الجمهورية الجزائرية الديمقراطية الشعبية
PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA
وزارة التعليم العالي و البحث العلمي
MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH

جامعة محمد بوضياف – المسيلة
كلية التكنولوجيا
قسم الإلكترونيك

MOHAMED BOUDIAF UNIVERSITY OF M'SILA
FACULTY OF TECHNOLOGY
DEPARTMENT OF ELECTRONICS

جامعة محمد بوضياف - المسيلة
Université Mohamed Boudiaf - M'sila

الرقم : 3../ك.إ/2025

المسيلة في : 2025/11/24

شهادة إدارية

بعد الإطلاع على التقارير الايجابية الواردة من السادة الخبراء أعضاء لجنة دراسة المطبوعة الجامعية والاتية أسماؤهم:

- أمير منير — أستاذ محاضر "أ" — جامعة مولود معمري – تيزي وزو
- بن تومي الميلود — أستاذ محاضر "أ" — جامعة محمد بوضياف – المسيلـــة
- والي محمد عصام — أستاذ محاضر "أ" — جامعة محمد بوضياف – المسيلـــة

صادق أعضاء اللجنـــة العلميـــة على قبول المطبوعة البيداغوجية مع إمكانية إتخاذها سندا في تدريس طلبة السنة الثالثة ليسانس اتصالات، في ميدان علوم و تكنولوجيا و أن تعتمد في أي تقييم المسار العلمي للأستاذ المعني **حرحوز أحلام** (أستاذ محاضر قسم "أ"– جامعة محمد بوضياف - المسيلة) تحت عنوان :

Information security

رئيس اللجنة العلمية

جامعة محمد بوضياف - المسيلة
رئيس اللجنة العلمية
قسم الإلكترونيك
كلية التكنولوجيا

بوراس

رئيس القسم

جامعة محمد بوضياف المسيلة
رئيس قسم
الإلكترونيك
كلية التكنولوجيا

طباخ مصطفى

PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA

MINISTRY OF HIGHER EDUCATION

AND SCIENTIFIC RESEARCH

Mohamed Boudiaf University - M'sila

L3-Telecommunications
Department of electronics

Course

Information security

Dr. HARHOUZ Ahlam

Course structuring and planning

Information Security Course Details

Faculty: Technologies

Department: Electronics

Target Audience: Bachelor's (L3), Specialization: Telecommunications

Course Title: Information Security

Credits: 01

Coefficient: 01

Semester Hours: 22.5 hours (15 weeks)

Evaluation Mode: 100% Exam

Teacher:

Dr. Ahlam HARHOUZ

Contact: by email at ahlam.harhouz@univ-msila.dz

Access link

https://moodle.univ-msila.dz/moodle/course/view.php?id=3506

Objectives:

This course titled "Information Security" aims to:

- Help you understand the basics of computer security and its criteria.
- Understand the fundamental techniques and technologies used in communication network security.

Specifically, this course aims to:

- Present detailed concepts related to information security, focusing on existing security risks and weaknesses.
- Understand various concepts of cryptography, the notions related to cryptography and cryptanalysis, from traditional systems to modern (computerized) systems.

Prerequisites:

To make the most of this course, you should have knowledge of:

- Basic concepts of digital electronics.
- Telecommunications applications.
- Basic knowledge of telecommunication systems and networks.

Course Contents:

- Chapter 1: Introduction to Information Security
- Chapter 2: Cryptography and Cryptanalysis Concepts
- Chapter 3: Firewall Security
- Chapter 4: Virtual Private Networks (VPNs)
- Chapter 5: Switch Security (Concepts of VLANs, Attacks, and Data Link Layer Responses)
- Chapter 6: Wireless Network Security

