

Cryptography and Network Security—CY44

William Stallings 4th Edition

What is Cryptography?



Course Objectives:

- To discuss various paradigms and principles of modern cryptography.
- Focus will be on the formal security definitions and constructions of various cryptographic primitives.
 - Encryption and Decryption, Message authentication codes, Hash Functions, Digital Signatures etc.

Syllabus

Unit I

Introduction: Security Trends, Security attacks, Security services, Security Mechanisms, A Model for Network Security Model, Classical Encryption Techniques, Symmetric Cipher Model, Substitution Techniques, Transposition Techniques, Rotor Machines, Steganography.

Unit II

Block Ciphers and Data Encryption Standard: Block Cipher Principles, Data Encryption Standard, Strength of DES, Differential and Linear Cryptanalysis, Block Cipher Design Principles, Advanced Encryption Standard, Evaluation Criteria of AES, AES Cipher, Multiple encryption and Triple DES, Block Cipher Modes of Operation, RC4, Cast-128, Blowfish Algorithms

Unit III

Public - Key Encryption and Hash Functions : Principles of Public Key Cryptosystems, RSA Algorithm, Key Management, Message Authentication and Hash Functions, Authentication Requirements, Authentication Functions, Message Authentication, Hash Functions, Security of Hash Functions and MACs, Digital Signatures, Authentication Protocols, Digital Signature Standard.

Unit IV

Network Security Applications: Kerberos, X.509 Authentication Service, Public Key Infrastructure, Pretty Good Privacy, S/MIME, IP Security Overview, IP Security architecture, Authentication Header, Encapsulating Security Payload, Combining Security associations, Key Management.

Unit V

System Security: Secure Socket Layer and Transport Layer Security, Secure Electronic Transaction, Intruders, Intrusion Detection, Password Management, Malicious Software, Firewalls, Trusted Systems.

Applications of Cryptography



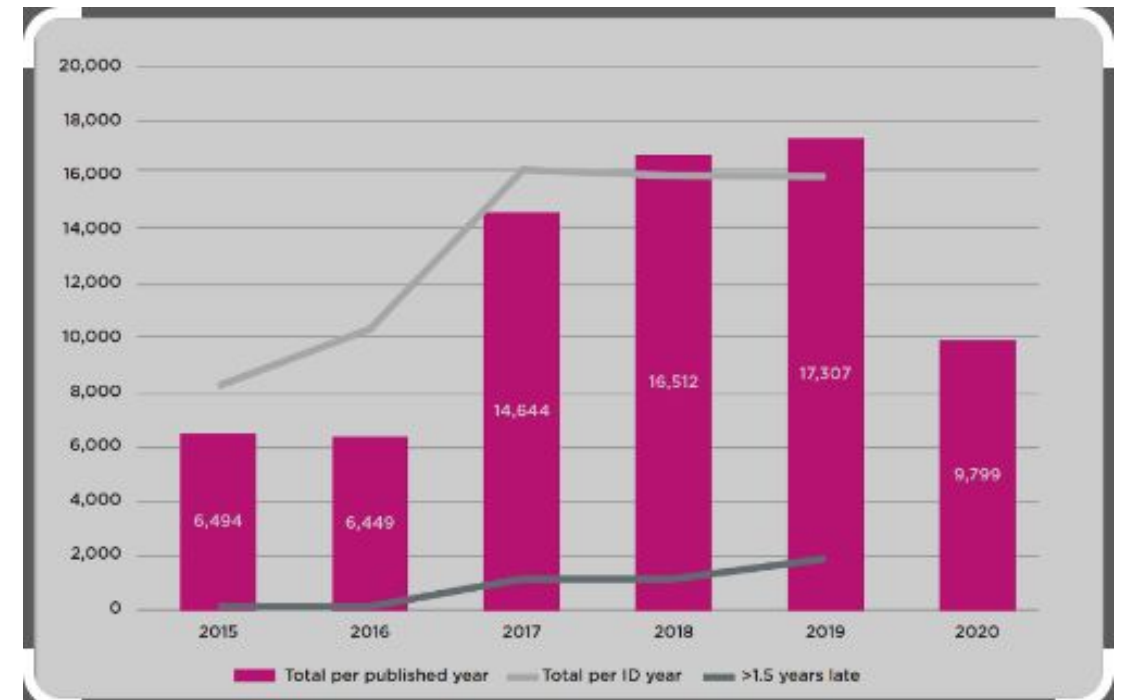
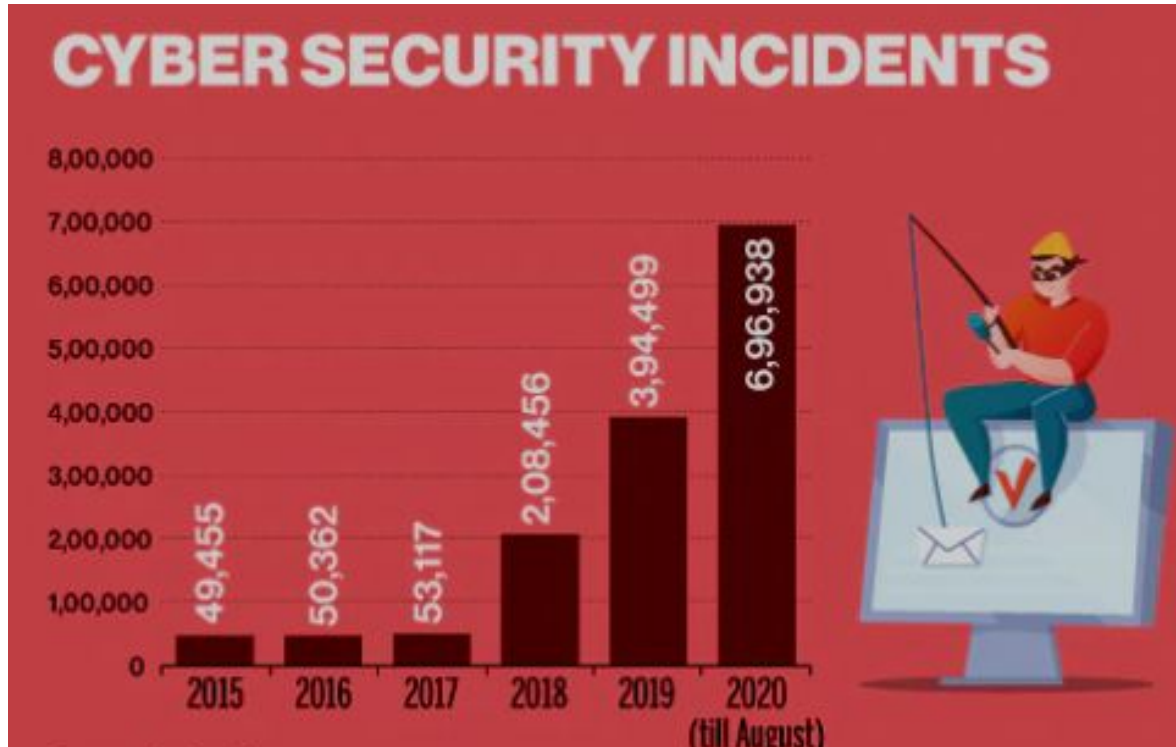
Unit-01

