# Info Security Technology

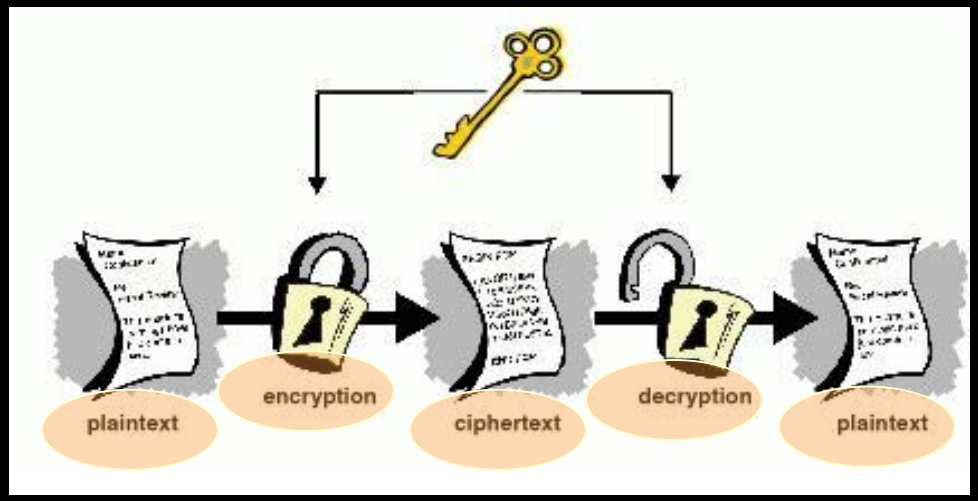
Topic 5
Cryptography
(Classic Crypto)

# Objectives

- Define Cryptography
- Define Steganography
- Understand Cipher, Encryption and Decryption

# What Is Cryptography?

- **Cryptography**
  - The science of transforming information into an unintelligible form while it is being transmitted or stored so that unauthorized users cannot access it. [using a key]
  - The transforming process scrambles a message so that it cannot be viewed.



# SYMBOL - A 4 Letter Word

CAN YOU 'DECODE' THE MESSAGE FROM PICTURE?

# SYMBOL - A 5 Letter Word

CAN YOU 'DECODE' THE MESSAGE FROM PICTURE?

# *Cryptography and Security*

Cryptography can provide basic security protection for information:

1. Cryptography can protect the confidentiality of information
   - Confidentiality – Ensures only authorised parties can **view** the information
2. Cryptography can protect the integrity of the information
   - Integrity – Ensures no unauthorised person or malicious software has **altered** the data
3. Cryptography can help ensure the availability of the data
   - Availability – Ensures that data is **accessible** to authorised users
4. Cryptography can verify the authenticity of the sender
   - Authenticity – Provides proof of the **genuineness** of the user
5. Cryptography can enforce non-repudiation
   - Non-repudiation – Proves that a **user performed an action**

# *Algorithms*

- All the current encryption schemes are based upon an **algorithm**.
- An **algorithm** is a step-by-step problem-solving procedure.
- It is a recursive computational procedure for solving a problem in finite steps.
- A **cryptographic algorithm** is a set of mathematical steps for encrypting and decrypting information.

# *Steps for Encryption*

- The steps for encrypting data **can be published** because of the design of the systems.
  - They are designed to use a key.
- The algorithms remain the same.
  - Every implementation uses a different **key**.
  - This ensures that even if other know the algorithm, they cannot break the security.

