I: INTRODUCTION

Ms. Stevina Correia

Security Goals

- Information is an asset that has value as any other asset.
- As an asset, information needs to be secured from attacks.
- To be secured, information needs to be:
  - Hidden from unauthorized access (**confidentiality**)
  - Protected from unauthorized change (**integrity**)
  - Available to an authorized entity only (**availability**)

- Until a few decades information was stored in physical files.
- **Confidentiality** was achieved by restricting access to few authorized and trusted people in the organization
- Similarly, only few people authorized people were allowed to change the contents of the file
- Availability was achieved by designating at least one person who has access to the files at all times

- Information storage has now become electronic. It is now stored on computers and is distributed as well.
- Information can be send and received through computer networks.
- The 3 security goals did not change but have some new dimensions

OSI Security Architecture

- The OSI security architecture is useful to managers as a way of organizing the task of providing security.
- The OSI 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 (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.
- Examples of common security mechanisms are as follows:
- Cryptography
- Message digests and digital signatures
- Digital certificates
- Public Key Infrastructure (PKI)

- Security service: A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization.
- The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

Network Security Services

- Data Integrity
- Data Confidentiality
- Authenticity
- Non-repudiation
- Access Control

Threats and Attacks on Information

- A threat is a potential violation of security and causes harm.
- A threat can be a malicious program, a natural disaster or a thief.
- Threat is a possible danger that might exploit vulnerability; the actions that cause it to occur are the security attacks.
- *Vulnerability* is a weakness of system that is left unprotected. Systems that are vulnerable are exposed to threats.
- For example,
  - if we leave the house lock open—it is **vulnerable to theft**;
  - an intruder in our locality (might exploit the open lock)—is a security threat;
  - the intruder comes to know of the open lock and gets inside the house—This is a security attack.

Cryptographic attacks

- Cryptographic attacks:
  - Cryptanalytic: combination of statistical and algebraic techniques.
  - Non-Cryptanalytic: threatens the 3 security goals of security namely confidentiality, integrity and availability

Threat to confidentiality

Snooping: Snooping, in a security context, is unauthorized access to another person's or company's data.

- The practice is similar to eavesdropping but is not necessarily limited to gaining access to data during its transmission.
- Snooping can include casual observance of an e-mail that appears on another's computer screen or watching what someone else is typing.
- More sophisticated snooping uses software programs to remotely monitor activity on a computer or network device.

Traffic Analysis: Traffic analysis is the process of intercepting and examining messages in order to deduce information from patterns in communication.

- It can be performed even when the messages are encrypted and cannot be decrypted. In general, the greater the number of messages observed, or even intercepted and stored, the more can be inferred from the traffic.

Threat to integrity

- **Modification:** An attacker can modify the transmitted information, without needing to know the actual content.
  - Example: change DB values, alter credit card record, change grades etc
  - Customer sends message to the bank for some transaction. Attacker intercepts and changes the type of transaction

- **Masquerading:** An attacker can modify the communication data to pretend (spoof) as a legal sender or receiver to obtain the information to which it does not have access.
  - User contacting a bank. Another party pretends to be the bank and obtains some information

- **Replaying:** An attacker copies a message sent by a different user and replays later.
  - User sends login information over the network to the server (authentication system). Attacker intercepts the message and replays it again

- **Repudiation:** performed by 1 of the parties involved in the communication
  - Sender of a message may later deny that it has sent it.
    - Example, a user may deny a third party payment request.
  - A receiver of a data may also refuse the receipt.
    - Example, a merchant may refuse the receipt of a credit card payment.

- It is obvious, that cryptography should guarantee non-repudiation in these applications

Threat to availability

- **Denial of Service (DoS):** Slow down or totally disable the system.
  - Example: slow down the system with multiple requests.
  - delete the acknowledgements from the server

Security Attacks: Passive and Active attacks

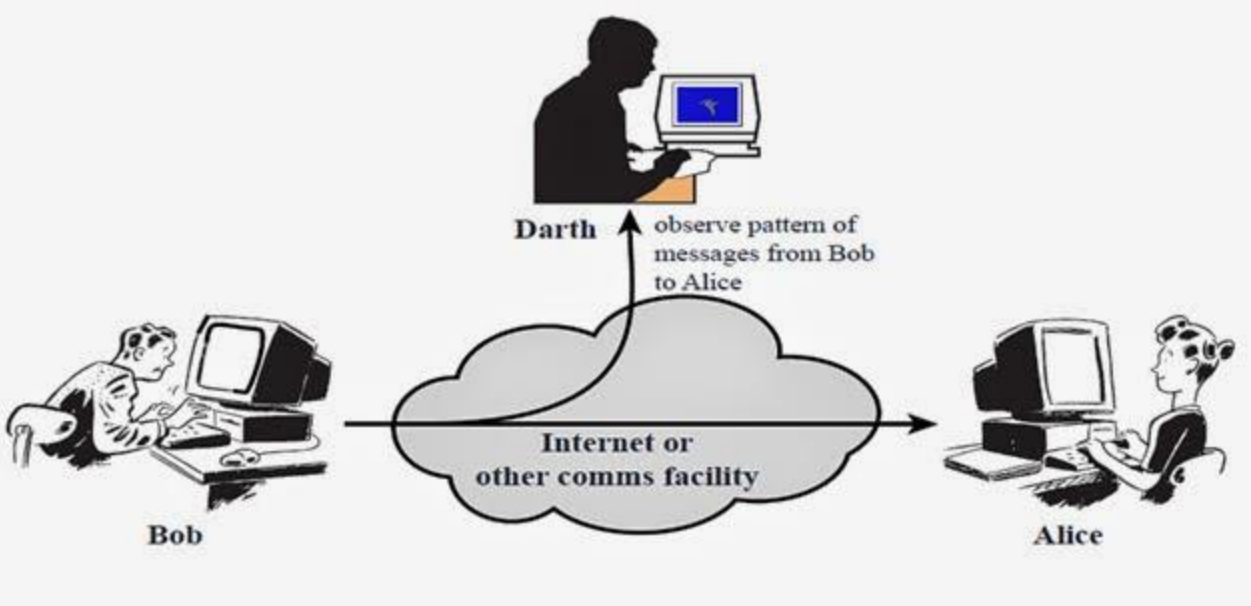
Attacks	Passive/Active	Threatening
Snooping Traffic Analysis	Passive	Confidentiality
Modification, masquerading, replaying, repudiation	Active	Integrity
DoS	Active	Availability