Chapter-01-Introduction

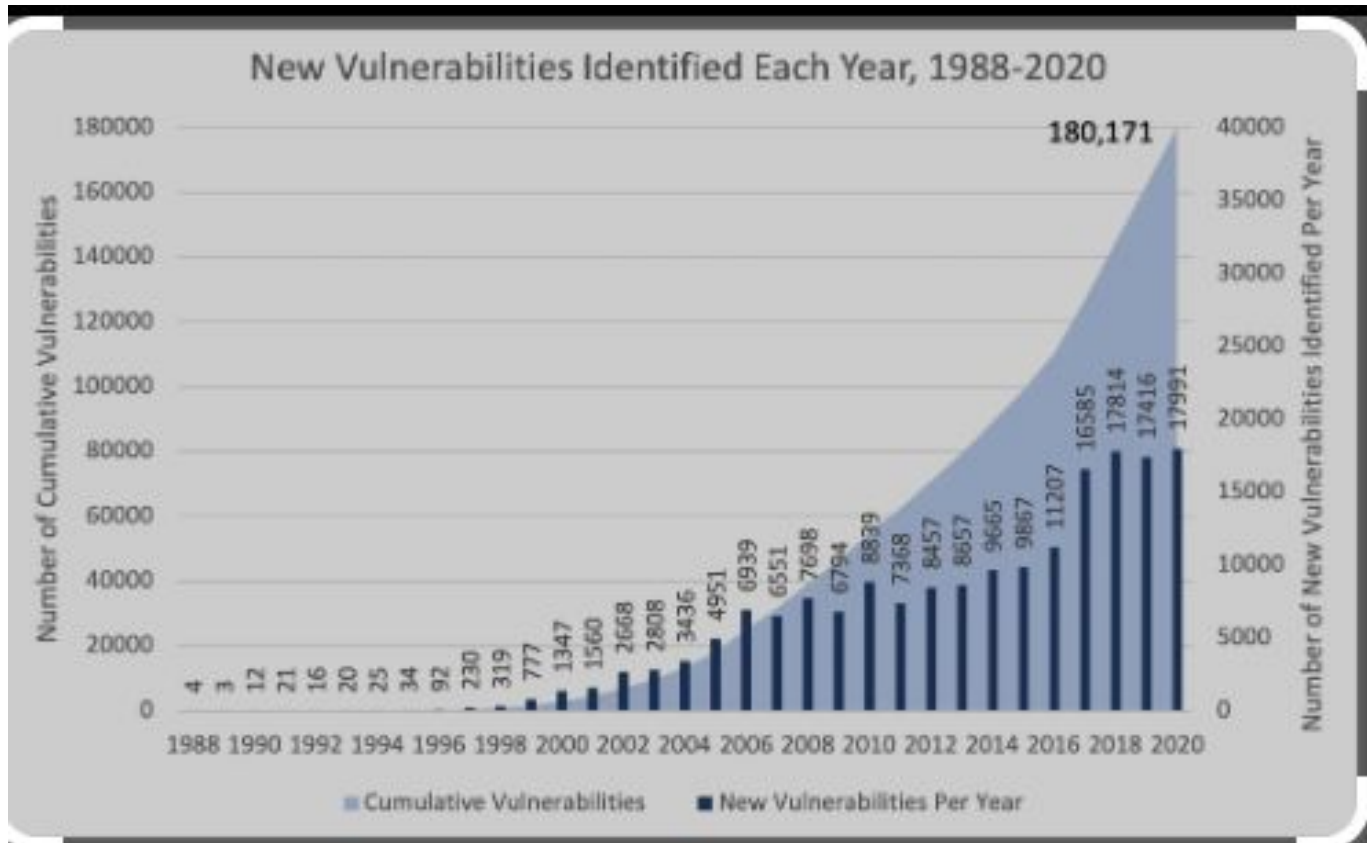


- Security Trends
- Security Attacks
- Security Services
- Security Mechanisms
- A Model of Network Security

Security Trends



Security Trends



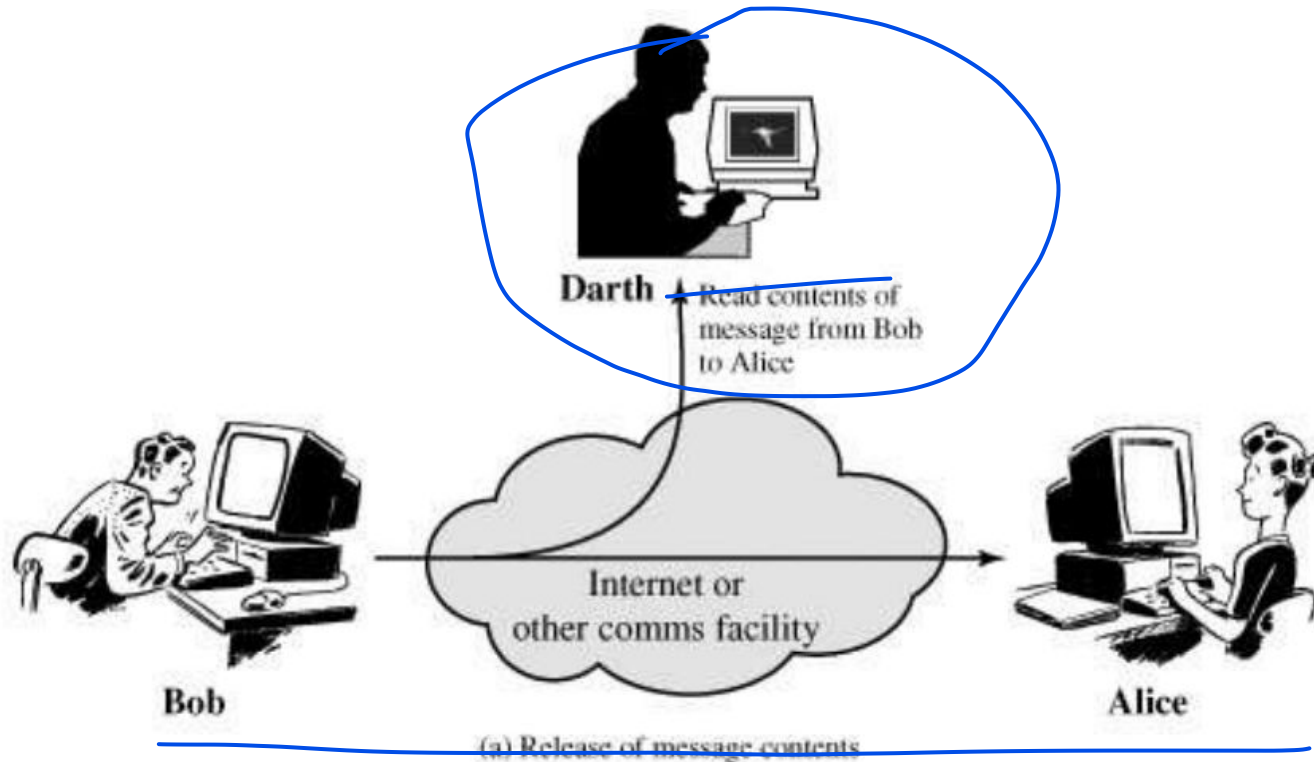
Security Trends

- Greater IOT vulnerabilities
- Ransomware attack damage
- Data manipulation Attacks
- Extortion Attacks

Security Attacks

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

a. Release of message contents



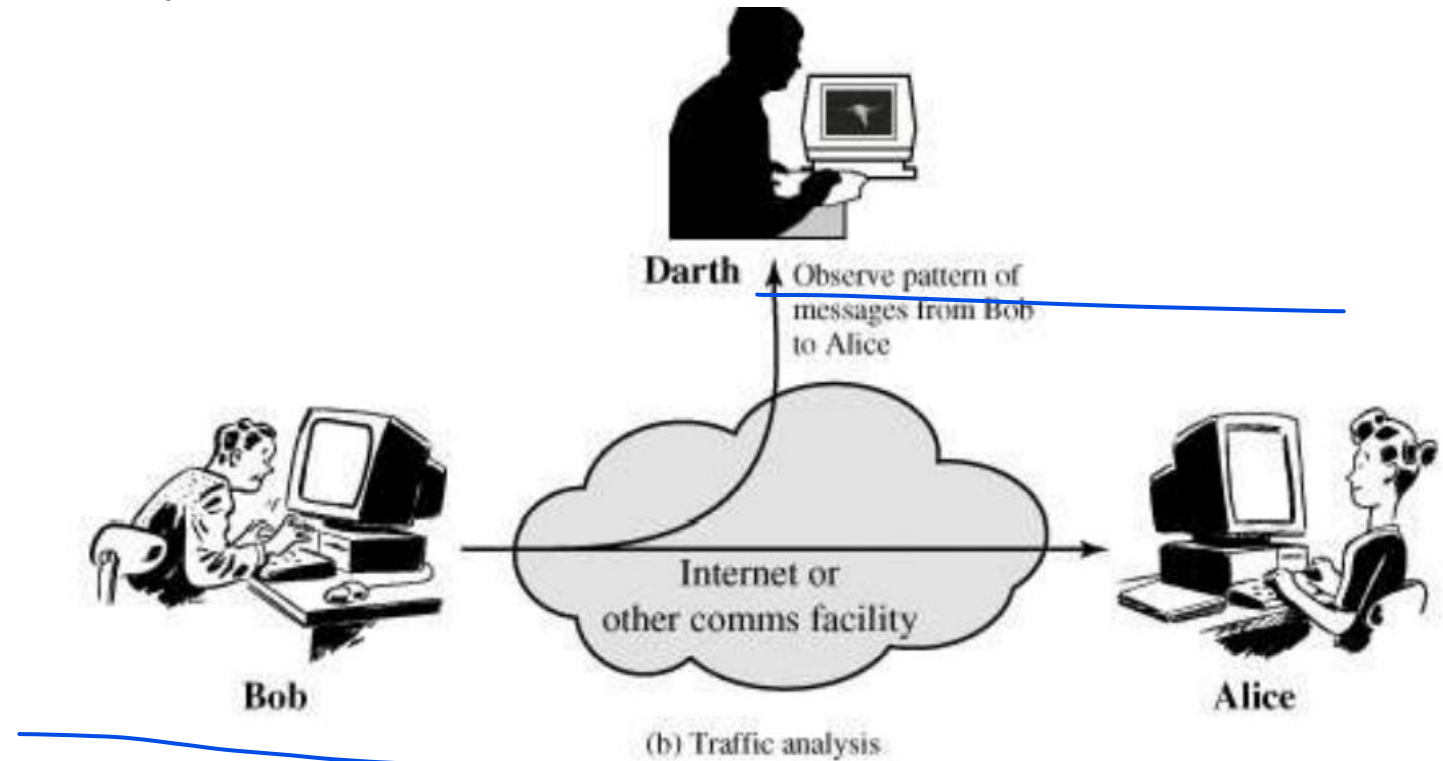
Collect
acquire
info

Security Attacks

Traffic Analysis:-

If we had a way of masking the contents of messages or other traffic information so that opponents cannot get it, even if they have captured the message, could not extract the information from message.

