x^2+x	x^2+x+1	0	1	x	$x+1$
101	x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1	0	$x+1$	x
110	x^2+x	x^2+x	x^2+x+1	x^2	x^2+1	x	$x+1$	0	1
111	x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2	$x+1$	x	1	0

(a) Addition

	×	000 0	001 1	010 x	011 $x+1$	100 x^2	101 x^2+1	110 x^2+x	111 x^2+x+1
000	0	0	0	0	0	0	0	0	0
001	1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
010	x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
011	$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
100	x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
101	x^2+1	0	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
110	x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
111	x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+x	x^2	$x+1$

(b) Multiplication

Computational Example

- In GF(2^3) have (x^2+1) is 101_2 & (x^2+x+1) is 111_2
- So addition is
  - $(x^2+1) + (x^2+x+1) = x$
  - 101 XOR $111 = 010_2$
- And multiplication is
  - $(x+1).(x^2+1) = x.(x^2+1) + 1.(x^2+1)$
    $= x^3+x+x^2+1 = x^3+x^2+x+1$ (which is 1111)
- Polynomial modulo reduction (get q(x) & r(x)) is
  - $(x^3+x^2+x+1) \bmod (x^3+x+1) = 1.(x^3+x+1) + (x^2) = x^2$ (which is 0100)

Euler Totient Function ∅(n)

- When doing arithmetic modulo n
- **complete set of residues** is: `0..n-1`
- **Reduced set of residues** is those numbers (residues) which are relatively prime to n
  - e.g. for n=10,
  - Complete set of residues is {0,1,2,3,4,5,6,7,8,9}
  - Reduced set of residues is $Z_n^* = Z_{10}^* = \{1,3,7,9\}$
- **Number of elements** in reduced set of residues is called the **Euler Totient Function ø(n)**
- ϕ(1) = 1 since for n = 1 the only integer in the range from 1 to n is 1 itself, and gcd(1, 1) = 1

Euler Totient Function ø(n) (Cont.)

- To compute ø(n) need to count number of residues to be excluded
- In general need prime factorization, but
  - For p (p prime) ø(p) = p-1
  - For p*q (p,q prime) ø(p*q) =(p-1)x(q-1)
- Multiplicative group Z**n** is denoted by Z**n***
- Examples

$|Z_{10}^*| = \phi(10)=\phi(2)*\phi(5)=(2-1)*(5-1)=4$

$|Z_{37}^*| = \phi(37) = 36$

$|Z_{21}^*| = \phi(21) = \phi(3)*\phi(7)=(3-1)x(7-1) = 2x6 = 12$

$|Z_{27}^*| = \phi(27) = \phi(3^3)= 3^2*\phi(3)= 9*2 = 18$

(for a prime p, ϕ(p^n) = p^n - p^(n-1))

Euler's Theorem

- Also known as the **Fermat–Euler Theorem** or **Euler's Totient Theorem**
- States that if *n* is a positive integer and *a* is a positive integer relatively prime to *n* (i.e. gcd (a,n)=1), then $a^{\phi(n)} \equiv 1 \pmod{n}$
- e.g.

  a=3;*n*=10; (3 is relative prime to 10)

  ø(10)=ø(2) x ø(5)=4;

  hence $3^4 = 81 \equiv 1 \bmod 10$

  a=2;*n*=11; ø(11)=10;

  hence $2^{10} = 1024 \equiv 1 \bmod 11$

Modular Multiplicative Inverse

- The modular multiplicative inverse of A mod C is the B value that makes A * B mod C = 1
- **Example: A=3, C=7**

  Calculate A * B mod C for B values <u>0 through C-1</u>

  3 * 0 ≡ 0 (mod 7)

  3 * 1 ≡ 3 (mod 7)

  3 * 2 ≡ 6 (mod 7)

  3 * 3 ≡ 9 ≡ 2 (mod 7)

  3 * 4 ≡ 12 ≡ 5 (mod 7)

  3 * 5 ≡ 15 (mod 7) ≡ <u>1</u> (mod 7) <------ FOUND INVERSE!

