Cryptography & Classical Ciphers

by
Alaaddin Abbas

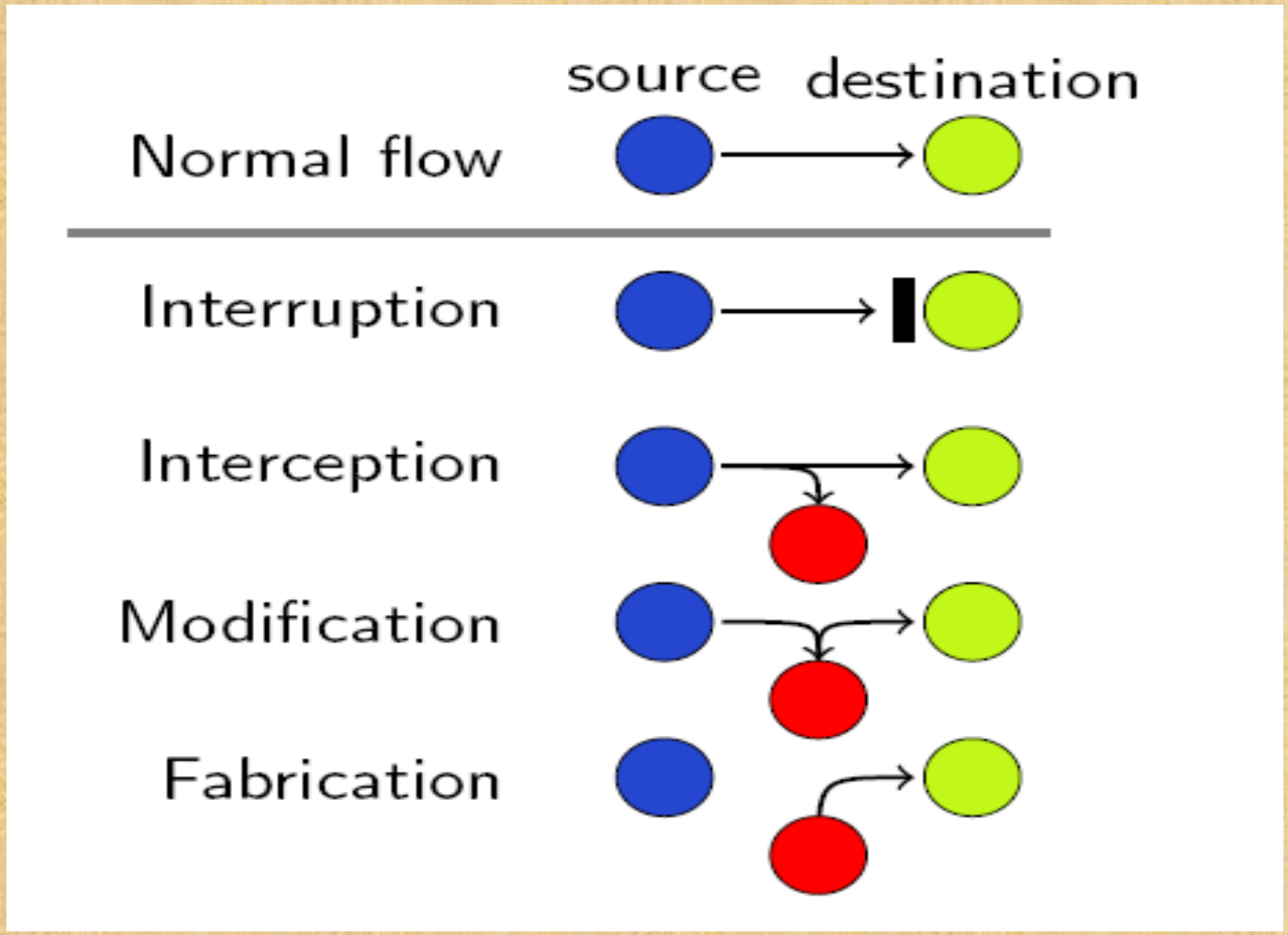
Introduction

- **Computer Security** - generic name for the collection of tools designed to protect data and to prevent hackers.
- **Network Security** - measures to protect data during their transmission.
- **Internet Security** - measures to protect data during their transmission over a collection of interconnected networks.