The common method for masking the contents is Encryption

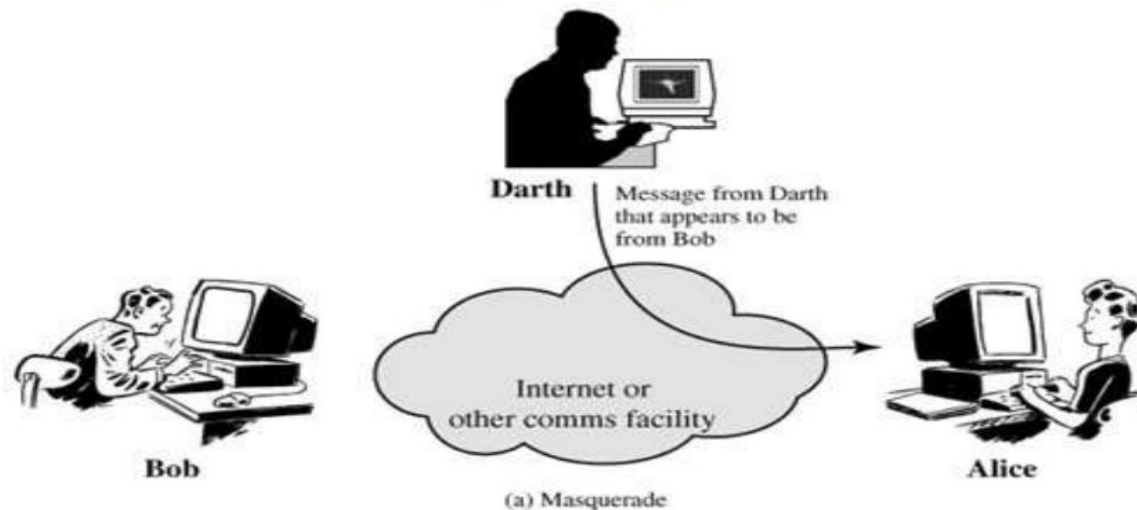


Active Attacks

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

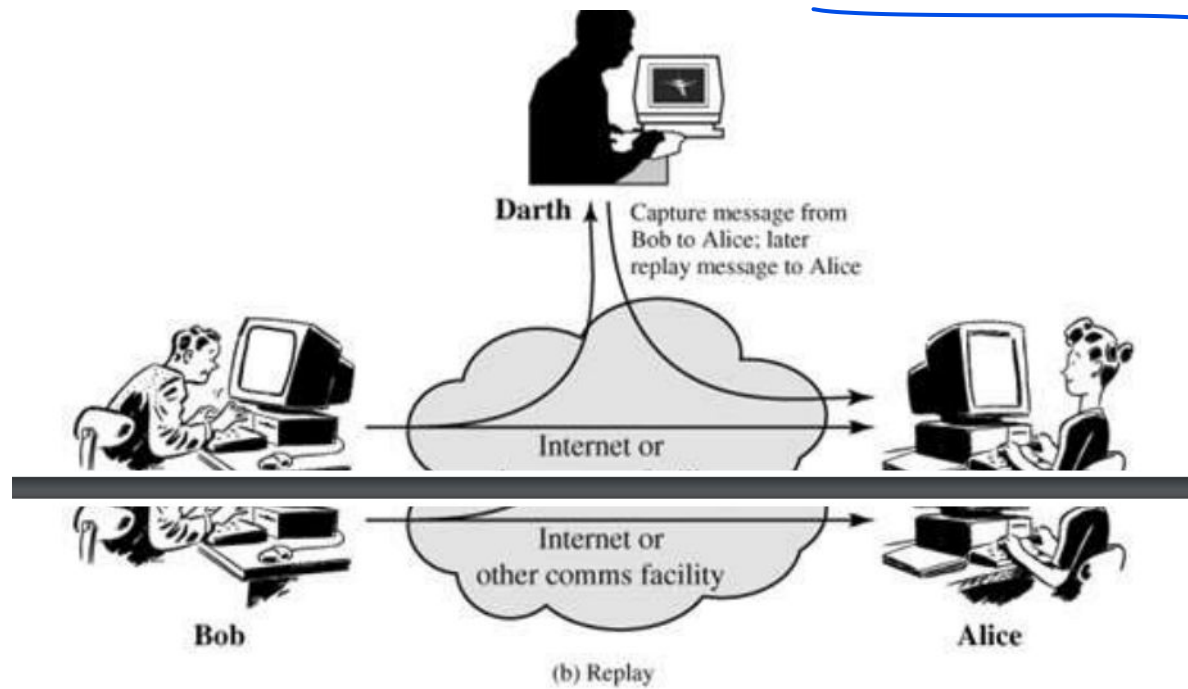
A masquerade takes place when one entity pretends to be a different entity. A masquerade attack usually includes one of the other forms of active attack.

For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.