  3 * 6 ≡ 18 (mod 7) ≡ 4 (mod 7)
- **Example: A=2 C=6**

  Calculate A * B mod C for B values 0 through C-1

  2 * 0 ≡ 0 (mod 6)

  2 * 1 ≡ 2 (mod 6)

  2 * 2 ≡ 4 (mod 6)

  2 * 3 ≡ 6 ≡ 0 (mod 6)

  2 * 4 ≡ 8 ≡ 2 (mod 6)

  2 * 5 ≡ 10 ≡ 4 (mod 6)

  No value of B makes A * B mod C = 1. Therefore, A has no modular inverse (mod 6). This is because 2 is not coprime to 6 (they share the prime factor 2).

  ∎

Extended Euclidean Algorithm

- It is easy to find multiplicative inverse for small value of n by just constructing multiplication table.
- But this method is not practical for large value of n. so for that we need Extended Euclidean algorithm.
- Euclidean Algorithm can be extended so that in addition to finding gcd(m,b), if gcd is 1, the algorithm returns the multiplicative inverse of b.

Finding Inverses – Extended Euclidean algorithm

```
EXTENDED_EUCLID(m, b)
1. (A1, A2, A3)=(1, 0, m);
   (B1, B2, B3)=(0, 1, b)
2. if B3 = 0
   return A3 = gcd(m, b); no inverse
3. if B3 = 1
   return B3 = gcd(m, b); B2 = b^-1 mod m
4. Q = A3 div B3
5. (T1, T2, T3)=(A1 - Q B1, A2 - Q B2, A3 -
   Q B3)
6. (A1, A2, A3)=(B1, B2, B3)
7. (B1, B2, B3)=(T1, T2, T3)
8. goto 2
```

Inverse of 49 in GF(37)

i.e. calling Extended_Euclid(37, 49)

Q	A1	A2	A3	B1	B2	B3
—	1	0	37	0	1	49
0	0	1	49	1	0	37
1	1	0	37	-1	1	12
3	-1	1	12	4	-3	1

- Hence $49^{-1} \equiv (-3) \bmod 37$
- But, $-3 \pmod{37} \equiv 34 \pmod{37}$. Hence,

multiplicative inverse of 49 modulo 37 is 34.

Inverse of 550 in GF(1759)

i.e. calling Extended_Euclid(1759, 550)

Q	A1	A2	A3	B1	B2	B3
—	1	0	1759	0	1	550
3	0	1	550	1	–3	109
5	1	–3	109	–5	16	5
21	–5	16	5	106	–339	4
1	106	–339	4	–111	355	1

Primitive Roots

- A primitive root is any number g in multiplicative group that generates whole group of integers
- e.g. $Z_{14}^*=\{1,3,5,9,11,13\}$

  1 : 1

  3 : 3, 9, 13, 11, 5, 1

  5 : 5, 11, 13, 9, 3, 1

  9 : 9, 11, 1

  11 : 11, 9, 1

  13 : 13, 1

  Thus, 3 and 5 are primitive roots modulo 14

Discrete Logarithms

- Discrete logarithms are fundamental to a number of public-key algorithms, including Diffie-Hellman key exchange and the digital signature algorithm (DSA).
- The inverse problem to exponentiation is to find the **discrete logarithm** of a number modulo p
- That is to find x such that $y = g^x \pmod p$
  - This is written as $x = \log_g y \pmod p$
- If g is a primitive root then it always exists, otherwise it may not,
  - e.g.

    $x = \log_3 4 \bmod 13$ has no answer !

    $x = \log_2 3 \bmod 13 = 4$ (i.e. $3=2^4 \bmod 13$)
- Exponentiation is relatively easy, but finding discrete logarithms is generally a **hard** problem

Divisibility & the Division Algorithm

"b divides a" if $a = mb$ $[\ b \mid a\ ]$

Eg:- 13 divides 182 , $13 \mid 182$
-5 divides 30 , $-5 \mid 30$
17 divides 0 , $17 \mid 0$

Properties

↳ If $a \mid 1$, then $a = \pm 1$

↳ If $a \mid b$ and $b \mid a$, then $a = \pm b$

↳ Any $b \neq 0$ divides 0

↳ If $a \mid b$ and $b \mid c$, then $a \mid c$

↳ If $b \mid g$ and $b \mid h$, then $b \mid (mg + nh)$ for arbitrary integers m & n.