# *Steps for Encryption*

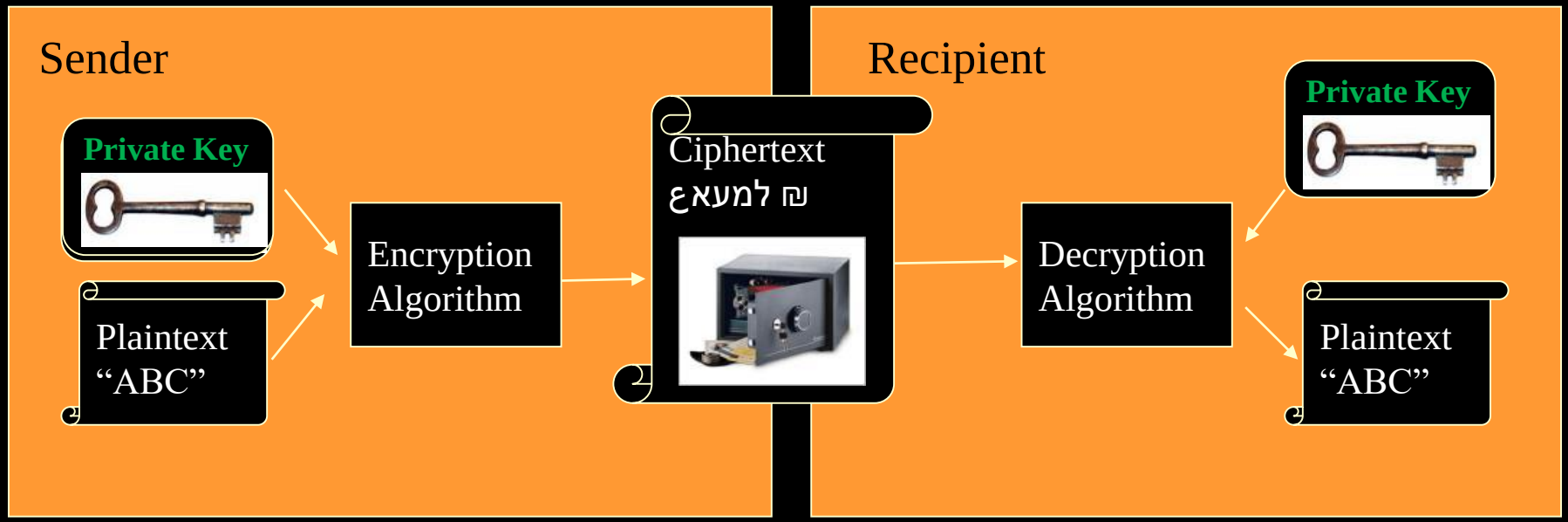
- Plaintext
  - refers to the information in plain language. Also referred to as cleartext, plaintext is commonly referred to as the input to a cipher or encryption algorithm.
- Ciphertext
  - Every implementation uses a different **key**.
  - This ensures that even if other know the algorithm, they cannot break the security.

# *Cryptographic Algorithms*

- There are three categories of cryptographic algorithms:
  - Symmetric-key algorithm
  - Asymmetric-key algorithm
  - Hashing algorithm

# Symmetric-key Algorithm

- Symmetric-key algorithm
  - The same identical key is used to encrypt and decrypt a document.
  - The key must be kept secret



# *Symmetric Algorithm*

- Also called private key cryptography; uses the same single key to encrypt and decrypt a message
- Encryption is the process of transforming information (referred to as plaintext) using an algorithm to make it unreadable.
- Decryption is, the reverse process, to make the encrypted information readable again.
- A cipher is an algorithm for performing encryption or decryption

# *Symmetric Algorithm*

- Classified into 2 categories:
  - Stream Cipher
    - Works on one character at a time
    - Examples: Shift, Substitution and Polyalphabetic Ciphers
  - Block Cipher
    - Manipulates an entire block of plaintext at a time
    - The plaintext is divided into separate blocks.
    - Each block is encrypted independently.

# Shift Cipher

- One of the most famous ancient cryptographers was Julius Caesar
- Caesar shifted each letter (Left-shift) of his messages to his generals WITH KNOWN places down in the alphabet
- A total of 26 Alphabetical letters were used

```
Table                : ABCDEFGHIJKLMNOPQRSTUVWXYZ
Substitution         : ABCDEFGHIJKLMNOPQRSTUVWXYZ

Key                  : Left shift of 0

Plaintext            : ATTACK AT DAWN
Ciphertext           :
```

# Shift Cipher

- Caesar shifted each letter (Left-shift) of his messages to his generals 1 place down in the alphabet

```
Table          : ABCDEFGHIJKLMNOPQRSTUVWXYZ
Substitution   : BCDEFGHIJKLMNOPQRSTUVWXYZA

Key            : Left shift of 1 position

Plaintext      : ATTACK AT DAWN
Ciphertext     : BUU …
```