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.
- Two types of passive attacks are
  - release of message contents
  - traffic analysis

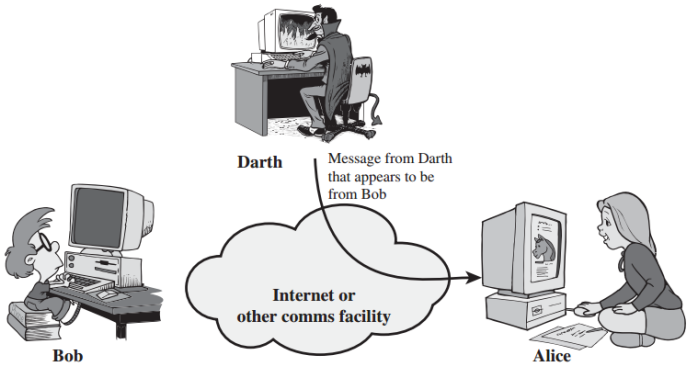
Release of Message Contents

Traffic Analysis

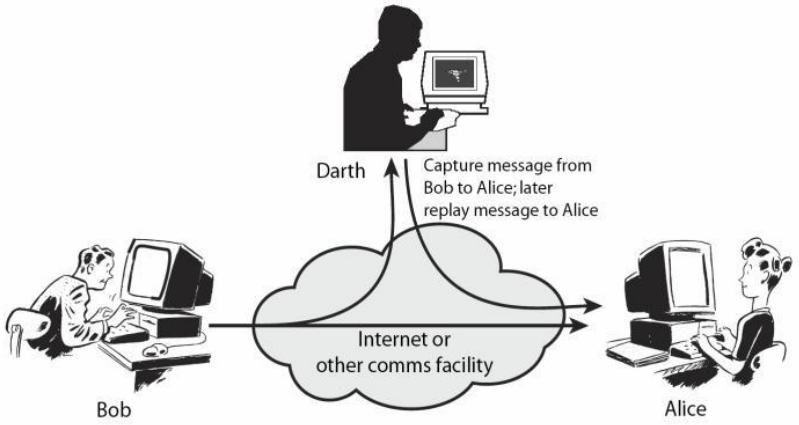


Active Attacks

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

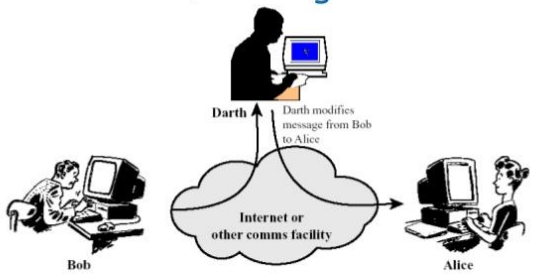


Masquerade

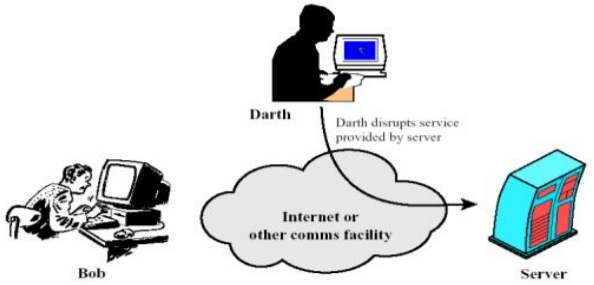


Replay

Active Attacks: Modification of Messages



Active Attacks: Denial of Service

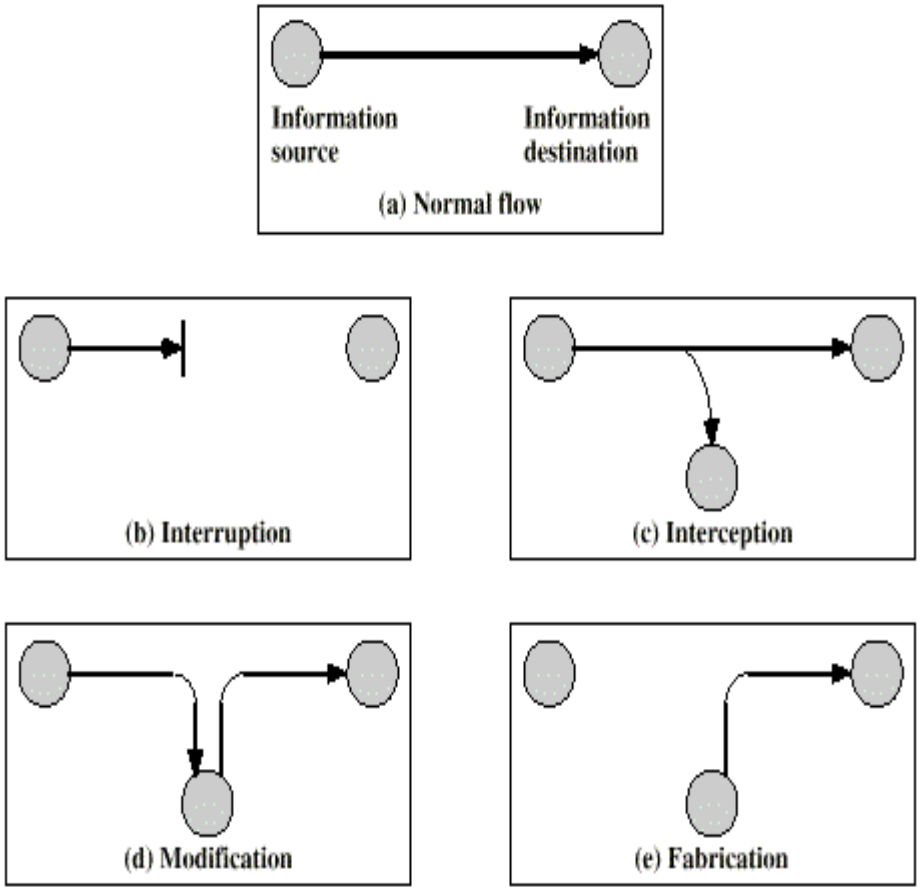


Passive attacks	Active attacks
Attacker's goal is to obtain information. Does not modify data or harm the system. May harm sender/ receiver of message. It does not harm or modify the system.	Attacker may harm or modify the system.
Attacks that threaten confidentiality are passive attacks	Attacks that threaten integrity and availability are active attacks
Difficult to detect because they do not involve any alteration of the data. Can be prevented by encryption of data.	Easier to detect than prevent (attacker can launch in a number of ways)
Emphasis is on prevention rather than detection	Goal is to detect and recover

- Another way of looking at security in computer systems is that we attempt to protect the services and data it offers against security threats
- There are four types of security threats to consider (Pfleeger, 1997):
  1. Interception
  2. Interruption
  3. Modification
  4. Fabrication

System Security Threats

- B)Interruption: threat against availability
- C)Interception: threat against confidentiality
- D)Modification: threat against integrity
- E)Fabrication: threat against integrity



Security Services

- Processing or communication service that is provided by a system to give a specific kind of protection to system resources; security services implement security policies and are implemented by security mechanisms.
  - Authentication
  - Access Control
  - Data Confidentiality
  - Data Integrity
  - Nonrepudiation
  - Availability Service

Authentication

- The assurance that the communicating entity is the one that it claims to be.
- **Peer Entity Authentication**
  - Used in association with a logical connection to provide confidence in the identity of the entities connected.
  - It attempts to provide confidence that an entity is not performing either a masquerade or an unauthorized replay of a previous connection.

- **Data-Origin Authentication**
  - In a connectionless transfer, provides assurance that the source of received data is as claimed.

ACCESS CONTROL

- The prevention of unauthorized use of a resource.
- This service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do.

DATA CONFIDENTIALITY