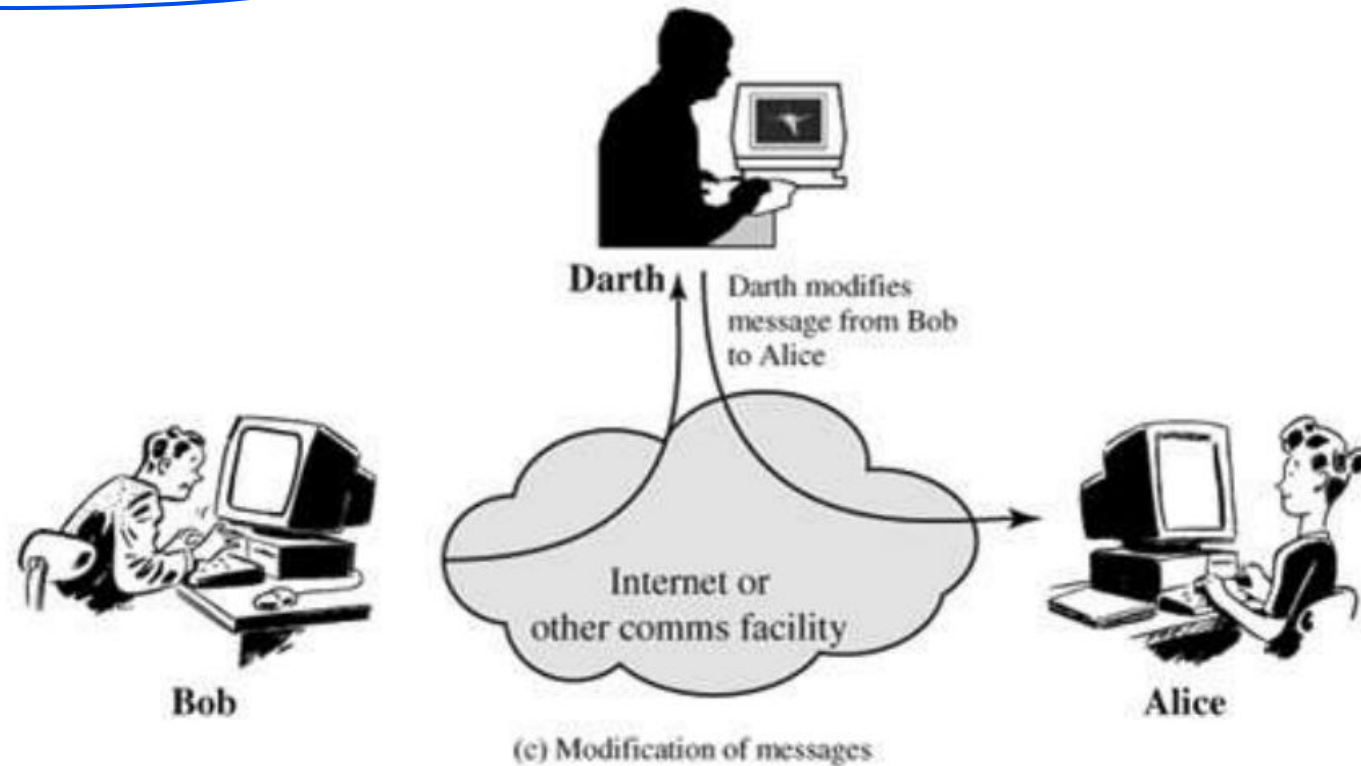
Active Attacks

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



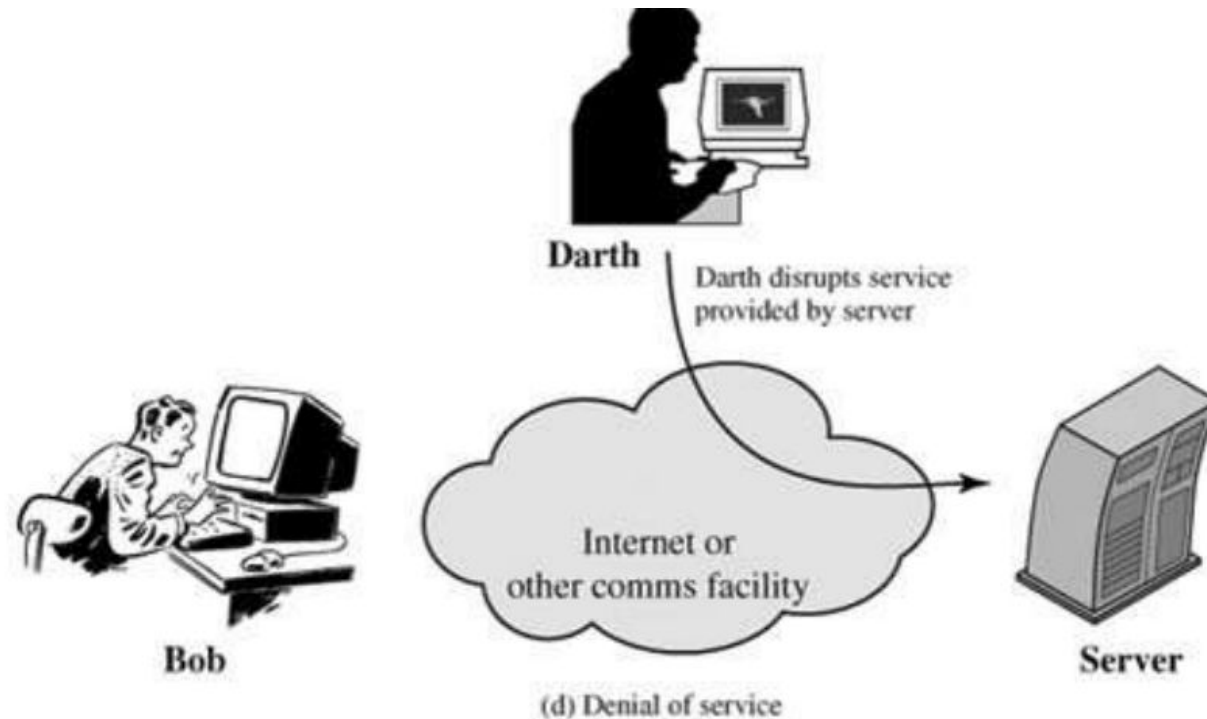
Active Attacks

Modification of messages simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect. For example, a message meaning "Allow John Smith to read confidential file accounts" is modified to mean "Allow Fred Brown to read confidential file accounts."



Active Attacks

The **denial of service** prevents or inhibits the normal use or management of communications facilities. This attack may have a specific target; for example, an entity may suppress all messages directed to a particular destination (e.g., the security audit service). Another form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance.



Security Services

X.800 defines a security service as a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers.

Security Services

- Authentication: The assurance that the communicating entity is the one that it claims to be
 - a. Peer Entity Authentication
 - b. Data Origin Authentication
- Access Control: The prevention of unauthorized use of a resource(Who can access to resource, under what conditions..)
- Data Confidentiality:- The protection of data from unauthorized disclosure
 - a. Connection Confidentiality
 - b. Connectionless Confidentiality
 - c. Selective-Field Confidentiality
 - d. Traffic Flow Confidentiality

Security Services

- Integrity: The assurance that data received is exactly as sent by an authorized entity (contain no modification, insertion, deletion..)
 - a. Connection Integrity with Recovery
 - b. Connection Integrity without Recovery
 - c. Selective-Field Connectionless Integrity
 - d. Connectionless Integrity
 - e. Selective –Field Connectionless Integrity
- Nonrepudiation: Provides protection against denial by one of the entities involved in a communication of having participated in all or part of communication.
 - a. Nonrepudiation ,Origin
 - b. Nonrepudiation, Destination

Security Mechanisms

Security mechanism X.800 defines a security service as a service.

Specific Security Mechanism

- Encipherment:- The use of mathematical algorithm to transfer data into a form that is not readily intelligible. The transformation and recovery of the data depend on an algorithm and zero or more encryption keys.
- Digital Signature:- Data appended to, or cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of data unit and protect against forgeries.
- Access Control:- A variety of mechanisms to enforce access rights to resources.
- Data Integrity:- A variety of mechanisms used to assure the integrity of data unit.
- Authentication Exchange:- A mechanism intended to ensure the identity of an entity by means of information exchange.
- Traffic Padding:- The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.

Security Mechanisms

Specific Security Mechanism

- Routing Control: Enables selection of particular physically secure routes for certain data and allows routing changes, when a breach of security suspected.
- Notarization: The use of a trusted party to assure certain properties of a data exchange.

Security Mechanisms

Pervasive Security Mechanism:- Mechanism that are not specific to any particular protocol layer.

- Trusted Functionality
- Security Label
- Event Detection
- Security Audit Trail
- Security Recovery

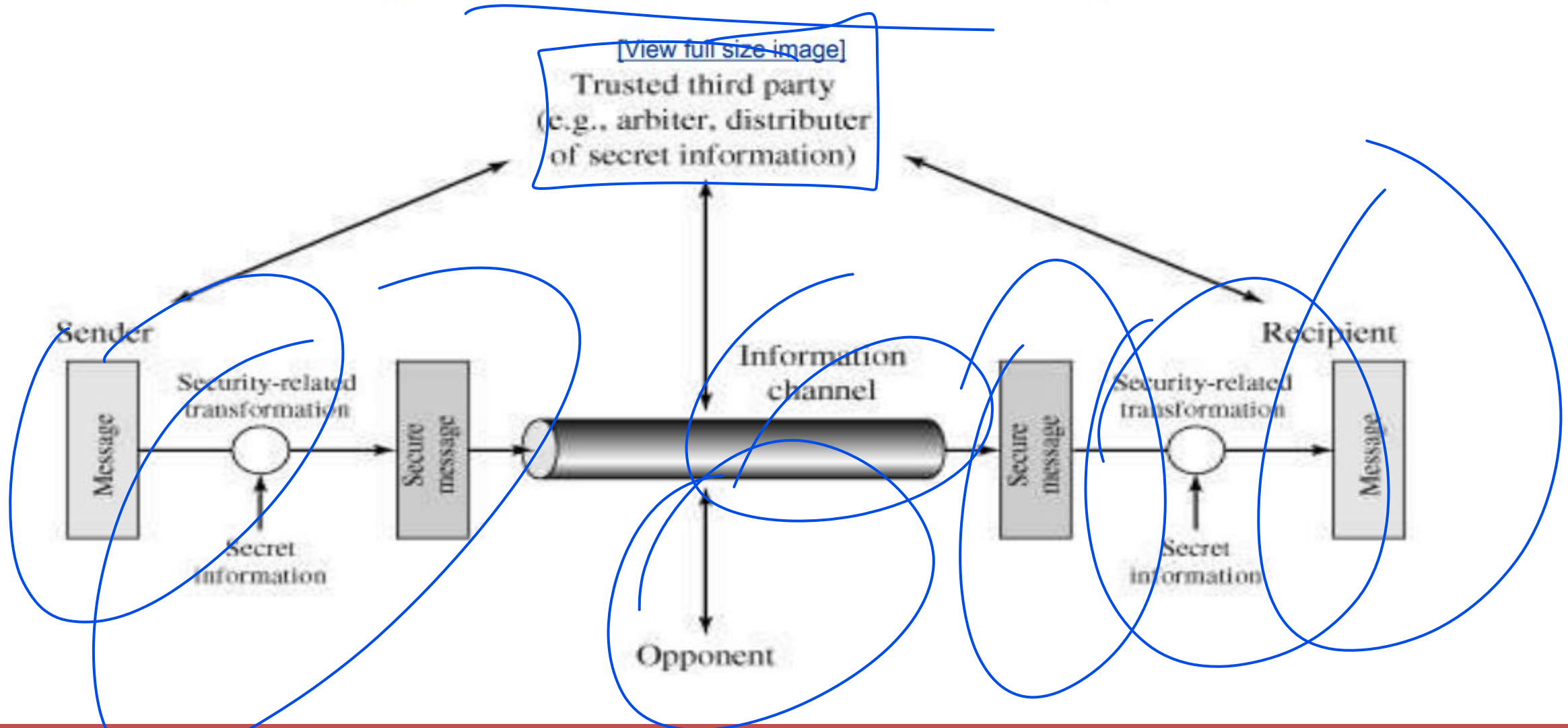
Security Mechanisms

Table 1.4. Relationship between Security Services and Mechanisms

| Mechanism | | | | | | | | |
|------------------------------|--------------|-------------------|----------------|----------------|-------------------------|-----------------|-----------------|--------------|
| Service | Encipherment | Digital Signature | Access Control | Data Integrity | Authentication Exchange | Traffic Padding | Routing Control | Notarization |
| Peer entity authentication | Y | Y | | | Y | | | |
| Data origin authentication | Y | Y | | | | | | |
| Access control | | | Y | | | | | |
| Confidentiality | Y | | | | | | Y | |
| Traffic flow confidentiality | Y | | | | | Y | Y | |
| Data integrity | Y | Y | | Y | | | | |
| Nonrepudiation | | Y | | Y | | | | Y |
| Availability | | | | Y | Y | | | |

Model for Network Security

Figure 1.5. Model for Network Security



Model for Network Security

1. Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose.
2. Generate the secret information to be used with the algorithm.
3. Develop methods for the distribution and sharing of the secret information.
4. Specify a protocol to be used by the two principals that makes use of the security algorithm and the secret information to achieve a particular security service.