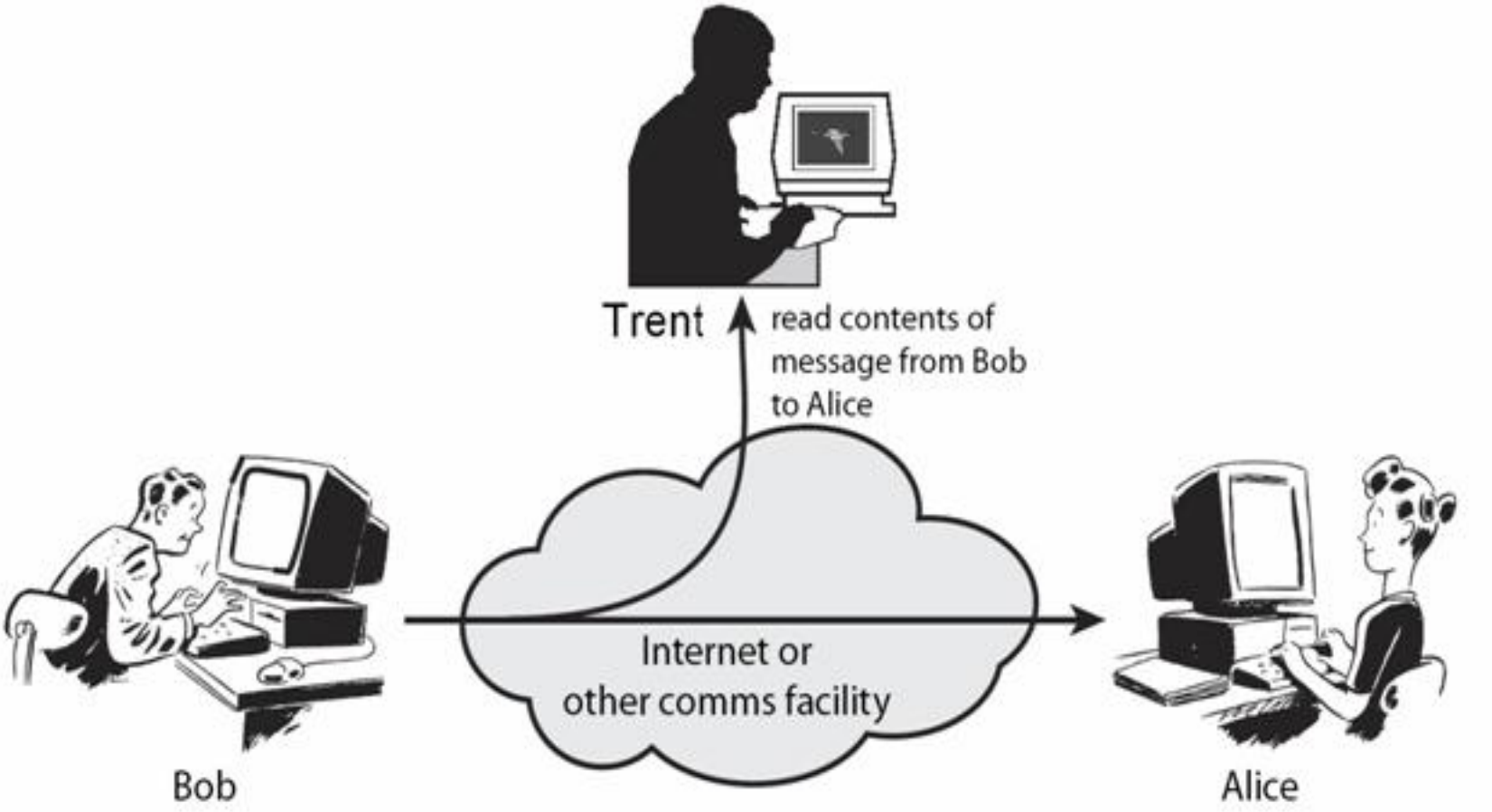
Security Attack

- "Any action that compromises the security of information owned by an organization"
- Information security is about how to prevent attacks, or failing that, to detect attacks on information-based systems
- Generic types of attacks
  - passive
  - active