REFERENCES

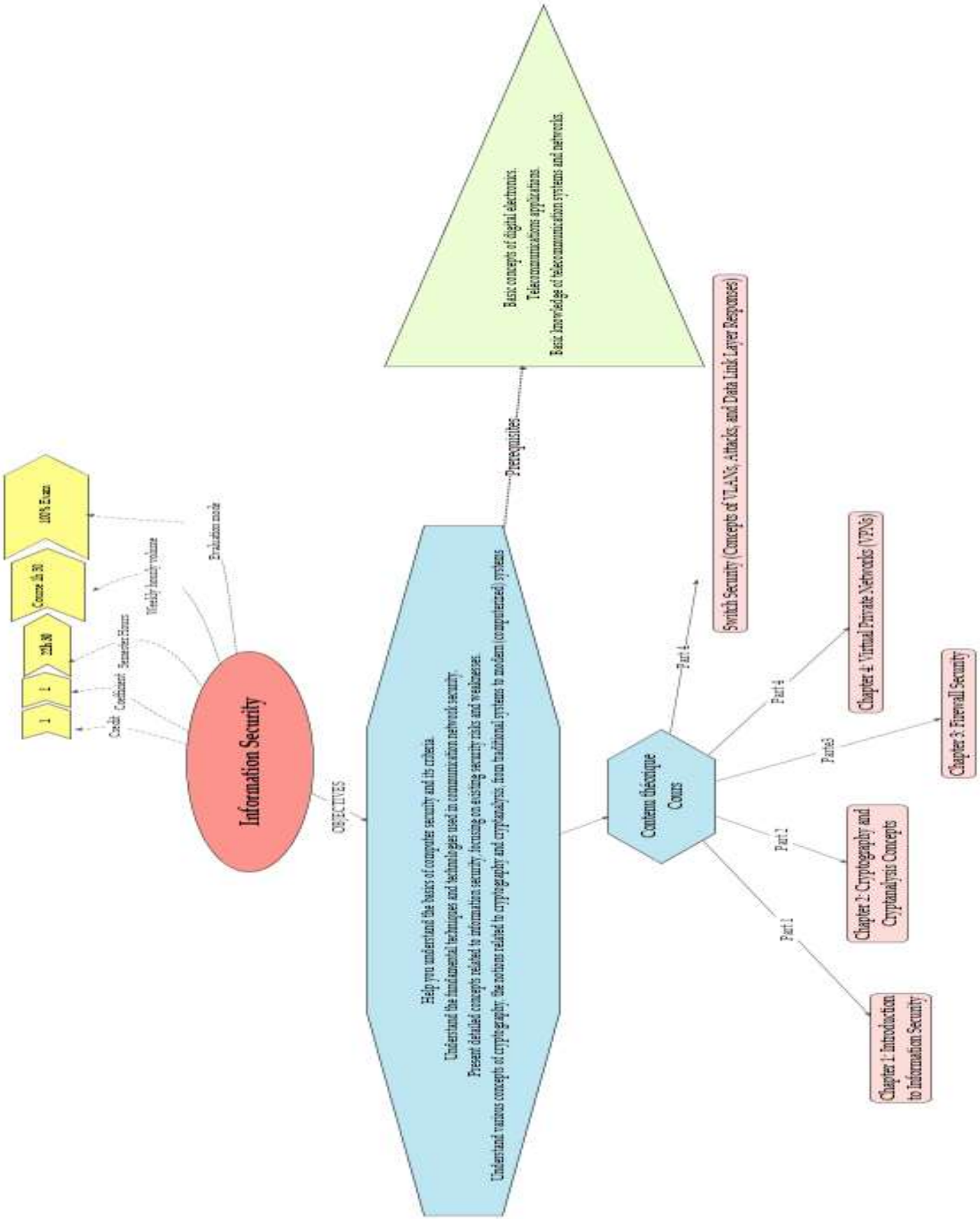
[1] A. Chouarfia. Introduction à la sécurité des réseaux et des systèmes d'information, 2010.

[2] Jean-François Pillou. Protection - introduction à la sécurité des réseaux, 2019.

[3] InfoCrise. Définition de la cyber-sécurité, 2016.

[4] Darril Gibson. Understanding the three factors of authentication, 2011.

Course concept map



Summary

Chapter 1.

Introduction to

Information Security

1.1. Introduction

Information security (often abbreviated as InfoSec) refers to the practice of protecting information from **unauthorized access**, **disclosure**, **alteration**, or **destruction**. Its primary goal is to ensure the confidentiality, integrity, and availability (often referred to as the CIA triad) of data, whether it is stored on physical devices, in digital systems, or transmitted across networks.

Today, with innovations based on **Information and Communication Technologies**, the requirements for **information security** are constantly increasing. This progress is strongly linked to the techniques and communication mediums used in networks.