Proof

If $b \mid g$, then $g = b * g_1$ for some integer g_1

If $b \mid h$, then $h = b * h_1$ " " " h_1

$$mg + nh = mbg_1 + nbh_1$$
$$= b * (mg_1 + nh_1)$$

$\therefore$ b divides $mg + nh$

Eg:- $b = 7$, $g = 14$, $h = 63$

$7 \mid 14$ and $7 \mid 63$

$\therefore 7 \mid 14m + 63n$ where $m = 3$, $n = 2$

$14m + 63n$
$= 14 * 3 + 63 * 2$
$= 2 * 3 [7 + 21]$
$= 7 [6 + 18]$

Division algorithm

If we divide positive int. 'a' by positive int. 'n'

quotient = q
remainder = r ('residue')

$$n \overline{)\, a \,(\, q}$$
$$\underline{\quad\quad}$$
$$r$$

$$\boxed{a = qn + r}$$

$$0 \leq r \leq n$$

$$q = \lfloor a/n \rfloor$$

$$qn \leq a$$
$$(q+1)n > a$$

The dist^n from qn to a is r

Eg:- $a = 11$, $n = 7$
$q = 1$, $r = 4$

$11 = 7 * 1 + 4$

Eg:- $a = -11$, $n = 7$
$q = -2$, $r = 3$

$-11 = 7 * -2 + 3$

Euclidean Algorithm

↳ to determine (gcd) greatest common divisor
or (hcf) highest common factor

GCD of 'a' & 'b': The largest integer that divides both 'a' and 'b'

$$gcd(a,b) = \max [k, \text{such that } k|a \text{ and } k|b]$$

GCD should be positive

$$gcd(a,b) = gcd(a,-b) = gcd(-a,b) = gcd(-a,-b)$$
$$= gcd(|a|, |b|)$$

→ Because all non-zero integers divide 0,
∴ $\gcd(a,0) = |a|$

→ 'a' and 'b' are relatively prime if $\gcd(a,b) = 1$

How to find GCD (a,b)?

Divide a by b

$a = q_1 b + r_1 \quad 0 < r_1 < b$

$b = q_2 r_1 + r_2 \quad 0 < r_2 < r_1$

$r_1 = q_3 r_2 + r_3 \quad 0 < r_3 < r_2$

Euclidean algorithm

$b \overline{)a} (q_1$

$r_1 \overline{)b} (q_2$

$r_2 \overline{)r_1} (q_3$

r_3

$r_{n-1} = q_{n+1} r_n + 0 \quad 0 < r_n < r_{n-1}$

$GCD(a,b) = r_n$

Eg:- Find GCD of 326 and 16

$16 \overline{)326} (20$
320

$6 \overline{)16} (2$
12

$4 \overline{)6} (1$
4

$2 \overline{)4} (2$
4

0

Ans :- 2

Modular Arithmetic

Two integers 'a' and 'b' are said to be congruent modulo n,

if $(a \bmod n) = (b \bmod n)$ This is written as $a \equiv b \pmod n$

Eg: $-73 \equiv 4 \pmod{23}$

$21 \equiv -9 \pmod{10}$

Properties

↳ $a \equiv b \bmod n$ if $n \mid (a-b)$

↳ $a \equiv b \pmod n$ implies $b \equiv a \pmod n$

↳ $a \equiv b \pmod n$, $b \equiv c \pmod n$ implies $a \equiv c \pmod n$

Modular Arithmetic operations properties.

↳ $[(a \bmod n) + (b \bmod n)] \bmod n = (a+b) \bmod n$

↳ $[(a \bmod n) - (b \bmod n)] \bmod n = (a-b) \bmod n$

↳ $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$

Eg:- Find $11^7 \bmod 13$

$11^2 \bmod 13 = 121 \bmod 13 = 4$

$11^4 \bmod 13 = (11^2)^2 \bmod 13 = 4^2 \bmod 13 = 16 \bmod 13 = 3$

$11^7 = 11 \times 11^2 \times 11^4$

$11^7 \bmod 13 = (11 * 4 * 3) \bmod 13$

$= 132 \bmod 13$

$= 2$

$Z_n = \{0, 1, 2, \ldots, n-1\}$

Arithmetic Modulo 8.