Security Attacks



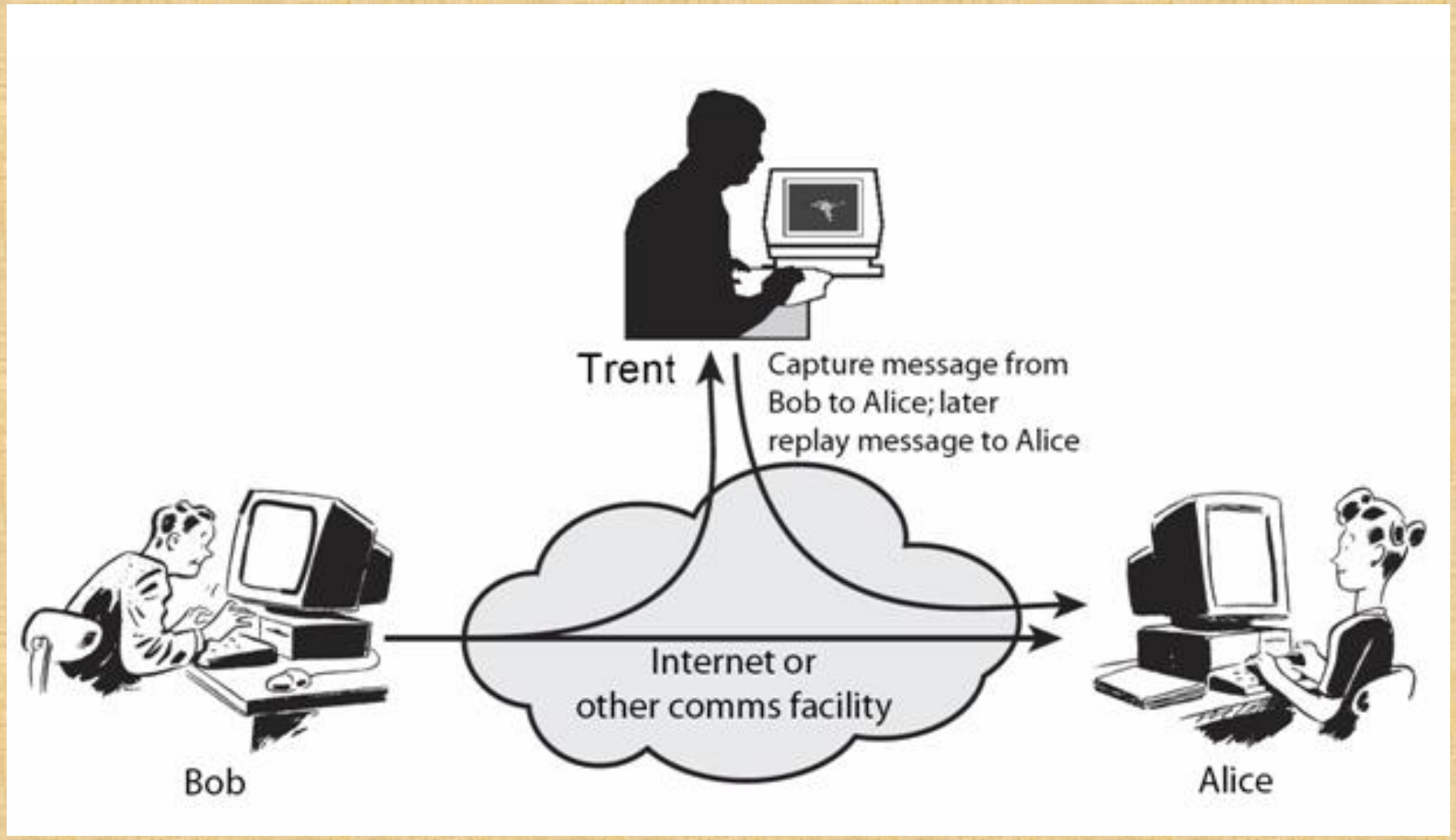
Passive Attacks



Passive Attacks

- **"Passive attacks"** attempt to learn or make use of information from the system but does not affect system resources.
- By eavesdropping on, or monitoring of, transmissions to:
  - obtain message contents or
  - monitor traffic flows
- Are difficult to detect because they do not involve any alteration of the data.

Active Attacks



Active Attacks

- **"Active attacks"** attempt to alter system resources or affect their operation.
- Passive attacks are relatively easier to detect. Measures are available to prevent their success.
- On the contrary, it is quite difficult to prevent active attacks because of the wide variety of potential physical, software, and network vulnerabilities.
- Instead, the goal is to detect active attacks and to recover from any disruption or delays caused by them.

Security Service

- A processing or communication service that enhances the security of the data processing systems and the information transfer for an organization. The services are intended to defy security attacks, and they make use of one or more security mechanisms to serve the purpose.