Motivations

Facts: certain facts reported by cyber-security research centers

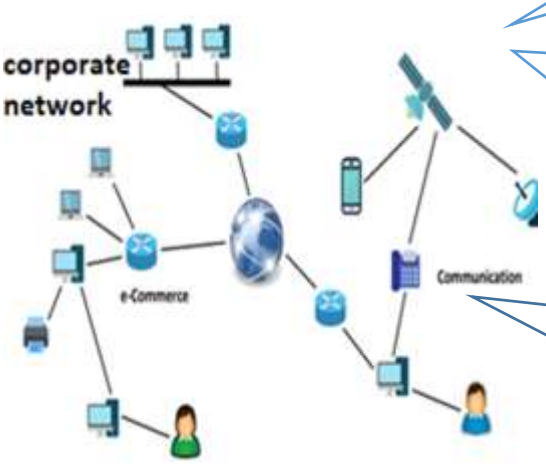
97% of corporate networks show signs of suspicious activity.

Interconnection of networks

According to Microsoft, individuals are twice as likely to be infected as professionals.

Microsoft

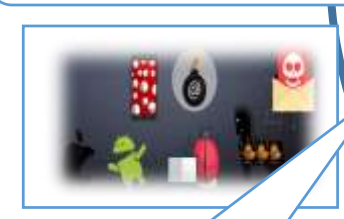
82% of companies worldwide have been victims of cyberattacks and data losses in 2019



According to the Anti-Phishing Working Group, 1.22 million phishing attacks (fraudulent links) occurred in 2016 (140 attacks/hour)

In 2016, Google removed 1.7 billion misleading, illegal, or deceptive advertisements.

Google

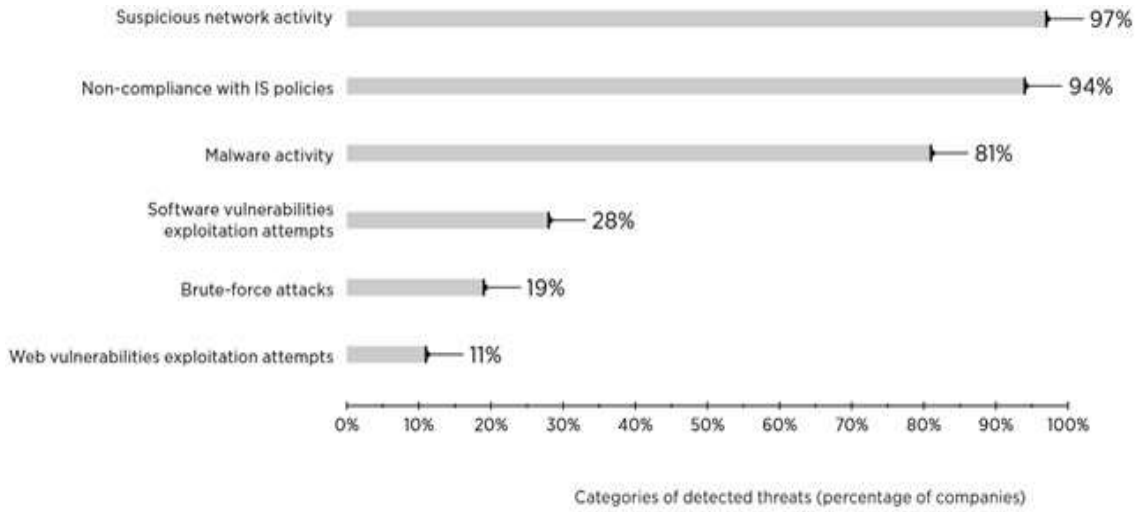


There are three million new malware (malicious software programs) that appear every day, according to *Symantec* in 2017

In the Internet of Things environment, less than 3 minutes are needed for a malicious person to take control of a connected object since generally, the owners of these objects do not change the default password.

Most of this malware spreads through traditional fraudulent links in emails or by downloading a malicious application from pirated download sites.

According to Gemalto, 5.6 million personal data are hacked or lost each year, which is 3900 data thefts per minute.



Effects

- Loss or endangerment of human life.
- Financial losses,
- Denial of service, which renders IT systems out of service
- Unauthorized use or abuse of IT systems for criminal purposes
- Loss, change, and/or alteration of data or software important for the functioning of businesses

Examples

In May 2017, the **WANNACRY** virus paralyzed more than 300,000 computers of multinational companies and public services

- It was reported in 150 countries
- Economic losses between 4 and 8 billion USD.