Model for Network Security

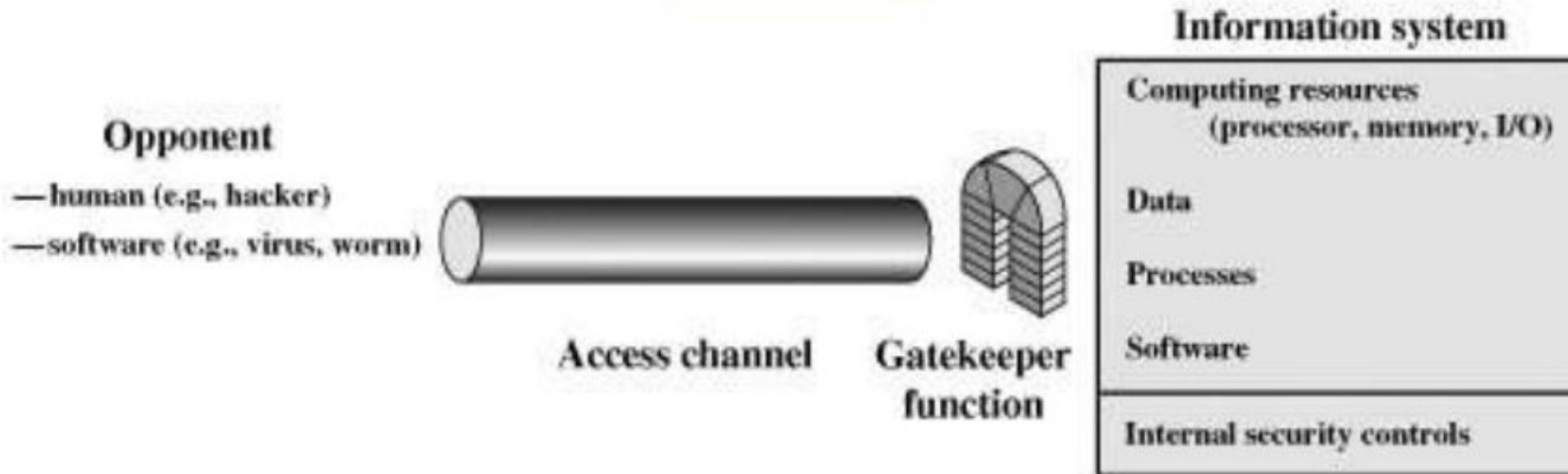
A message is to be transferred from one party to another across some sort of internet. The two parties, who are the principals in this transaction, must cooperate for the exchange to take place. A logical information channel is established by defining a route through the internet from source to destination and by the cooperative use of communication protocols (e.g., TCP/IP) by the two principals.

A security-related transformation on the information to be sent. Examples include the encryption of the message, which scrambles the message so that it is unreadable by the opponent, and the addition of a code based on the contents of the message, which can be used to verify the identity of the sender.

- Some secret information shared by the two principals and, it is hoped, unknown to the opponent. An example is an encryption key used in conjunction with the transformation to scramble the message before transmission and unscramble it on reception.

Figure 1.6. Network Access Security Model

[\[View full size image\]](#)



Classical Encryption Techniques

Symmetric Cipher Model

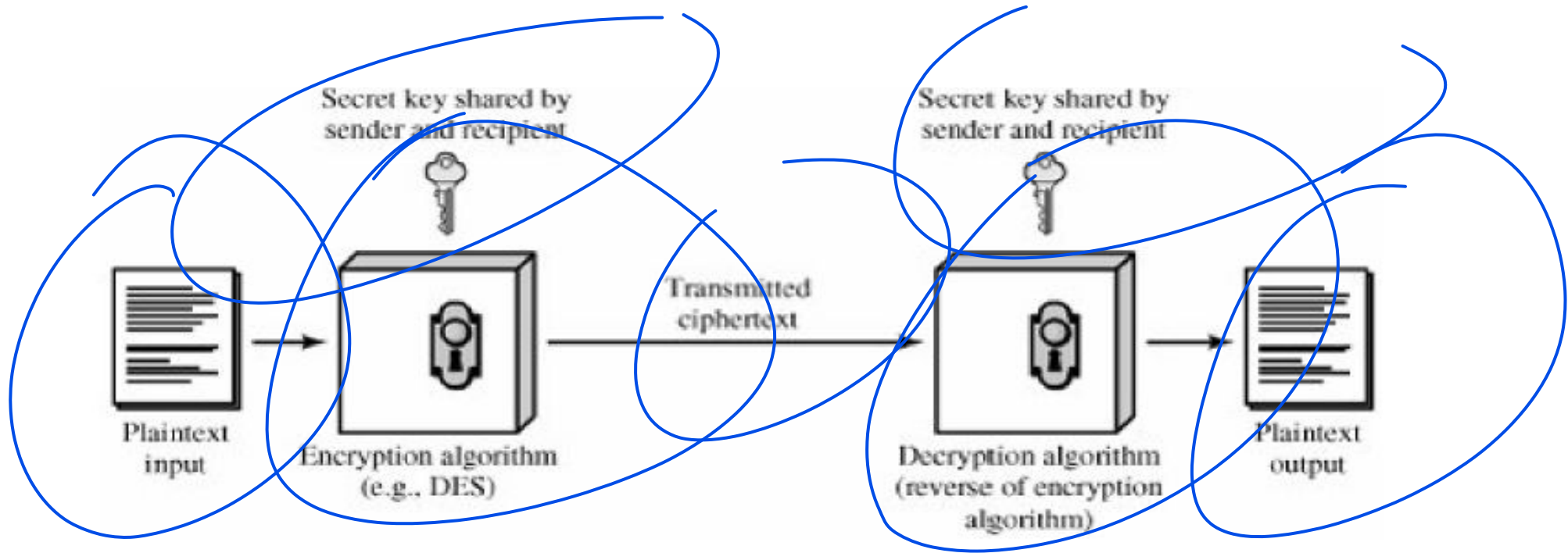


Fig: A simplified model of conventional Encryption

Classical Encryption Techniques

Symmetric Cipher Model

Plaintext: This is the original intelligible message or data that is fed into the algorithm as input.

Encryption algorithm: The encryption algorithm performs various substitutions and transformations on the plaintext.

Secret key: The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key.

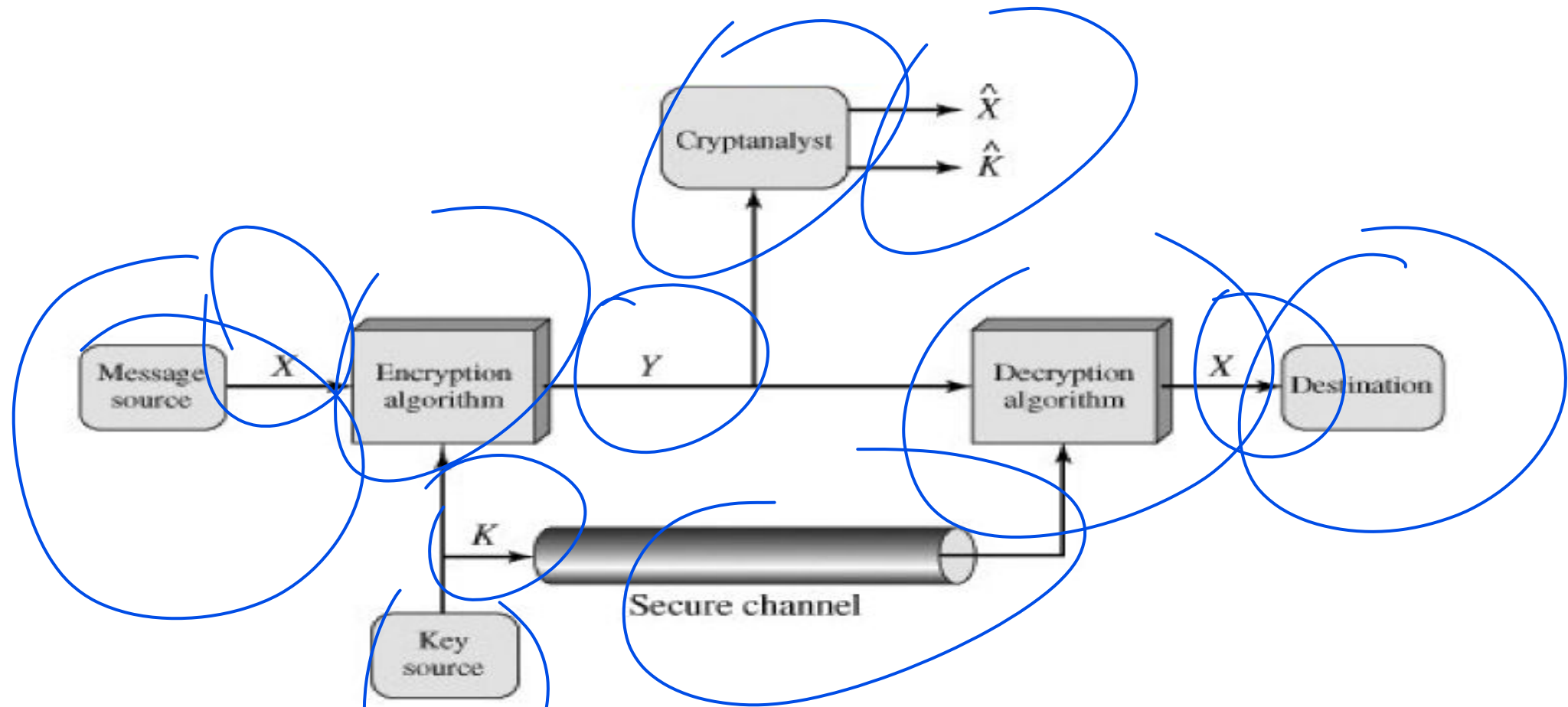
Ciphertext: This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts. The ciphertext is an apparently random stream of data and as it stands, is unintelligible.