Security Services (X.800)

- Authentication
  - Assurance that the communicating entity is the one claimed
- Access Control
  - Prevention of the unauthorized use of a resource
- Data Confidentiality
  - Protection of data from unauthorized disclosure
- Data Integrity
  - Assurance that the contents of the data received are the same as sent by an authorized entity
- Non-Repudiation
  - Protection against denial by one of the parties in a communication

Security Mechanisms

- Feature designed to detect, prevent, or recover from a security attack.
- There is no single mechanism to provide security of the data to be transmitted.
- However the element that underlies most of the security mechanisms is the use of cryptographic techniques.
- Cryptography is the art of secret writing, is the process of converting information, such as this slide, that can be read by most, into a secret code, that can only be read by those who are party to the secret.

Terminologies

plaintext	original message
encryption	encoding the message to hide its contents
ciphertext	encrypted message
decryption	retrieving the plaintext from the ciphertext
key	is used by the encryption and decryption. The decryption can be performed only by knowing the proper key

Security Mechanisms

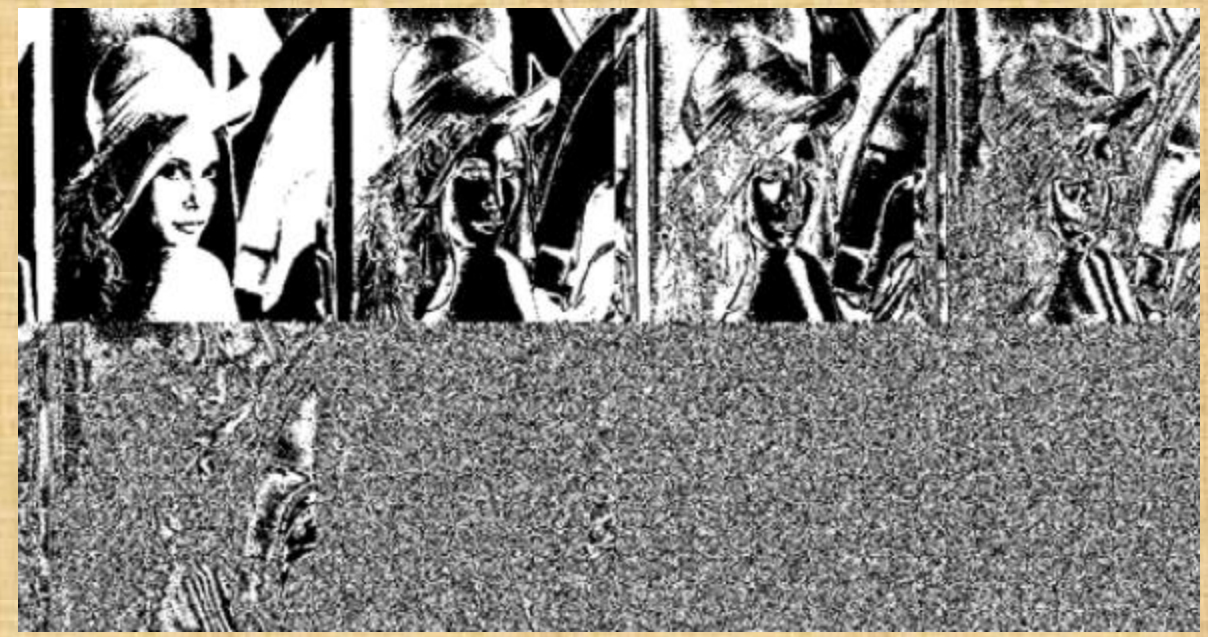
Encryption	confidentiality, authentication, integrity protection
Check/Hash algorithms	integrity protection, authentication
Digital signatures	authentication, integrity protection, non–repudiation

Cryptography vs. Steganography

- Cryptography
  - Overt writing: Evident that there is a secret message.
  - Enemy can intercept the message
  - Enemy can decrypt the message
- Steganography
  - Covert writing: Its not evident that there is a secret message.

Steganography

- Change the LSB (least siginificant bit) of pixels in a random walk.
- Change the LSB of subsets of pixels (i.e. around edges).
- Increment/Decrement the pixel value instead of flipping the LSB.



Steganography- Example

- News Eight Weather:

  Tonight increasing snow. Unexpected precipitation Smothers Eastern towns. Be extremely cautious and use snow-tires especially heading east. The highways are knowingly slippery. Highway evacuation is suspected. Police report emergency situations in downtown ending near Tuesday.