- The protection of data from unauthorized disclosure.
- The protection of transmitted data from passive attacks.
- With respect to the content of a data transmission
  - service may protect all user data transmitted between two users over a period of time, protection of a single message or even specific fields within a message
- Other aspect of confidentiality is the protection of traffic flow from analysis
  - attacker not be able to observe the source and destination, frequency, length, or other characteristics of the traffic

- **Connection Confidentiality**
  - The protection of all user data on a connection.
- **Connectionless Confidentiality**
  - The protection of all user data in a single data block
- **Selective-Field Confidentiality**
  - The confidentiality of selected fields within the user data on a connection or in a single data block.
- **Traffic-Flow Confidentiality**
  - The protection of the information that might be derived from observation of traffic flows.

Data Integrity

- The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).
  - **Connection Integrity with Recovery**
  - **Connection Integrity without Recovery**
  - **Selective-Field Connection Integrity**
  - **Connectionless Integrity**
  - **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 the communication.
- **Nonrepudiation, Origin**
  - Proof that the message was sent by the specified party.
- **Nonrepudiation, Destination**
  - Proof that the message was received by the specified party.

Availability Service

- Property of a system or a system resource being accessible and usable upon demand by an authorized system entity

Security Mechanisms

- Mechanisms provide security services.
- Mechanisms are divided into those that are implemented in a specific protocol layer, such as TCP or an application-layer protocol, and those that are not specific to any particular protocol layer or security service.
- A reversible encipherment mechanism is simply an encryption algorithm that allows data to be encrypted and subsequently decrypted.
- Irreversible encipherment mechanisms include hash algorithms and message authentication codes, which are used in digital signature and message authentication applications.

Mechanisms

- **Encipherment**
- **Digital Signature**
- **Access Control**
- **Data Integrity**
- **Authentication Exchange**
- **Traffic Padding**
- **Routing Control**
- **Notarization**

- **Encipherment**
  - 2 techniques
    - Cryptography (very general)
    - Steganography (very specific)
- **Data Integrity**
  - Produces a small check sum for a large message.
  - It is usually appended and sent with the message.
  - If the message is modified, then the receiver computes the hash value and checks for a match.