Decryption algorithm: This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

Symmetric Cipher Model

Two requirements for the Secure use of Conventional Encryption:

1. We need strong encryption algorithm. The opponent should be unable to decrypt ciphertext or discover the key even if he or she is in possession of a number of ciphertexts together with the plaintext that produced each ciphertext.
2. The Sender and Receiver must obtain the same copies of the secret key in a secure fashion and keep the key secure.



A Model of Conventional Crypto System

Cryptography

Cryptographic Systems are characterized along 3 independent dimensions:

- The type of operations used for transforming plaintext to ciphertext
- The number of keys used
- The way in which plaintext is processed

Cryptanalysis

Two general approaches for attacking conventional encryption scheme

- Cryptanalysis
- Brute Force Attack

Table 2.1. Types of Attacks on Encrypted Messages

| Type of Attack | Known to Cryptanalyst |
|-------------------|--|
| Ciphertext only | <ul style="list-style-type: none">● Encryption algorithm● Ciphertext |
| Known plaintext | <ul style="list-style-type: none">● Encryption algorithm● Ciphertext● One or more plaintext-ciphertext pairs formed with the secret key |
| Chosen plaintext | <ul style="list-style-type: none">● Encryption algorithm● Ciphertext● Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key |
| Chosen ciphertext | <ul style="list-style-type: none">● Encryption algorithm● Ciphertext● Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key |

Chosen text

- Encryption algorithm
- Ciphertext
- Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
- Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

Imp things to remember:

- An encryption scheme is **unconditionally secure** if the ciphertext generated by the scheme does not contain enough information to determine uniquely the corresponding plaintext, no matter how much ciphertext is available

The users of Encryption Algorithm strive for an algorithm must meet at least one or both of following criteria, if they are met algorithm is **computationally secure**.

- The cost of breaking the cipher exceeds the value of the encrypted information.
- The time required to break the cipher exceeds the useful lifetime of the information.

Substitution Techniques

- A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols.
- If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns.

Caesar Ciphers

The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet.

For example,

plain: meet me after the toga party

cipher: PHHW PH DIWHU WKH WRJD SDUWB

Let us assign a numerical equivalent to each letter:

| | | | | | | | | | | | | |
|----|----|----|----|----|----|----|----|----|----|----|----|----|
| a | b | c | d | e | f | g | h | i | j | k | l | m |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| n | o | p | q | r | s | t | u | v | w | x | y | z |
| 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

Caesar Ciphers

The algorithm

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

A shift may be of any amount, so that the general Caesar algorithm is

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

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

Monoalphabetic Ciphers

With only 25 possible keys, the Caesar cipher is far from secure. A dramatic increase in the key space can be achieved by allowing an arbitrary substitution.

Frequency Analysis

- Suppose we have a long ciphertext, the challenge is to decipher it.
- Let us know the text is in English and has been encrypted using a monoalphabetic substitution cipher.

Searching all possible keys is impractical as the key space is of size $26!$

Monoalphabetic Ciphers

Ciphertext:-

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

P 13.33

H 5.83

F 3.33

B 1.67

C 0.00

Z 11.67

D 5.00

W 3.33

G 1.67

K 0.00

S 8.33

E 5.00

Q 2.50

Y 1.67

L 0.00

U 8.33

V 4.17

T 2.50

I 0.83

N 0.00

O 7.50

X 4.17

A 1.67

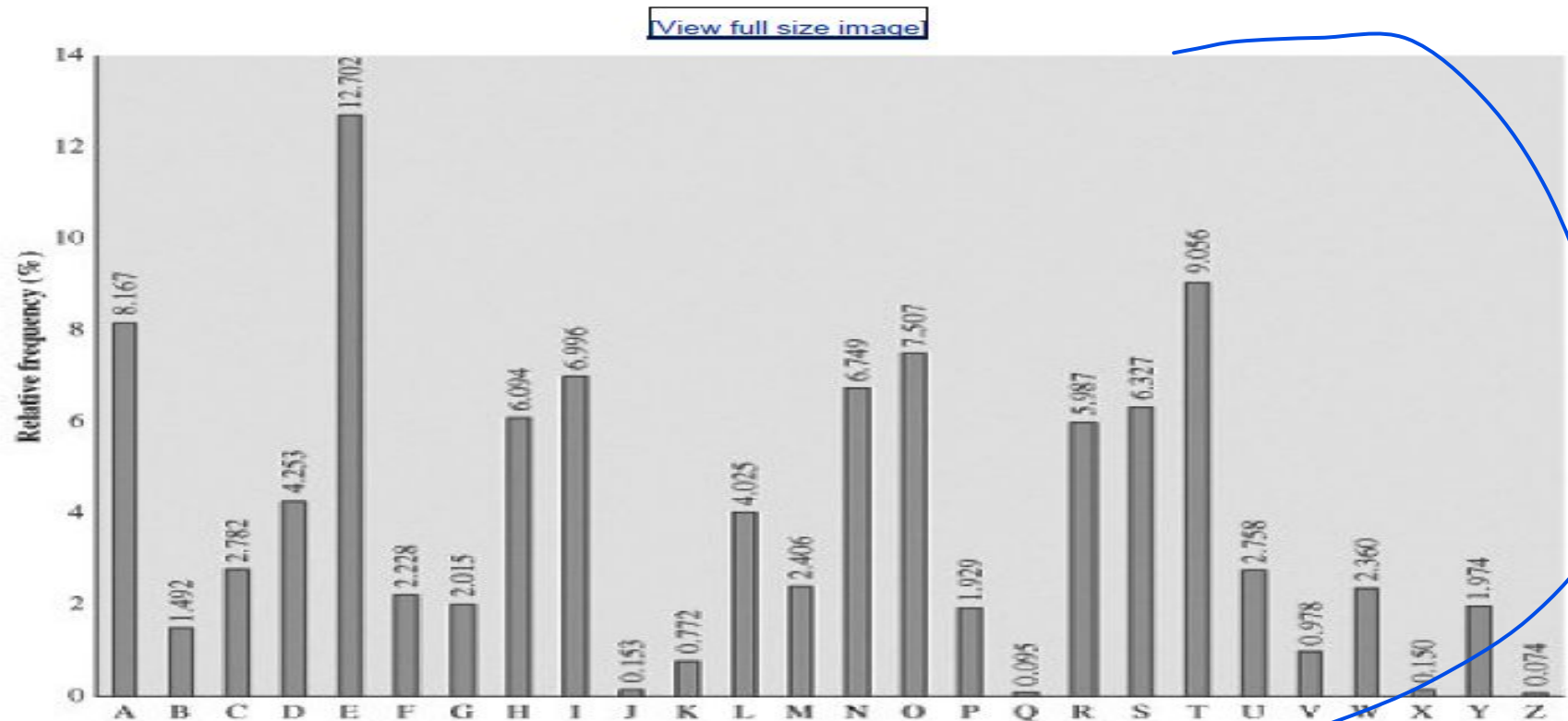
J 0.83

R 0.00

M 6.67

As a first step, the relative frequency of the letters can be determined and compared to a standard frequency distribution for English, such as is shown in below figure

Figure 2.5. Relative Frequency of Letters in English Text



- cipher letters P and Z are the equivalents of plain letters e and t, but it is not certain which is which.
- The letters S, U, O, M, and H are all of relatively high frequency and probably correspond to plain letters from the set {a, h, i, n, o, r, s}.
- The letters with the lowest frequencies (namely, A, B, C, Y, I, J) are likely included in the set {b, j, k, q, v, x, z}.
- A powerful tool is to look at the frequency of two-letter combinations, known as digrams.
- The most common such digram is th. In our ciphertext, the most common digram is ZW, which appears three times. So we make the correspondence of Z with t and W with h. Then, by our earlier hypothesis, we can equate P with e.
- Now ZWP replaced with "the" trigram(three letter combination)

Monoalphabetic ciphers

Decrypted Text:

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

- Monoalphabetic ciphers are easy to break because they reflect the frequency data of the original alphabet.
- A countermeasure is to provide multiple substitutes, known as homophones, for a single letter.
- For example, the letter e could be assigned a number of different cipher symbols, such as 16, 74, 35, and 21, with each homophone used in rotation, or randomly.