  - First letter of each word yields:

    Newt is upset because he thinks he is President.

Steganography- Example

- From WWII German spy (Kahn):

  Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by products, ejecting suet and vegetable Oils.

  - Second letter of each word yields:

    Pershing sails from NY June 1.

Cryptography-- Cæsar Cipher

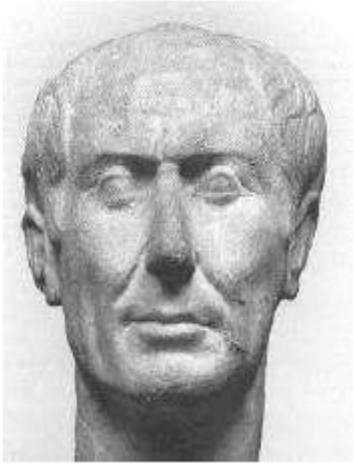
Cæsar cipher:

key: new letter = old letter + 3

a	b	c	d	e	f	g	h	i	j	k	l	m	n	...
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
d	e	f	g	h	i	j	k	l	m	n	o	p	q	...

Example:

`Julius Caesar` ⇒ `Mxolxv Fdhvdu`



Conventional Encryption

Requirements for secure use of conventional encryption

- Strong encryption algorithm
- Sender and receiver obtained the secret key in a secure fashion.
- The key must be kept secure at all times

Classification of Cryptographic Systems

Classification of cryptographic systems

1. The type of operations used for transforming plaintext to ciphertext
2. The number of keys used
3. The way in which the plaintext is processed

In current encryption techniques the security depends on the secrecy of the key and not on the secrecy of the algorithm.

Classification of Cryptographic Systems

Type of operations:

1. Substitution: Each element of the plaintext is mapped into another element. (element = bit, letter, group of letters ...)
2. Transposition: Each element of the plaintext is rearranged.

Diffusion and Confusion (Shannon). No information is lost, and the operations are reversible.

Classification of Cryptographic Systems

- Substitution: Cæsar $\Rightarrow$ mxolxv
  substitute one letter for another
- Transposition: Cæsar $\Rightarrow$ raacse
  where the operation is to change the order of the letters

Classification of Cryptographic Systems

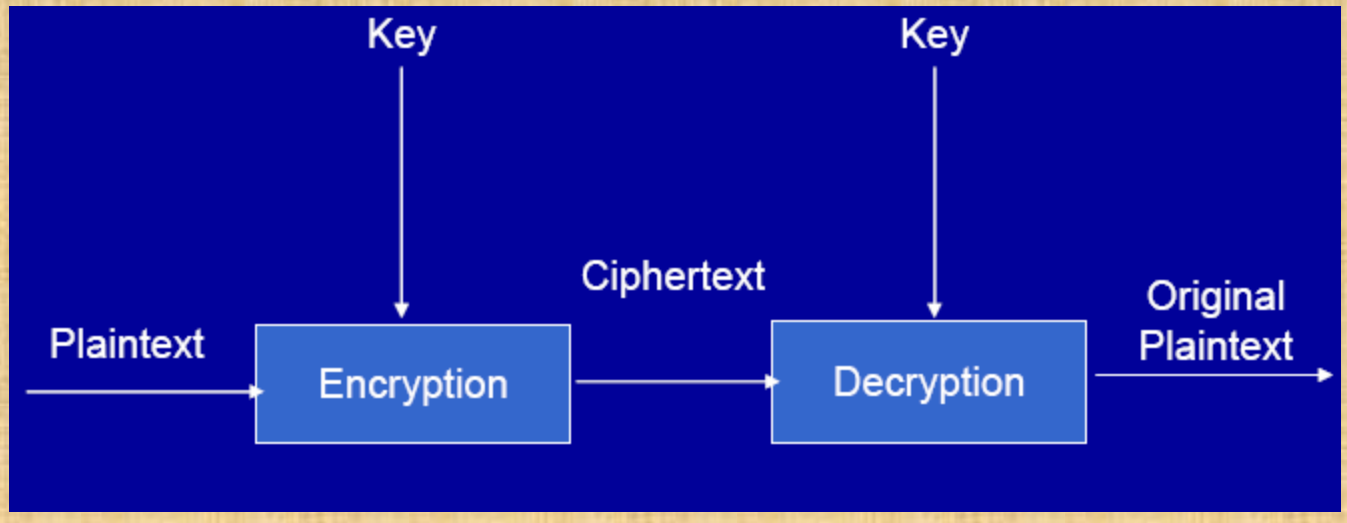
The number of keys used

- Symmetric: Sender and receiver use the same key. This is known as conventional encryption.
- Asymmetric: Sender and receiver each uses a different key. This is know as public–key encryption.