- **Digital Signature**
  - Sender can electronically sign data and receiver can electronically verify the signature.

- **Authentication Exchange**
  - 2 entities exchange some messages to prove their identity
    - An entity may prove she knows the secret key that only she is supposed to know.

- **Traffic padding**
  - Inserting some bogus data into the traffic to thwart the adversary's attempt to use traffic analysis

- **Routing Control**
  - Changing route to prevent opponent from eavesdropping on a particular route
- **Notarization**
  - Selecting a 3rd party (trusted) to control the communication
  - Can be used to prevent repudiation
- **Access Control**
  - Methods to prove user has access rights
    - Passwords and PINs

Relationship Between Security Services and Mechanisms

SERVICE \ MECHANISM	Enchipherment	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			

Types of Cryptographic Algorithms

1. Symmetric Key Ciphers/ single key/ secret-key/ conventional:
   - The sender and the receiver share the same piece of key (secret) for their message exchange.

2. Asymmetric Key Ciphers (2 key/ public key encryption):
   - The sender encrypts the message using receiver's public key and the receiver decrypts using his own secret (or private) key.
   - Secret (key) is personal (unshared)

3. Hash Functions:
   - Produces a small check sum for a large message.
   - It is usually appended and sent with the message.
   - If the message is modified, then the receiver computes the hash value and checks for a match.

Some Basic Terminology

- **plaintext** - original message
- **ciphertext** - coded message
- **cipher** - algorithm for transforming plaintext to ciphertext
- **key** - info used in cipher known only to sender/receiver
- **encipher (encrypt)** - converting plaintext to ciphertext
- **decipher (decrypt)** - recovering ciphertext from plaintext
- **cryptography** - study of encryption principles/methods
- **cryptanalysis (codebreaking)** - study of principles/ methods of deciphering ciphertext *without* knowing key
- **cryptology** - field of both cryptography and cryptanalysis

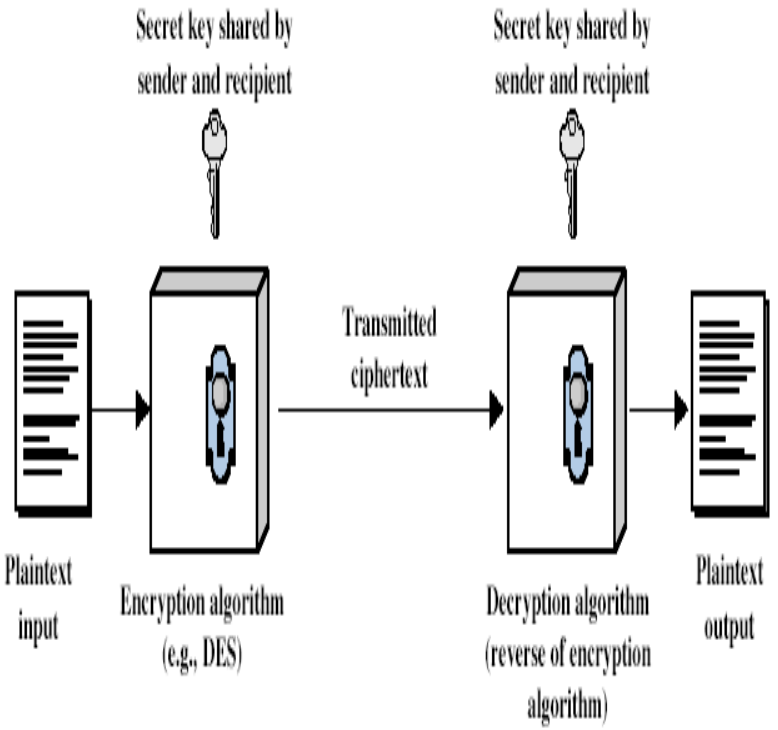
Symmetric Key Encryption

- Classic/ conventional / private-key / single-key
- sender and recipient share a common key
- two requirements for secure use of symmetric encryption:
  - a strong encryption algorithm
  - a secret key known only to sender / receiver
- mathematically have:

  $Y = E_K(X)$ [= E(K, X)]