Addition modulo 8

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

Multiplication modulo 8

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Additive & Multiplicative inverse modulo 8

w	−w	w^{-1}
0	0	–
1	7	1
2	6	–
3	5	3
4	4	–
5	3	5
6	2	–
7	1	7

Set of residues / residue classes (mod n)

$Z_n = \{0, 1, 2, \ldots (n-1)\}$

Residue classes (mod n) are $[0], [1], [2] \ldots, [n-1]$

where $[r] = \{a : a \text{ is an integer}, a \equiv r \pmod n\}$

Eg:- The residue classes (mod 4) are

$[0] = \{\ldots, -16, -12, -8, -4, 0, 4, 8, 12, 16, \ldots\}$

$[1] = \{\ldots, -15, -11, -7, -3, 1, 5, 9, 13, 17, \ldots\}$

$[2] = \{\ldots, -14, -10, -6, -2, 2, 6, 10, 14, 18, \ldots\}$

$[3] = \{\ldots, -13, -9, -5, -1, 3, 7, 11, 15, 19, \ldots\}$

The smallest non-negative integer is used to represent the residue class.

Z_n is a commutative ring with a multiplicative identity element.

If $(a+b) \equiv (a+c) \bmod n$
then $b \equiv c \pmod n$

Eg:- $(5+23) \equiv (5+7) \bmod 8$
then $23 \equiv 7 \bmod 8$

Properties for modular arithmetic for integers in Z_n

- Commutative laws. $(w+x) \bmod n = (x+w) \bmod n$
  $(w*x) \bmod n = (x*w) \bmod n$
- Associative laws
- Distributive laws
- Identities $(0+w) \bmod n = w \bmod n$
  $(1*w) \bmod n = w \bmod n$
- Additive inverse For each $w \in Z_n$, there exists a z such that $w+z \equiv 0 \bmod n$

If $(a \times b) \equiv (a \times c) \bmod n$
then $b \equiv c \pmod n$ if 'a' is relatively prime to 'n'.

Two integers are relatively prime if their only common positive integer factor is 1

$ab \equiv ac \bmod n$
$(a^{-1})ab \equiv (a^{-1})ac \bmod n$
$b \equiv c \bmod n$

Eg:- 6 and 8 are not relatively prime [$\gcd(6,8) \neq 1$]

$6 \times 3 = 18 \equiv 2 \bmod 8$
$6 \times 7 = 42 \equiv 2 \bmod 8$
Yet $3 \not\equiv 7 \pmod 8$

With $a = 6$ and $n = 8$,

Z_8 =	0	1	2	3	4	5	6	7
Multiply by 6	0	6	12	18	24	30	36	42
Residues	0	6	4	2	0	6	4	2

∴ There is not a unique inverse to the multiply operation

With $a = 5$ and $n = 8$ $\quad \gcd(5, 8) = 1$

Z_8	0	1	2	3	4	5	6	7
Multiply by 5	0	5	10	15	20	25	30	35
Residues	0	5	2	7	4	1	6	3

→ Integers 1, 3, 5 and 7 have a multiplicative inverse in Z_8, but 2, 4 and 6 do not.

Euclidean Algorithm Revisited

$$\gcd(a, b) = \gcd(b, a \bmod b)$$

Eg:- $\gcd(55, 22) = \gcd(22, 55 \bmod 22)$
$= \gcd(22, 11) = 11$

~~Proof~~ :- ~~gcd(a,b).~~

~~a = kb + r~~

~~gcd(b, a mod b)~~
~~b = k'(a mod b) + r'~~
~~b = k'kb + r'~~

Extended Euclidean Algorithm (useful in RSA)

↳ not only it calculates the gcd 'd', but also 2 additional integers 'x' and 'y' that satisfy the following equation :-

$$ax + by = d = \gcd(a, b)$$

Eg:- $\gcd(42, 30) = 6 = 42x + 30y$
$= 6(7x + 5y)$

y \ x	3	2	-1	0	1	2	3
3	-216	-174	-132	-90	-48	-6	36
2	-186	-144	-102	-60	-18	24	66
-1	-156	-114	-72	-30	12	54	96
0	-126	-84	-42	0	42	84	126
1	-96	-54	-12	30	72	114	156
2	-66	-24	18	60	102	144	186
3	-36	6	48	90	132	174	216

$42x + 30y = 6(7x + 5y)$ is a multiple of 6.