Process of the plaintext

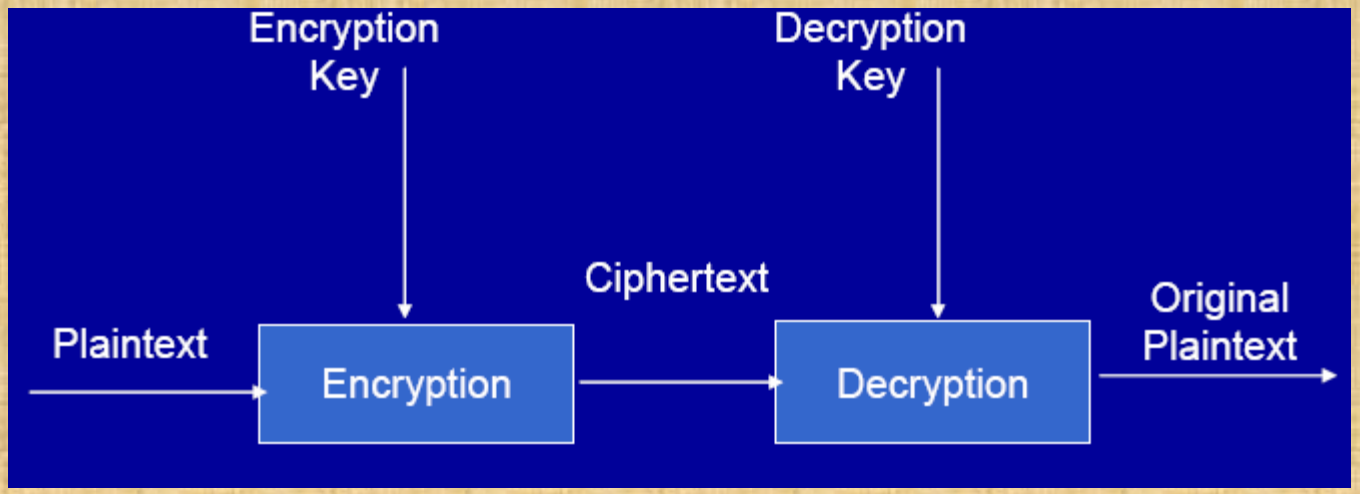
- Stream Cipher: Process one input element at a time
- Block Cipher: Process a block of elements at a time

Symmetric Case



- $E_k (M) = C$
- $D_k (C) = M$
- $D_k (E_k (M)) = M$

Asymmetric Case



- $E_{k1}(M) = C$
- $D_{k2}(C) = M$
- $D_{k2}(E_{k1}(M)) = M$

Kerchoff's Principle

- *The security of cryptosystem must not depend on keeping secret the crypto-algorithm. It must depend on keeping secret the key.*

- Reasons:
  - Details of the crypto-algorithm can be captured or reverse-engineered.
  - Even if so, frequently changing the key maintains the security.

Note:

In symmetric-key cryptography, the same key is used by the sender (for encryption) and the receiver (for decryption). The key is shared.

Note:

In symmetric-key cryptography, the same key is used in both directions.

Class Exercise

- Caesar wants to arrange a secret meeting with Marc Anthony, either at the Tiber (the river) or at the Coliseum (the arena).
- He send the ciphertext *EVIRE*.
- However, Antony does not know the key, so he tries all possibilities.
- Where will he meet Caesar?