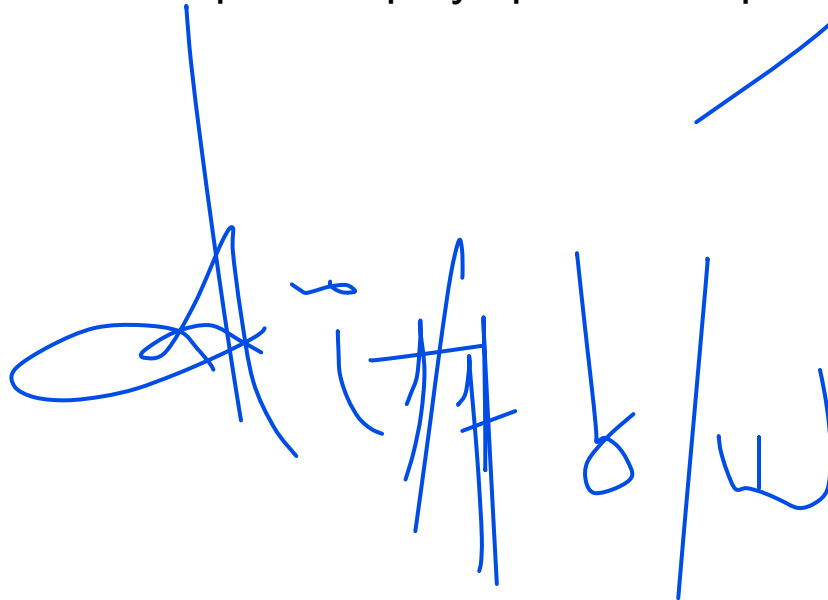
Polyalphabetic ciphers

1. Monoalphabetic Cipher:

A monoalphabetic cipher is any cipher in which the letters of the plain text are mapped to cipher text letters based on a single alphabetic key. Examples of monoalphabetic ciphers would include the Caesar-shift cipher, where each letter is shifted based on a numeric key, where each letter is mapped to the letter symmetric to it about the center of the alphabet.

2. Polyalphabetic Cipher :

A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets. The Playfair and Vigenère cipher is probably the best-known example of a polyalphabetic cipher, though it is a simplified special case.

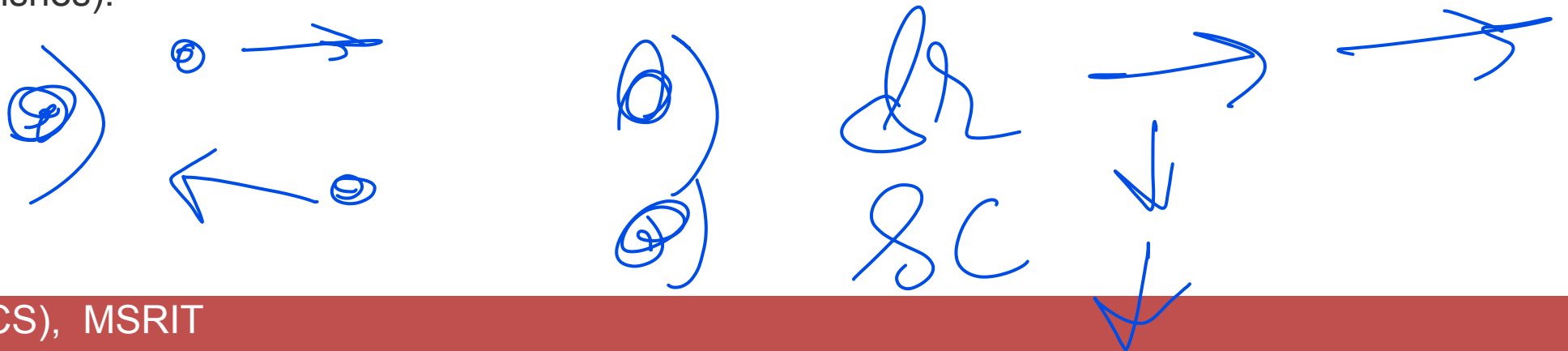
Handwritten blue ink scribbles and lines, possibly representing a signature or a stylized logo, located at the bottom center of the slide.

Playfair Cipher—Multi alphabet substitution Cipher

- The best-known multiple-letter encryption cipher is the Playfair, which treats digrams in the plaintext as single units and translates these units into ciphertext digrams.
- The Playfair algorithm is based on the use of a 5 x 5 matrix of letters constructed using a keyword.
- The best-known multiple-letter encryption cipher is the Playfair, which treats digrams in the plaintext as single units and translates these units into ciphertext digrams.

Rules for playfair cipher

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



Playfair Cipher

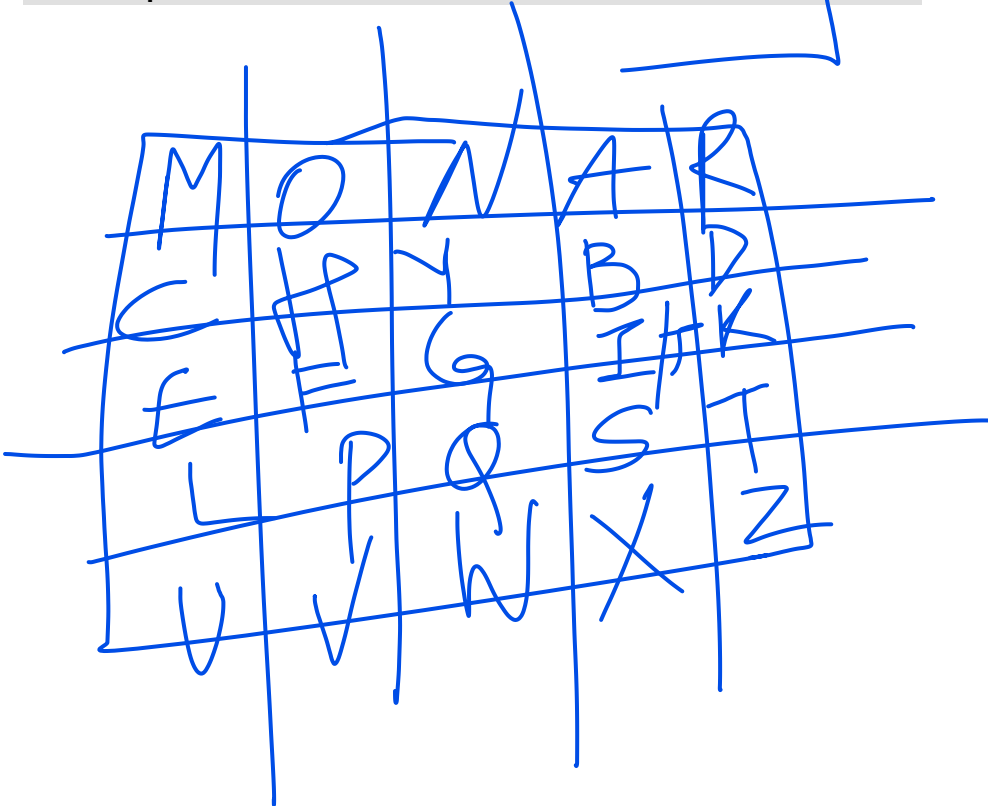
Keyword—Monarchy

Message(Plaintext)—Instruments

PlainText: "instruments"

After Split: 'in' 'st' 'ru' 'me' 'nt' 'sz'

in st ru me nt sz



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

Playfair Cipher

in:

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

st:

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

ru:

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

me:

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

nt:

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

sz:

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

Ciphertext is : GATLMZCLRQTX

Vigenere Cipher

- Vigenere Cipher is a method of encrypting alphabetic text.
- It uses a simple form of polyalphabetic substitution. A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets.
- The encryption of the original text is done using the Vigenère square or Vigenère table.

Input text:- hellostudents

Keyword:- cyber

The keyword is repeated in the circular manner until it matches the length of the plaintext.

Vigenere Cipher

[View full size image](#)

| | | Plaintext | | | | | | | | | | | | | | | | | | | | | | | | | |
|-----|---|-----------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| Key | a | 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 |
| | b | 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 | A |
| | c | C | 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 |
| | d | 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 |
| | e | 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 | D |
| | f | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E |
| | g | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F |
| | h | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G |
| | i | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H |
| | j | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I |
| | k | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J |
| | l | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K |
| | m | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L |
| | n | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M |
| | o | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N |
| | p | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
| | q | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P |
| | r | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q |
| | s | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R |
| | t | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S |
| | u | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T |
| | v | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U |
| | w | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V |
| | x | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W |
| | y | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X |
| | z | Z | 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 |

Vigenere Cipher

Encryption:

The first letter of the plaintext, h is paired with c, the first letter of the key. So use row h and column c of the Vigenère square, namely J. Similarly, for the second letter of the plaintext, the second letter of the key is used, the letter at row e, and column y is c. The rest of the plaintext is enciphered in a similar fashion.