# Caesar Cipher

## Shift Cipher

- Example Left Rotation of 1 Key
- Plaintext : A B C D E F G H I … Z

- Ciphertext : A B C D E F G H I …

| Plain Line | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Substitution | 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 |

**Plaintext : ATTACK AT DAWN**

**Ciphertext : BUUBDL#BU#EBXO**

# Shift Cipher

- Caesar shifted each letter (Left-shift) of his messages to his generals 2 places down in the alphabet

```
Table          : ABCDEFGHIJKLMNOPQRSTUVWXYZ
Substitution   : CDEFGHIJKLMNOPQRSTUVWXYZAB

Key            : Left shift of 2 position

Plaintext      : ATTACK AT DAWN
Ciphertext     : CVV …
```

# Shift Cipher

- Caesar shifted each letter (Left-shift) of his messages to his generals 25 places down in the alphabet

```
Table          : ABCDEFGHIJKLMNOPQRSTUVWXYZ
Substitution   : ABCDEFGHIJKLMNOPQRSTUVWXYZ

Key            : Left shift of 25 position

Plaintext      : ATTACK AT DAWN
Ciphertext     : ?
```


YZABCDEFGHIJKLMNOPQRSTUVWX
YZABCDEFGHIJKLMNOPQRSTUVWX
YZABCDEFGHIJKLMNOPQRSTUVWX

# Substitution Cipher

- The weakness of shift ciphers led to substitution ciphers.
  - Substitution ciphers work on the principle of substituting a different letter for every letter.
  - This system permits 26 possible values for every letter in a message.
  - The cipher is more complex than a standard shift cipher.

```
Table          :  ABCDEFGHIJKLMNOPQRSTUVWXYZ
Key            : THE QUICKBROWNFXJMPDVRLAZYG

Plaintext      : ATTACK AT DAWN
Ciphertext     :
```