Note $\gcd(42, 30) = 6$.

Eg:- Use $a = 1759$ and $b = 550$ and solve for $1759x + 550y = \gcd(1759, 550)$

i	r_i	q_i	x_i	y_i
-1	1759		1	0
0	550		0	1
1	109	3	1	-3
2	5	5	-5	16
3	4	21	106	-339
4	1	4	-111	355
5	0			

$\gcd$ ← 1 ; x ← -111 ; y ← 355

$\gcd(1759, 550) = 1 = 1759(-111) + 550(355)$

$$\begin{cases} x_n = x_{n-2} - q_n x_{n-1} \\ y_n = y_{n-2} - q_n y_{n-1} \end{cases}$$

550) 1759 (3
1650
109) 550 (5
545
5) 109 (21
105
4) 5 (1
4
1) 4 (4
4
x

Prime Numbers

An integer $p > 1$ is a prime no. if and only if its only divisors are ± 1 and $\pm p$.

Any integer 'a' can be factored in a unique way as :-

$$a = p_1^{a_1} \times p_2^{a_2} \times p_3^{a_3} \ldots \times p_t^{a_t}$$

where $p_1 < p_2 < p_3 \ldots < p_t$ are prime numbers and each a_i is a positive integer

---

Given, $a = \prod_{p \in P} p^{a_p}$ and $b = \prod_{p \in P} p^{b_p}$

If $a | b$ then $a_p \leq b_p \quad \forall p$

If $k = \gcd(a, b)$, then $k_p = \min(a_p, b_p) \quad \forall p$

Eg :- $300 = 2^2 \times 3^1 \times 5^2$

$18 = 2^1 \times 3^2$

$\gcd(18, 300) = 2^1 \times 3^1 \times 5^0 = 6$

FERMAT'S THEOREM. (Imp. in public key cryptography)

p is prime.
a is positive integer not divisible by p

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

Eg :- $a = 7, \quad p = 19$

$a^{p-1} = 7^{18}$

$7^{18} \bmod 19 = 1$

$7^{18} \equiv 1 \bmod 19$

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

$7^2 \bmod 19 = 11$

$7^4 \bmod 19 = 121 \bmod 19 = 7$

$7^8 \bmod 19 = 49 \bmod 19 = 11$

$7^{16} \bmod 19 = 121 \bmod 19 = 7$

$7^{18} \bmod 19 = (7 \times 11) \bmod 19 = 1$

Proof :-

$p : \{1, 2, \ldots\ldots p-1\}$

multiply each element by a and modulo p

$X = \{a \bmod p,\ 2a \bmod p, \ldots\ldots (p-1)a \bmod p\}$

None of the elements is 0 as p does not divide a

No two integers in X are equal.

[$\because ja \equiv ka \pmod p$ where $1 \le j < k \le p-1$

$\gcd(a, p) = 1$

So $j \equiv k \pmod p$

This is impossible because j & k are both positive int. less than p. $j \neq k$

$[a \times 2a \times 3a \ldots\ldots \times (p-1)a] \bmod p$

$\Rightarrow [1 \times 2 \times 3 \times \ldots\ldots (p-1)] \bmod p$

$[a^{p-1}(p-1)!] \bmod p \Rightarrow [(p-1)!] \bmod p$

$(p-1)!$ is relatively prime to p

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

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

Hence Proved

Alternate form of Fermat's theorem

$$\boxed{a^p \equiv a \bmod p}$$

Eg:- $a = 3,\ p = 5$

$3^5 \equiv 3 \bmod 5$

$3^2 * 3^2 * 3$

4 4 3

16

1

3

Euler's Totient function : $\phi(n)$

$\phi(n)$ ⇒ defined as the no. of positive integers less than n & relatively prime to n.

$\phi(37) = 36$ (All no.s 1 to 36 are relatively prime to 37, because 37 is prime no.)