In June 2017, the **Ransomware NOTPETYA** virus. Spread faster than the Wannacry virus, it first hit banks, airports, and government structures in **Ukraine**.

- then struck the Russian oil company **Rosneft**, the German **Beiersdorf** (**Nivéa**), Auchan, the major shipping company Mærsk (Maritime Transport), **fedEx**, and **Mondelez**
- The bill is estimated at 10 billion USD, including 3 billion USD in insured losses.

In 2018, **the Marriott International hotel group** suffered a massive hack

- Due to an IT(information technology) security breach
- The data of 500 million customers were leaked.

On February 19, 2019, a series of attacks targeted domain names worldwide,

- The hackers attacked governments, intelligence or police services, airlines, and oil companies in the **Middle East** and **Europe**

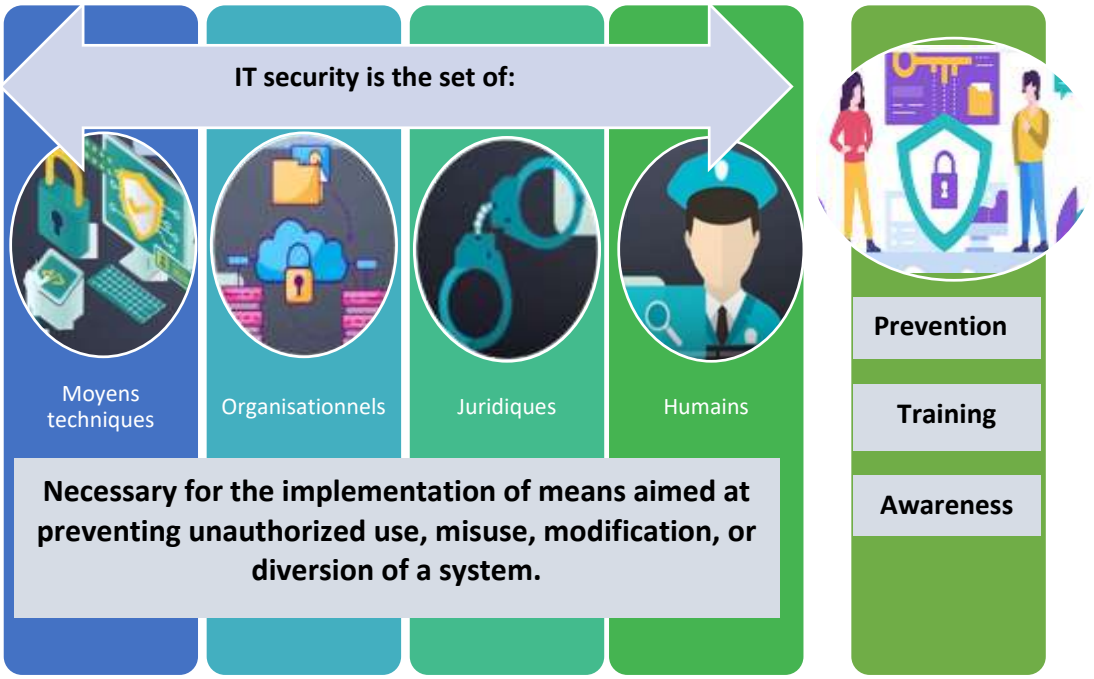
- In July 2019, theft of 106 million personal data of customers of the American bank **Capital One** in the **USA** and **Canada**.

1.2. Definitions

An **information system** is generally defined as the set of data and hardware and software resources of the company that allow storing or circulating them.

Information security is the set of means implemented to **reduce** the vulnerability of a system against accidental or intentional threats. The objective is to ensure that the hardware and/or

software resources of an IT system are only used within the intended framework and by authorized persons.