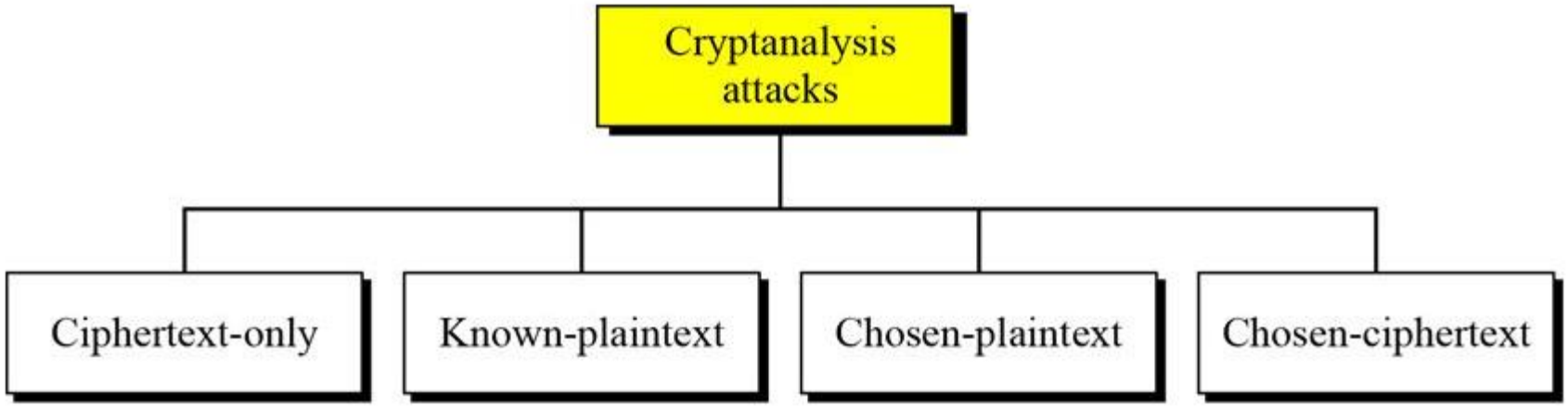
  $X = D_K(Y)$ [= D(K, Y)]

  plaintext X, ciphertext Y, key K, encryption algorithm E_K, decryption algorithm D_K.
- Often are **block-ciphers**

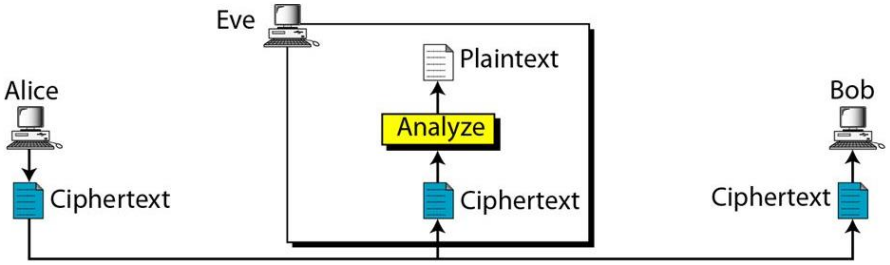


- Kerckhoff's Principle:
  - Assume that adversary knows the encryption algorithm.
  - Guessing the key should be so difficult that there is no need to hide the algorithm

Cryptanalysis

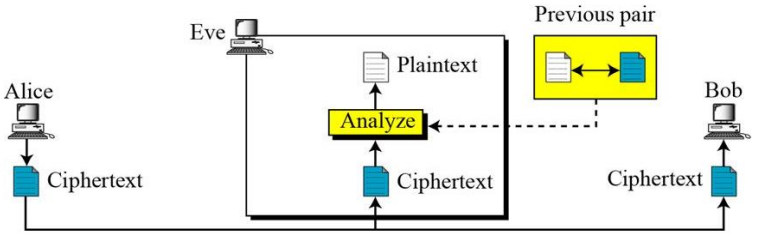


Ciphertext-Only Attack



- Brute Force
  - Use all possible keys
- Statistical Attack
  - Benefit from inherent characteristics of plaintext
  - Hide characteristics of the language
- Pattern Attack

Known-Plaintext Attack



- Eve has access to some plaintext/ciphertext pairs in addition to the intercepted ciphertext

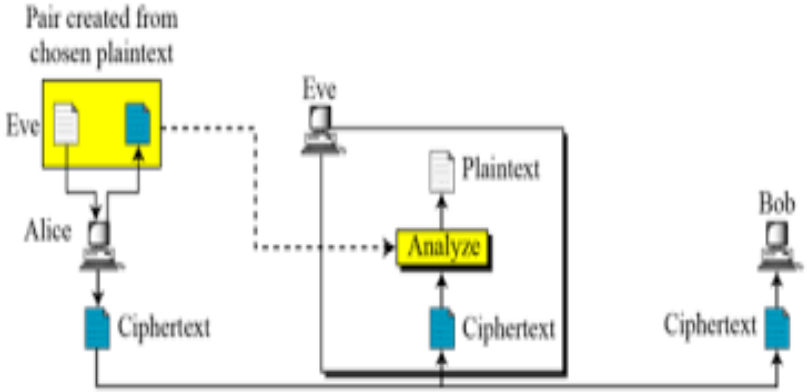
- Eg of brute force attack
- Eve has intercepted the following ciphertext. Using a statistical attack, find the plaintext.

XLILSYWIMWRSAJSVWEPIJSVJSYVQMPPMSRHSPPEVWMXMWASVX-LQSVILY-
VVCFIJSVIXLIWIPPIVVIGIMZIWQSVISJJIVW

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

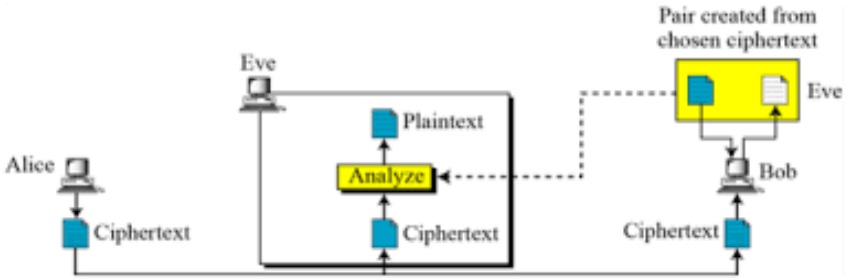
the house is now for sale for four million dollars it is worth more hurry before the seller receives more offers