Polyalphabetic Substitution: Vigen`ere Cipher

There are stream ciphers that use polyalphabetic substitution. An example is the Vigenère Cipher

1. Identify letters with numbers, a= 0, b=1, . . . , z= 25
2. The secret key is a sequence of letters, e.g a word
3. Encrypt by adding the plaintext letter to a key letter using rotation

Example: Vigen`ere Cipher

Example:

Plaintext: `my password is tomato`

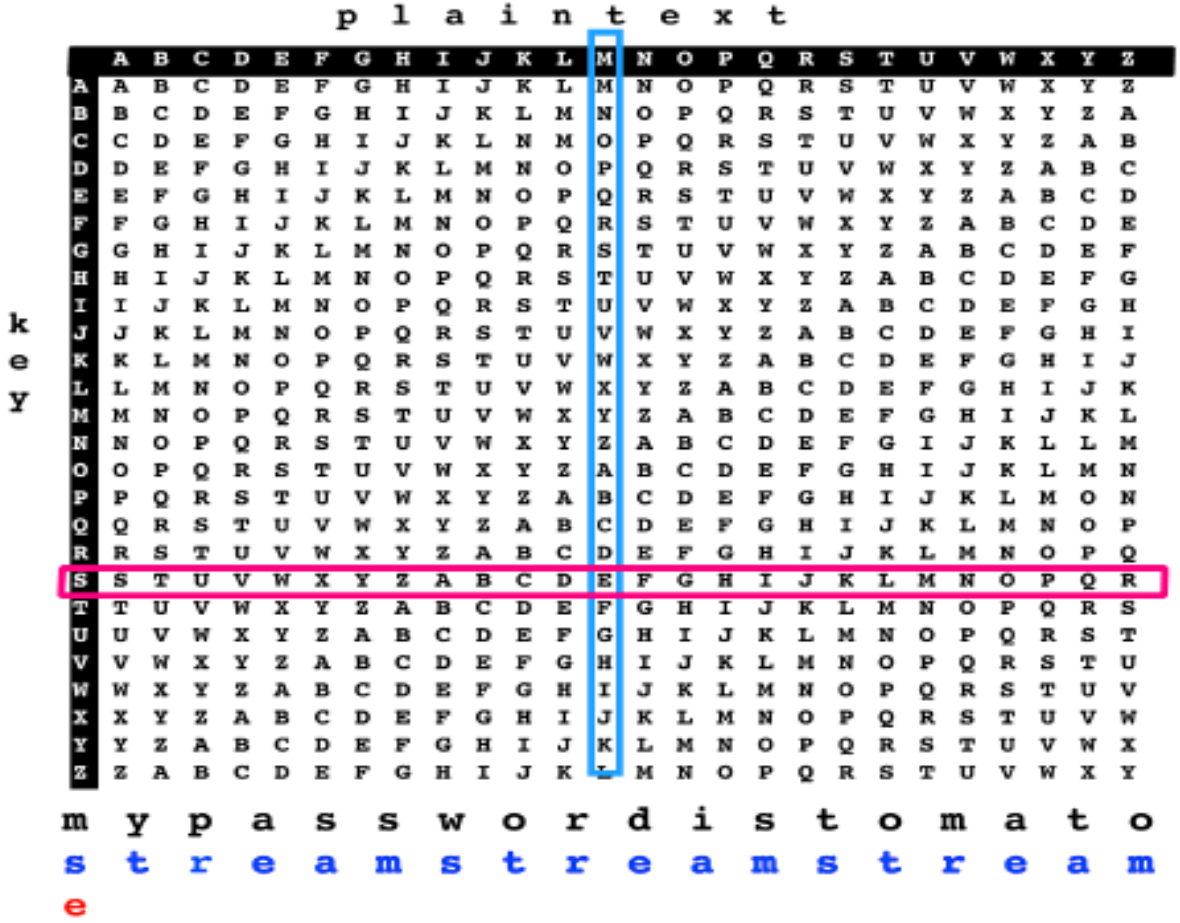
Key: `stream`

m	y	p	a	s	s	w	o	r	d	i	s	t	o	m	a	t	o
s	t	r	e	a	m	s	t	r	e	a	m	s	t	r	e	a	m
e	r	g	e	s	e	o	h	i	h	i	e	l	h	d	e	t	a

the last line is the ciphertext

Example: Vigen`ere Cipher

How does it works?



Example: Vigen`ere Cipher

Example using numbers:

- M $\Rightarrow$ 12 plaintext
- S $\Rightarrow$ 18 key

Encryption:

- $(12+18) \mod (26) = 4$
- 4 $\Rightarrow$ E ciphertext

Class Quiz

- You have intercepted a message encrypted with a cipher of the form:-

  C = aM+b

  where **M** is the plaintext and **C** is the ciphertext (both integers modulo 26).

  - The ciphertext starts with **BBDJ**.
  - The plaintext starts with **OOPS**.
- **Find the key**.