JCMPFURVHVPRT

Decryption:

Decryption is performed by going to the row in the table corresponding to the key, finding the position of the ciphertext letter in this row, and then using the column's label as the plaintext. For example, in row c(from cyber), the ciphertext J appears in column h.

Vigenere Cipher

Encryption

The plaintext(P) and key(K) are added modulo 26.

$$E_i = (P_i + K_i) \bmod 26$$

Decryption

$$D_i = (E_i - K_i) \bmod 26$$

Hill Cipher

Hill cipher is a polygraphic substitution cipher based on linear algebra. Each letter is represented by a number modulo 26. Often the simple scheme $A = 0, B = 1, \dots, Z = 25$ is used, but this is not an essential feature of the cipher.

To encrypt a message, each block of n letters is multiplied by an invertible $n \times n$ matrix, against modulus 26.

To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption.

The matrix used for encryption is the cipher key, and it should be chosen randomly from the set of invertible $n \times n$ matrices (modulo 26)

Hill Cipher

Input : Plaintext: ACT

Key: GYBNQKURP

Output : Ciphertext: POH

GYBNQKURP:

Handwritten: Yet
Vid

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$

ACT

$$\begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix}$$

Hill Cipher

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} = \begin{bmatrix} 67 \\ 222 \\ 319 \end{bmatrix} \equiv \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} \pmod{26}$$

Hill Cipher

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \stackrel{-1}{\equiv} \begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \pmod{26}$$

the previous Ciphertext 'POH':

$$\begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} \equiv \begin{bmatrix} 260 \\ 574 \\ 539 \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} \pmod{26}$$

One Time pad

The two requirements for the One-Time pad are

- The key should be **randomly generated as long as the size of the message.**
- The key is to be **used to encrypt and decrypt a single message, and then it is discarded.**

Consider a ciphertext

ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS

We now show two different decryptions using two different keys:

ciphertext: ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS

key: ~~pxlmvmsydfuyrvzwc tnlebnecvgdupahfzzlmnyih~~

plaintext: mr mustard with the candlestick in the hall

ciphertext: ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS

key: ~~mfugpmiydgaxgoufhklmhsqdqogtewbqfgyovuhwt~~

plaintext: miss scarlet with the knife in the library

One Time Pad

Advantages

One time pad algorithm is truly breakable and can be used for low bandwidth channels requiring high security.

Disadvantages:

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

Transposition Techniques

A very different kind of mapping is achieved by performing some sort of permutation on the plaintext letters. This technique is referred to as a transposition cipher.

For example, to encipher the message "meet me after the toga party"

The encrypted message is

MEMATRHTGPRYETEFETEOAAT

This sort of thing would be trivial to cryptanalyze. 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. The order of the columns then becomes the key to the algorithm. For example,

Key: 4 3 1 2 5 6 7

Plaintext: a t t a c k p

o s t p o n e

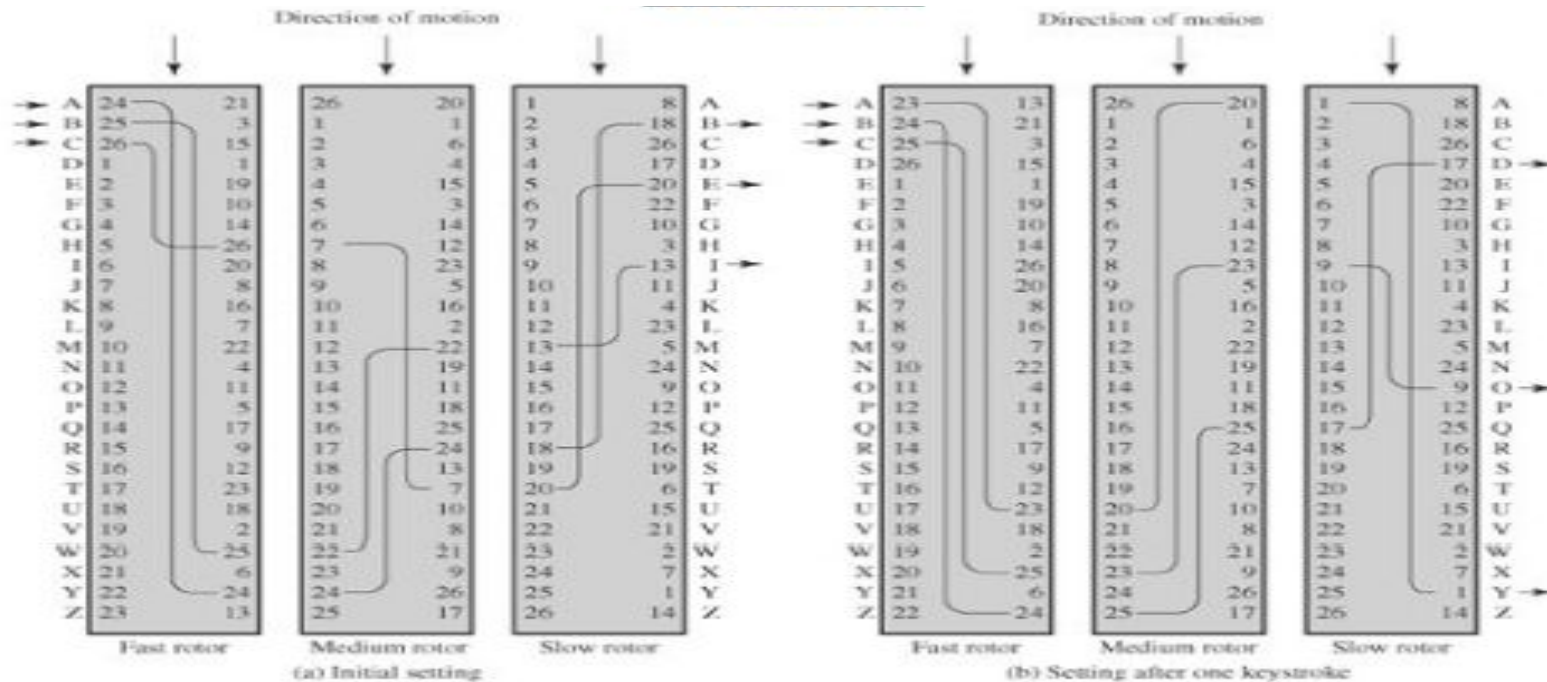
d u n t i l t

w o a m x y z

Ciphertext: TTNAAPTMTSUOAODWCOIXKNLYPETZ

Rotor machines

Multiple stages of encryption is represented by Rotor Machines. The machine consists of a set of independently rotating cylinders through which electrical pulses can flow. Each cylinder has 26 input pins and 26 output pins, with internal wiring that connects each input pin to a unique output pin. For simplicity, only three of the internal connections in each cylinder are shown



Three Rotor machine represented with wiring represented by numbered contacts

Rotor machines

If we associate each input and output pin with a letter of the alphabet, then a single cylinder defines a monoalphabetic substitution.

For example, in Figure 2.7, if an operator depresses the key for the letter A, an electric signal is applied to the first pin of the first cylinder and flows through the internal connection to the twenty-fifth output pin.

Consider a machine with a single cylinder. After each input key is depressed, the cylinder rotates one position, so that the internal connections are shifted accordingly. Thus, a different monoalphabetic substitution cipher is defined. After 26 letters of plaintext, the cylinder would be back to the initial position. Thus, we have a polyalphabetic substitution algorithm with a period of 26.

The power of the rotor machine is in the use of multiple cylinders, in which the output pins of one cylinder are connected to the input pins of the next.

Figure 2.7 shows a three-cylinder system. The left half of the figure shows a position in which the input from the operator to the first pin (plaintext letter a) is routed through the three cylinders to appear at the output of the second pin (ciphertext letter B).

The result is that there are $26 \times 26 \times 26 = 17,576$ different substitution alphabets used before the system repeats. The addition of fourth and fifth rotors results in periods of 456,976 and 11,881,376 letters, respectively.

Steganography

- The steganography technique involves hiding sensitive information within an ordinary, non-secret file or message so that it will not be detected.
- The sensitive information will then be extracted from the ordinary file or message at its destination, thus avoiding detection.
- Steganography is an additional step that can be used in conjunction with encryption in order to conceal or protect data.

A plaintext message may be hidden in one of two ways.

- The methods of steganography conceal the existence of the message.
- whereas the methods of cryptography render the message unintelligible to outsiders by various transformations of the text

Steganography

Examples:

Character marking: Selected letters of printed or typewritten text are overwritten in pencil. The marks are ordinarily not visible unless the paper is held at an angle to bright light.

Invisible ink: A number of substances can be used for writing but leave no visible trace until heat or some chemical is applied to the paper.

Pin punctures: Small pin punctures on selected letters are ordinarily not visible unless the paper is held up in front of a light.

Typewriter correction ribbon: Used between lines typed with a black ribbon, the results of typing with the correction tape are visible only under a strong light.