Chosen-plaintext attack



- Similar to known plaintext attack but plaintext/ ciphertext pairs are chosen by attacker

Chosen ciphertext



- Similar to chosen plaintext attack, eve choses some ciphertext and decrypts to form ciphertext/ plaintext pair

Table 2.1 Types of Attacks on Encrypted Messages

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

Classic Encryption Techniques (traditional)

- Substitution Ciphers
  - Mono-alphabetic Ciphers
    - Additive/ shift (k=3 Caesar cipher,k=15 etc)
    - Multiplicative Ciphers
    - Affine (combination of additive and multiplicative)
    - Monoalphabetic substitution cipher
  - Poly-alphabetic Ciphers
    - Autokey
    - Playfair
    - Vigenere Cipher/ Vignere tableu
    - Hill Cipher
    - One time pad
    - Rotor cipher
    - Enigma machine
- Transposition Ciphers
  - Keyless
  - Keyed
  - Keyed columnar/columnar
- Double transposition ciphers

- Examples of different ciphers----refer to notebook/ notes

Cryptanalysis

Additive ciphers are vulnerable to ciphertext-only attacks using exhaustive key searches (brute-force attacks). The key domain of the additive cipher is very small; there are only 26 keys. However, one of the keys, zero, is useless (the ciphertext is the same as the plaintext). This leaves only 25 possible keys. Eve can easily launch a brute-force attack on the ciphertext.

The size of the key space for the monoalphabetic substitution cipher is 26! (almost 4×10^{26}). This makes a brute-force attack extremely difficult for Eve even if she is using a powerful computer. However, she can use statistical attack based on the frequency of characters. The cipher does not change the frequency of characters.

The autokey cipher definitely hides the single-letter frequency statistics of the plaintext. However, it is still as vulnerable to the brute-force attack as the additive cipher. The first subkey can be only one of the 25 values (1 to 25). We need polyalphabetic ciphers that not only hide the characteristics of the language but also have large key domains.

Cryptanalysis of a Playfair Cipher

Obviously a brute-force attack on a Playfair cipher is very difficult. The size of the key domain is 25! (factorial 25). In addition, the encipherment hides the single-letter frequency of the characters. However, the frequencies of diagrams are preserved (to some extent because of filler insertion), so a cryptanalyst can use a ciphertext-only attack based on the digram frequency test to find the key.

Vigenere ciphers, like all polyalphabetic ciphers, do not preserve the frequency of characters. However, Eve still can use some techniques to decipher an intercepted ciphertext. The cryptanalysis here consists of two parts: finding the length of the key and finding the key itself.

Ciphertext-only cryptanalysis of Hill ciphers is difficult. First, a brute-force attack on a Hill cipher is extremely difficult because the key is an $m \times m$ matrix. Each entry in the matrix can have one of the 26 values. At first glance, this means that the size of the key domain is $26^{m \times m}$. However, not all of the matrices have multiplicative inverses. The key domain is smaller, but still huge.

Cryptanalysis of Transposition Ciphers

Transposition ciphers are vulnerable to several kinds of ciphertext-only attacks.

Statistical Attack

A transposition cipher does not change the frequency of letters in the ciphertext; it only reorders the letters. So the first attack that can be applied is single-letter frequency analysis. This method can be useful if the length of the ciphertext is long enough. We have seen this attack before. However, transposition ciphers do not preserve the frequency of digrams and trigrams. This means that Eve cannot use these tools. In fact, if a cipher does not preserve the frequency of digrams and trigrams, but does preserve the frequency of single letters, it is probable that the cipher is a transposition cipher.

Brute-Force Attack

Eve can try all possible keys to decrypt the message. However, the number of keys can be huge ($1! + 2! + 3! + \cdots + L!$), where L is the length of the ciphertext. A better approach is to guess the number of columns. Eve knows that the number of columns divides L. For example, if the length of the cipher is 20 characters, then $20 = 1 \times 2 \times 2 \times 5$.