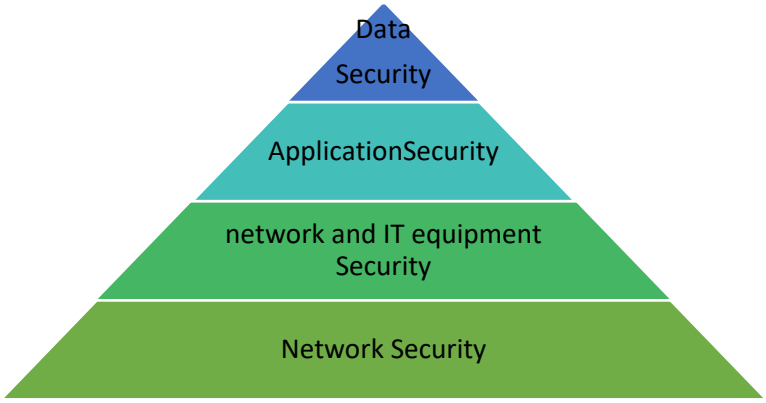


IT security is the set of means implemented to avoid and/or minimize natural failures due to the environment or defects in the information system and intentional malicious attacks whose consequences are catastrophic [1].

Network security is a level of assurance that the computers on the network function optimally and that users only have the rights that have been granted to them [2].

Cybersecurity is the set of tools, policies, security concepts and mechanisms, risk management methods, and technologies used to protect the hardware and software IT systems of organizations (businesses and governments) [3].

Security in general is present at several levels, whether it concerns the different scopes of information. Security must be considered in its full dimension, as illustrated in the following figure:

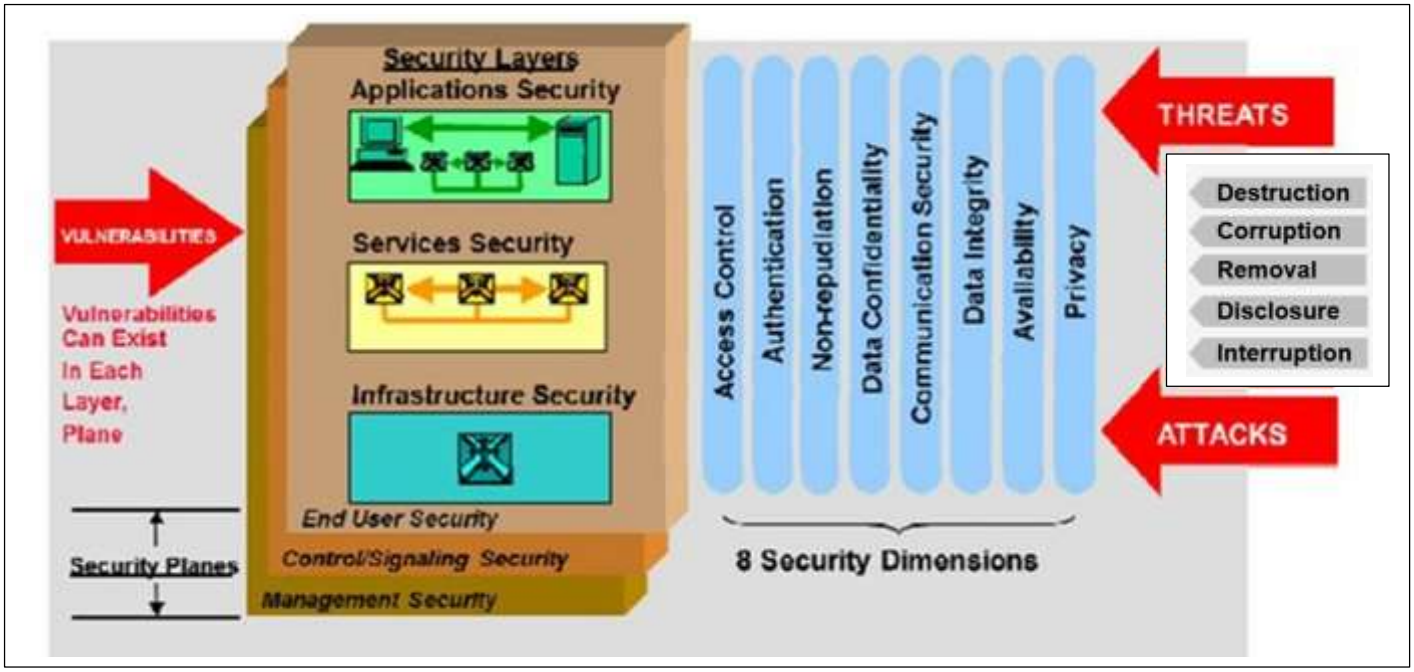


Levels of IT Security

IT security is concerned with protection against risks related to IT; it must take into account :