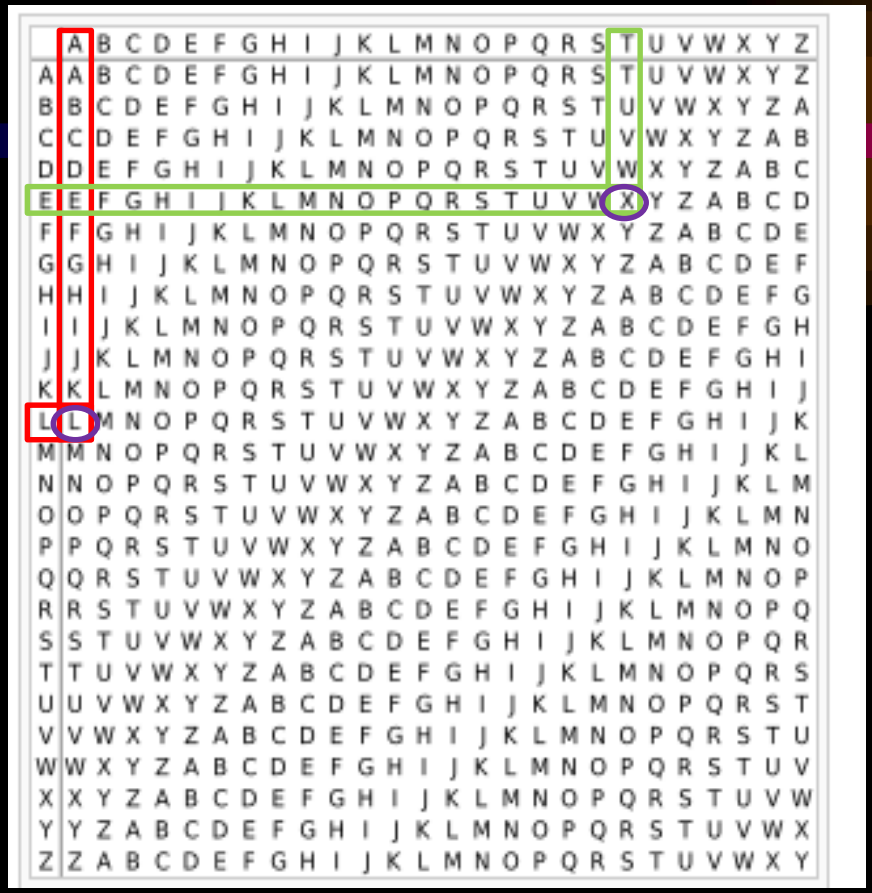
# Substitution Cipher

- The weakness of shift ciphers led to substitution ciphers.
  - Substitution ciphers work on the principle of substituting a different letter for every letter.
  - This system permits 27 possible values for every letter in a message. (E.g 26 Alphabetical chars and 1 space)
  - The cipher is more complex than a standard shift cipher.

```
Table          :  ABCDEFGHIJKLMNOPQRSTUVWXYZ
Key            : THE QUICKBROWNFXJMPDVRLAZYG

Plaintext      : ATTACK AT DAWN
Ciphertext     : HVVH OTHVTQHAF
```

# Polyalphabetic cipher



| | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 |

```
Plaintext     : ATTACK AT DAWN
Key           : LEMONLEMONLE
Ciphertext    : LXFOPVEFRNHR
```

# *Symmetric-key Algorithm*

- Information protections by Symmetric Cryptography

| Characteristic | Protection? |
|---|---|
| Confidentiality | Yes |
| Integrity | Yes |
| Availability | Yes |
| Authenticity | No |
| Non-repudiation | No |

**Table 11-6** Information protections by symmetric cryptography

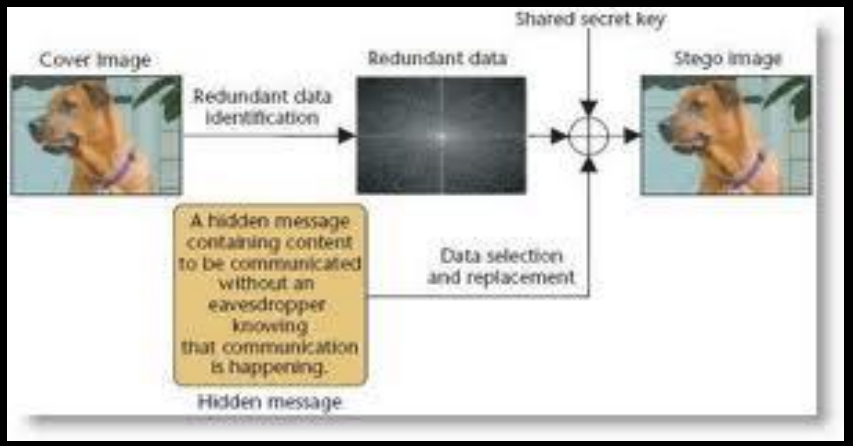
# Symmetric Algorithm

Popular Symmetric Algorithms:

- Data Encryption Standard (DES)
  - DES is a block cipher and encrypts data in 64-bit blocks
- Triple Data Encryption Standard (3DES)
  - Designed to replace DES
  - Uses three rounds of encryption instead of just one
- Advanced Encryption Standard (AES)
  - Approved as a replacement for DES
  - AES performs three steps on every block (128 bits) of plaintext
- Other symmetric algorithms:
  - Rivest Cipher (RC) family from RC1 to RC6
  - International Data Encryption Algorithm (IDEA)
  - Blowfish
  - Twofish

# What Is Steganography?

- **Steganography**
  - the art and science of hiding information by embedding it in some other data.
  - comes from the Greek word meaning covered writing.
  - Hides the existence of the data
  - What appears to be a harmless image can contain hidden data embedded within the image
  - Can use image files, audio files, or even video files (carrier file) to contain hidden information.



# *What Is Steganography?*

- Steganography is NOT Cryptography
  - **cryptography** - render message unintelligible
  - **steganography** - conceal the existence of the message

*Cryptography and steganography are similar in the sense that they are both techniques that are used to send information securely.*

# Digital Watermarking?

- Allows users to embed SPECIAL PATTERN or SOME DATA into digital contents without changing its perceptual quality.
- When data is embedded, it is not written at HEADER PART but embedded directly into digital media itself by changing media contents data
- Watermarking is a key process for the PROTECTION of copyright ownership of electronic data.