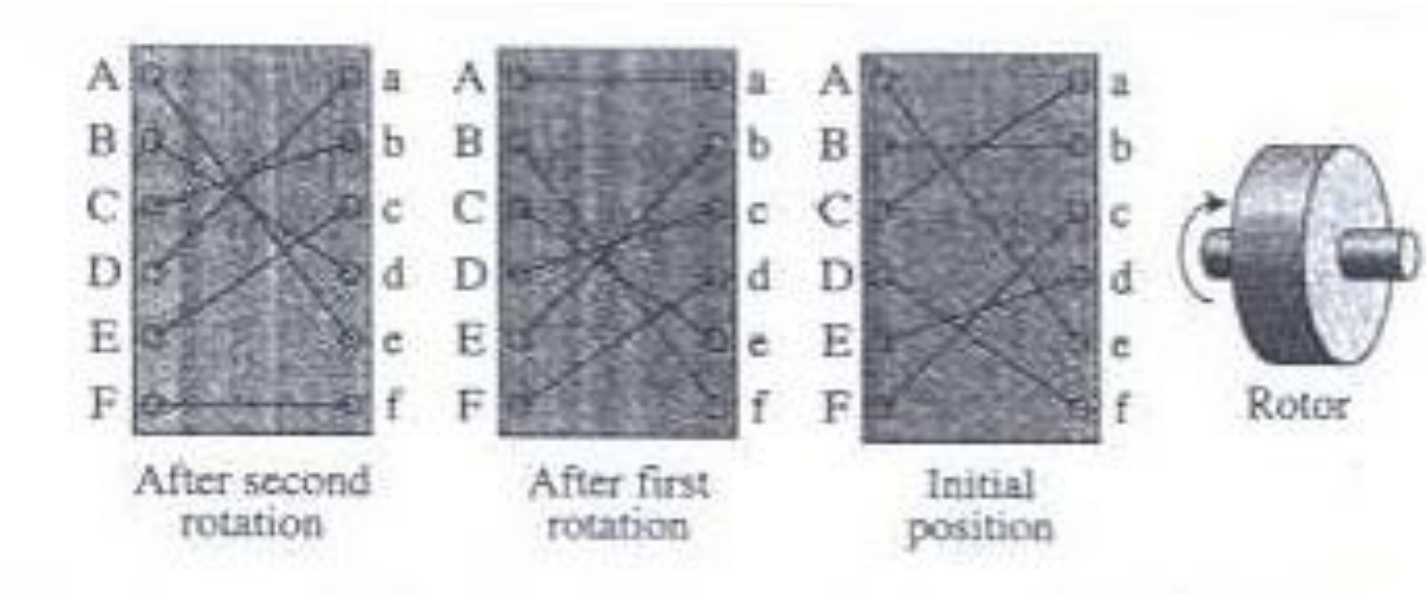
This means the number of columns can be a combination of these factors (1, 2, 4, 5, 10, 20). However, the first (only one column) is out of the question and the last (only one row) is unlikely.

One time Pad/ Vernam Cipher

- Similar to mono alphabetic substitution cipher.
- Key is randomly chosen each time as long as plaintext .
- Ciphertext only attack is impossible. So are other attacks.
- It’s a perfect cipher but impossible to implement commercially.
- Large quantities of random keys are required.
- Key distribution is a problem
- Suitable in some cases but not all-one time messages

Rotor Cipher

- Uses the idea behind mono alphabetic substitution but changes the mapping.
- bee-BAA (stationary)/ BCA(rotating)



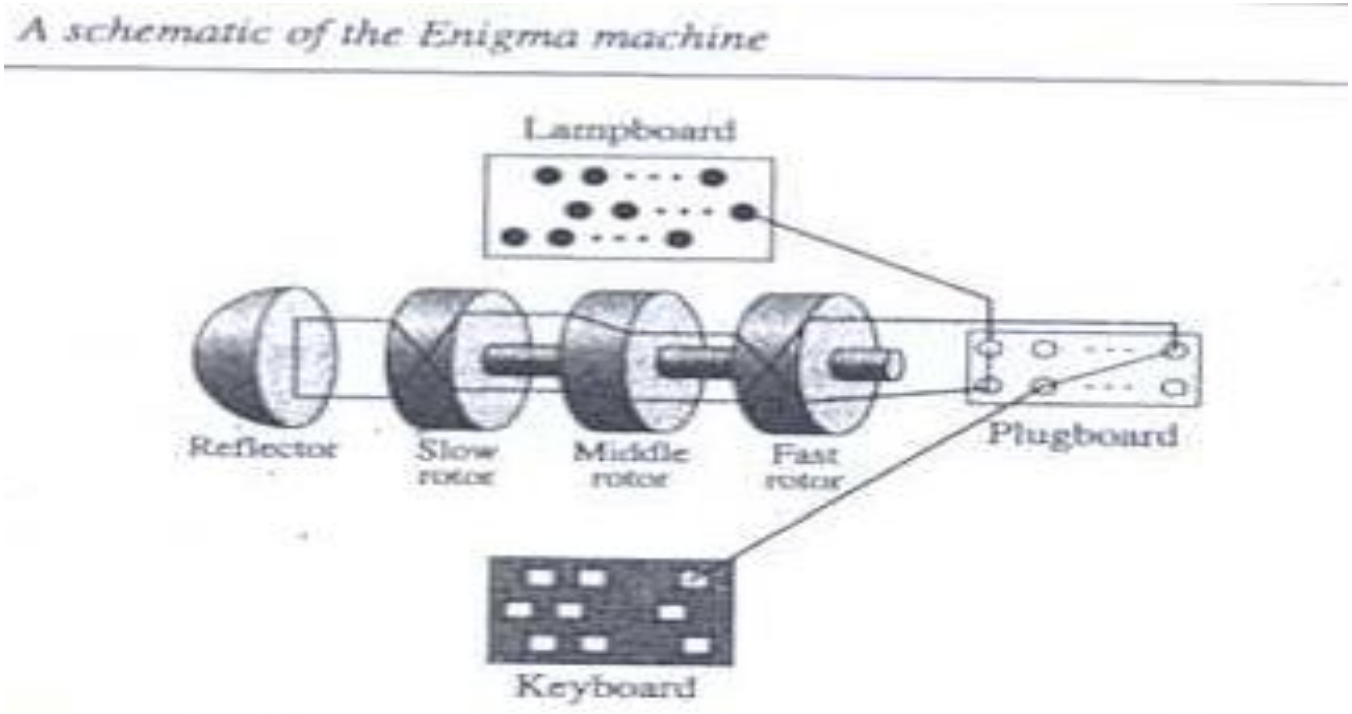
The rotor shown in Figure 3.19 uses only 6 letters, but the actual rotors use 26 letters. The rotor is permanently wired, but the connection to encryption/decryption characters is provided by brushes. Note that the wiring is shown as though the rotor were transparent and one could see the inside.