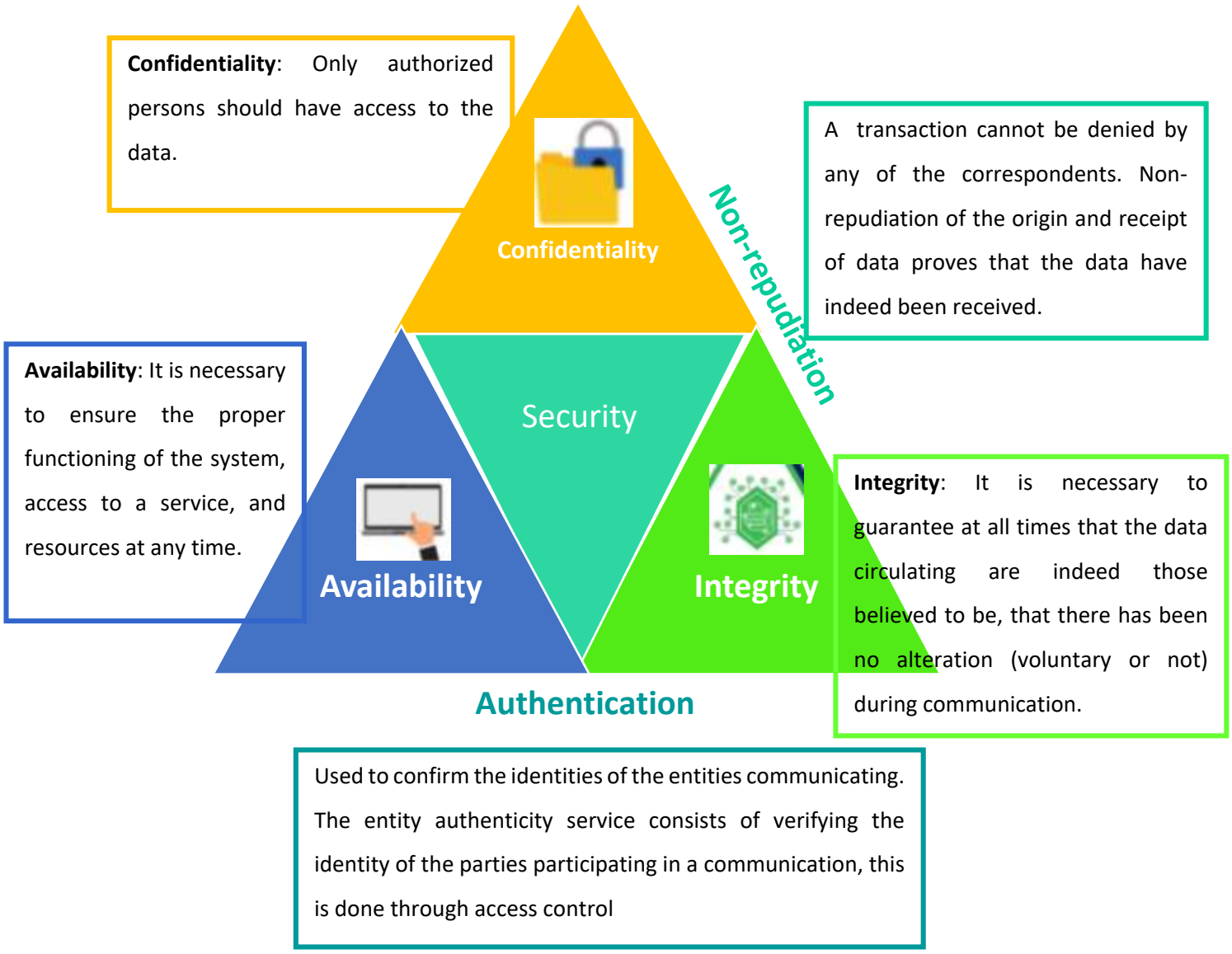
- ✓ The elements to protect: hardware, data, users;
- ✓ Their vulnerability;
- ✓ Their sensitivity: amount of work involved, confidentiality...
- ✓ The threats they face
- ✓ The means to address them (preventive and curative): complexity of implementation, cost...