$\phi(35) = 24$.

{1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 16, 17, 18, 19, 22, 23, 24, 26, 27, 29, 31, 32, 33, 34}

For prime numbers (p),

$$\phi(p) = p - 1$$

Let 2 prime no.s p & q , $p \neq q$

$$n = p \times q$$

$$\phi(n) = \phi(p*q) = \phi(p) * \phi(q)$$
$$= (p-1)(q-1)$$

Eg:-

$$\phi(21) = \phi(3) * \phi(7)$$
$$= 2 * 6$$
$$= 12$$

Euler's Theorem

For every 'a' and 'n' that are relatively prime:

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

If n is prime,

$\phi(n) = (n-1)$ then $a^{\phi(n)} = a^{n-1} \equiv 1 \bmod(n)$

[∵ Fermats' theorem]

Let set of integers : $R = \{x_1, x_2, \ldots x_{\phi(n)}\}$

Each element x_i of R is a unique positive int less than n with $\gcd(x_i, n) = 1$

$$S = \{(ax_1 \bmod n), (ax_2 \bmod n), \ldots (ax_{\phi(n)} \bmod n)\}$$

S is a permutation of R because

→ Because a is relatively prime to n
& x_i " " " " n

∴ ax_i must also be relatively prime to n

Thus all members of S are less than n, and that are relatively prime to n

→ There are no duplicates in S

$$\prod_{i=1}^{\phi(n)} (ax_i \bmod n) = \prod_{i=1}^{\phi(n)} x_i$$

$$\prod_{i=1}^{\phi(n)} ax_i \equiv \prod_{i=1}^{\phi(n)} x_i \pmod n$$

$$a^{\phi(n)} \left[\prod_{i=1}^{\phi(n)} x_i\right] \equiv \prod_{i=1}^{\phi(n)} x_i \pmod n$$

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

Euler's Theorem

Eg:- $a = 3, \quad n = 10$

$\phi(10) = 4 \qquad \{1, 3, 7, 9\}$

$a^{\phi(n)} = 3^4 = 81$

$81 \equiv 1 \bmod 10$

Alternate form of Euler's Theorem

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

Testing for primality

For many cryptographic algorithms, it is necessary to select one or more very large prime no.s at random. Thus, the task is :- determining whether a given large no. is prime.

Properties of Prime Numbers.

(1) p : prime
a is a +ve integer less than p,
then $a^2 \bmod p = 1$ iff $a \bmod p = 1$
or $a \bmod p = -1 \bmod p = p-1$

Proof :-
$(a \bmod p)(a \bmod p) = a^2 \bmod p$.
for $a^2 \bmod p = 1$, either $a \bmod p = 1$
or $a \bmod p = -1$

Conversely,
If $a^2 \bmod p = 1$, then $(a \bmod p)^2 = 1$
which is true only for
$a \bmod p = \pm 1$.

(2) p : prime no. > 2
$k > 0$, q : odd
then $p - 1 = 2^k q$.
Let a : int, $1 < a < p-1$
Then one of the two conditions is true.

(a) $a^q \equiv 1 \bmod p$

(b) One of the numbers $a^q, a^{2q}, a^{4q}, \ldots a^{2^{k-1}q}$
is congruent to $-1 \bmod p$
There is some int j, $1 \le j \le k$
such that $a^{2^{j-1}q} \bmod p = -1 \bmod p = p-1$
or $a^{2^{j-1}q} \equiv -1 \bmod p$

Miller - Rabin test / Rabin - Miller test

If n is prime, then either the first element in the list of residues or remainders

$(a^q, a^{2q}, a^{3q} \ldots a^{2^{k-1}q}, a^{2^k q})$ mod n

equals 1

Or, some element in the list equals $(n-1)$

Otherwise, n is composite (not prime)

Eg:- $n = 2047 = 23 * 89$

then $n-1 = 2046$

$= 2 * 1023$

$2^{1023} \bmod 2047 = 1$

2047 meets the condition, but is not prime

TEST (n)

(1) Find int. k, q with $k>0$, q: odd, so that $n-1 = 2^k q$

(2) Select a random int a, $1 < a < n-1$

(3) if $a^q \bmod n = 1$, then return ("inconclusive")

(4) For $j = 0$ to $k-1$, do

(5) If $a^{2^j q} \bmod n = n-1$, then return ("inconclusive")

(6) return ("composite")

Eg:- test for $n = 29$ (prime)

$n-1 = 28 = 2^2 * 7 = 2^k \cdot q$ $\quad k=2, q=7$

Let $a = 10$ (random)

$a^q \bmod n = 10^7 \bmod 29 = 17$

which is neither 1 nor $n-1$ 28

Next calculate $a^{(10^7)^2} \bmod 29 = 28$.