The initial setting (position) of the rotor is the secret key between Alice and Bob. The first plaintext character is encrypted using the initial setting; the second character is encrypted after the first rotation (in Figure 3.19 at 1/6 turn, but the actual setting is 1/26 turn); and so on.

The rotor cipher is as resistant to a brute-force attack as the monoalphabetic substitution cipher because Eve still needs to find the first set of mappings among 26! possible ones. The rotor cipher is much more resistant to statistical attack than the monoalphabetic substitution cipher because it does not preserve letter frequency.

Enigma Machine

- Extensively used during World War II.
- Machine was based on the principle of rotor ciphers.



The following lists the main components of the machine:

1. A keyboard with 26 keys used for entering the plaintext when encrypting and for entering the ciphertext when decrypting.
2. A lampboard with 26 lamps that shows the ciphertext characters in encrypting and the plaintext characters in decrypting.
3. A plugboard with 26 plugs manually connected by 13 wires. The configuration is changed every day to provide different scrambling.
4. Three wired rotors as described in the previous section. The three rotors were chosen daily out of five available rotors. The fast rotor rotates 1/26 of a turn for each character entered on the keyboard. The middle rotor makes 1/26 turn for each complete turn of the fast rotor. The slow rotor makes 1/26 turn for each complete turn of the middle rotor.
5. A reflector, which is stationary and prewired.

Code Book

Code Book

To use the Enigma machine, a code book was published that gives several settings for each day, including:

a. The three rotors to be chosen, out of the five available ones.
b. The order in which the rotors are to be installed.
c. The setting for the plugboard.
d. A three-letter code of the day.

Encryption/ decryption

Procedure for Encrypting a Message

To encrypt a message, the operator followed these steps:

1. Set the starting position of the rotors to the code of the day. For example, if the code was "HUA", the rotors were initialized to "H", "U", and "A", respectively.
2. Choose a random three-letter code, such as "ACF". Encrypt the text "ACFACF" (repeated code) using the initial setting of rotors in step 1. For example, assume the encrypted code is "OPNABT".
3. Set the starting positions of the rotors to OPN (half of the encrypted code).
4. Append the encrypted six letters obtained from step 2 ("OPNABT") to the beginning of the message.
5. Encrypt the message including the 6-letter code. Send the encrypted message.

Procedure for Decrypting a Message

To decrypt a message, the operator followed these steps:

1. Receive the message and separate the first six letters.
2. Set the starting position of the rotors to the code of the day.
3. Decrypt the first six letters using the initial setting in step 2.
4. Set the positions of the rotors to the first half of the decrypted code.
5. Decrypt the message (without the first six letters).

Cryptanalysis

Cryptanalysis

We know that the Enigma machine was broken during the war, although the German army and the rest of the world did not hear about this until a few decades later. The question is how such a complicated cipher was attacked. Although the German army tried to hide the internal wiring of the rotors, the Allies somehow obtained some copies of the machines. The next step was to find the setting for each day and the code sent to initialize the rotors for every message. The invention of the first computer helped the Allies to overcome these difficulties. The full picture of the machine and its cryptanalysis can be found at some of the Enigma Websites.

Stream and Block Ciphers

- Stream Cipher
  - Stream ciphers (encryption/ decryption is done on 1 symbol at a time)
  - Additive ciphers, multiplicative, vigenere are stream ciphers
  - If the algorithm is XOR, this is a stream cipher:

$p:$	p_1	p_2	p_3	p_4	p_5
	$\oplus$	$\oplus$	$\oplus$	$\oplus$	$\oplus$
$k:$	k_1	k_2	k_3	k_4	k_5
$c:$	c_1	c_2	c_3	c_4	c_5

Block ciphers

- Block ciphers (group of plain text symbols of size m (m>1)are encrypted together creating a group of cipher-text of the same size)
- Playfair, hill are block ciphers
- If the algorithm is XOR, this is a block cipher

$p:$	$p_1 p_2$	$p_3 p_4$	$p_5 p_6$	$p_7 p_8$	$p_9 p_{10}$
	$\oplus$	$\oplus$	$\oplus$	$\oplus$	$\oplus$
$k:$	k_1	k_2	k_3	k_4	k_5
$c:$	$c_1 c_2$	$c_3 c_4$	$c_5 c_6$	$c_7 c_8$	$c_9 c_{10}$

Advantages and Disadvantages

- Stream ciphers:
  - –They operate relatively fast since they work on only one character at a time
  - –Lower error propagation since each symbol is affected only by itself

- Block Ciphers:
  - –Higher diffusion since the material for each block affects the entire block
  - –Single characters can not be swapped in and out by an attacker

Symmetric Key cryptography

Block Cipher	Stream Cipher
Processing or encoding of the plain text is done as a fixed length block one by one. A block for example could be 64 or 128 bits in size.	Processing or encoding of plain text is done bit by bit. The block size here is simply one bit.
The same key is used to encrypt each of the blocks	A different key is used to encrypt each of the bits.
A Pad added to short length blocks	Bits are processed one by one in as in a chain
Uses Symmetric Encryption and is NOT used in asymmetric encryption	High speed and low hardware complexity
More secure in most cases	Equally secure if properly designed
Usually more complex and slower in operation	Usually very simple and much faster

Examples: AES, DES

Examples: one time pad, vigenere etc