Return "inconclusive"

$10^1 \bmod 29 = 10$
$10^2 \bmod 29 = 13$
$10^3 \bmod 29 = 14$
$10^4 \bmod 29 = 24$
$10^5 \bmod 29 = 8$
$10^6 \bmod 29 = 22$
$10^7 \bmod 29 = 17$

let $a = 2$. (random)

$2^q \bmod n$

$2^7 \bmod 29 = 12$

$2^{2q} \bmod n$

$2^{14} \bmod 29 = 28$

Reason Test for all $a \in [1, 28]$ we get same "inconclusive" result

Eg:- Test for $n = 221$ (composite)

$221 = 13 * 17$

$n - 1 = 220.$

$= 2 * 110$

$= 2 * 2 * 55$

$= 2^2 . (55)$

$= 2^k . q$

$k = 2$

$q = 55$

let $a = 5$.

$a^q \bmod n = 5^{55} \bmod 221 = 112$

$\neq 1.$

$\neq n-1 (220)$

$5^{55.2} \bmod 221 = 168$

After checking all values of j, test returns composite.

Only for $a = 21, 47, 174, 200.$

test returns ("inconclusive")

For all other $a \in [1, 220]$, test returns "composite"

Miller's test

Repeatedly invoke TEST(n) using randomly chosen values for 'a'. If at any point, TEST returns composite, then 'n' is determined to be non-prime.

If TEST continues to return inconclusive for t tests, then for sufficiently large values of 't', assume that 'n' is prime.

Chinese Remainder Theorem (example)

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

$$X \equiv a_1 \bmod m_1$$
$$X \equiv a_2 \bmod m_2$$
$$\vdots$$
$$X \equiv a_n \bmod m_n$$

CRT states that the above eqn has a unique solution if $m_1, m_2 \ldots m_n$ are relatively prime.

$$X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + \ldots + a_n M_n M_n^{-1}) \bmod M$$

Eg: 1 Solve the following equations using CRT

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

$a_1 = 2$, $a_2 = 3$, $a_3 = 2$. $m_1 = 3$, $m_2 = 5$, $m_3 = 7$

Solution :

$$X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \bmod M$$

unique soln exists because $(3, 5, 7)$ are m_1, m_2, m_3 relatively prime.

$$M = m_1 \times m_2 \times m_3$$
$$= 3 \times 5 \times 7$$
$$= 105$$

$$M_1 = \frac{M}{m_1} = \frac{105}{3} = 35$$

$$M_2 = \frac{M}{m_2} = \frac{105}{5} = 21$$

$$M_3 = \frac{M}{m_3} = \frac{105}{7} = 15$$

$$M_1 * M_1^{-1} = 1 \bmod m_1$$
$$35 * M_1^{-1} = 1 \bmod 3$$
$$M_1^{-1} = 2$$

$$M_2 * M_2^{-1} = 1 \bmod m_2$$
$$21 * M_2^{-1} = 1 \bmod 5$$
$$M_2^{-1} = 1$$

$$M_3 * M_3^{-1} = 1 \bmod m_3$$
$$15 * M_3^{-1} = 1 \bmod 7$$
$$M_3^{-1} = 1$$

$$X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \bmod M$$

$$= (2 * 35 * 2 + 3 * 21 * 1 + 2 * 15 * 1) \bmod 105$$

$$= (140 + 63 + 30) \bmod 105$$

$$= 233 \bmod 105$$

$$= 23$$

$23 \equiv 2 \bmod 3$

$23 \equiv 3 \bmod 5$

$23 \equiv 2 \bmod 7$