1.3. Basic Security Architectures and Services



Architectural Elements of Security (Rec. ITU-T X.805)

Main Dimensions of Security



Main Dimensions of Security

1.4. Threats (Les menaces)

A threat is a potential action likely to cause damage to a system and having an impact on its functionality, integrity, or availability. Therefore, a vulnerability of a system represents its level of exposure to a threat.

Examples of threats:


Intrusion


Information theft


Information falsification


Information destruction


Resource outage


..... etc.

Access the ***Symmantec Security Response*** website at the following address: Http://securityresponse.symantec.com/
See the list of the latest virus threats. What are the names of the top five?

List of the most common IT threats on the web

Trojan Horse: is a type of malicious software that is often disguised as legitimate software

Spyware: Spyware is simply spy software.

Keylogger: The keylogger is a threat related to spyware. This program records everything typed on a keyboard: passwords, credit card numbers, email addresses, etc.

Rootkit: Rootkits are particularly formidable: they are composed of several malicious software, which are difficult to detect. They allow intruders to access a computer or network via a backdoor, then manipulate and steal data.

Rogues or scareware (are fake anti-spyware),

Browser hijacker: is another type of **malicious software** that installs on your computer without your permission.

1.5. Attacks

An attack is an action representing the means of exploiting a vulnerability to compromise the security of a system. There can be several attacks for the same vulnerability, but not all vulnerabilities are exploitable.

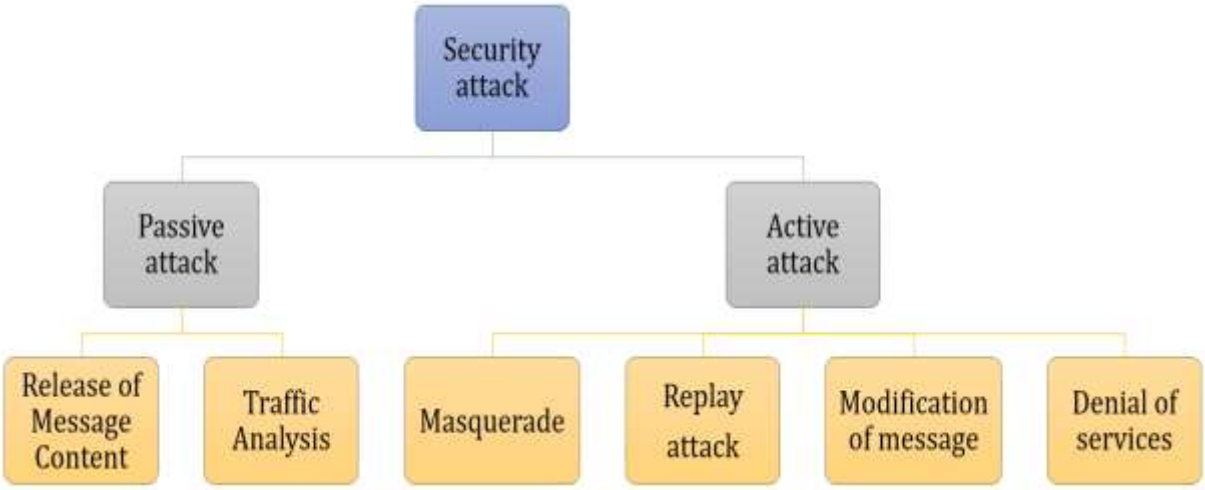
An attack corresponds to the realization of a threat. An attack is carried out by one or more aggressors. An attack is defined by:

- Its origin
- Its sponsor
- Its target
- Its objective
- Its means
- Its type
- Its motive or motivation
- Its justification

1.5.1. Network Attacks

A network attack is defined as an intrusion into a communication infrastructure to gain unauthorized access to resources or exploit existing vulnerabilities.

Goals of Attacks



Classification of Network Attacks

Active Attacks: consist of modifying transmitted messages, intruding into network equipment, or disrupting the proper functioning of the network. Unlike passive attacks, active attacks are detectable due to the significant damage they can cause. The goal of an attacker is to try to bypass or enter a secure system to steal, modify, disable, or destroy sensitive data. Here are the most well-known active attacks [5]:

Masquerade (or identity theft): This attack occurs when an entity pretends to be a different entity. This type of attack is the origin of all other active attacks,

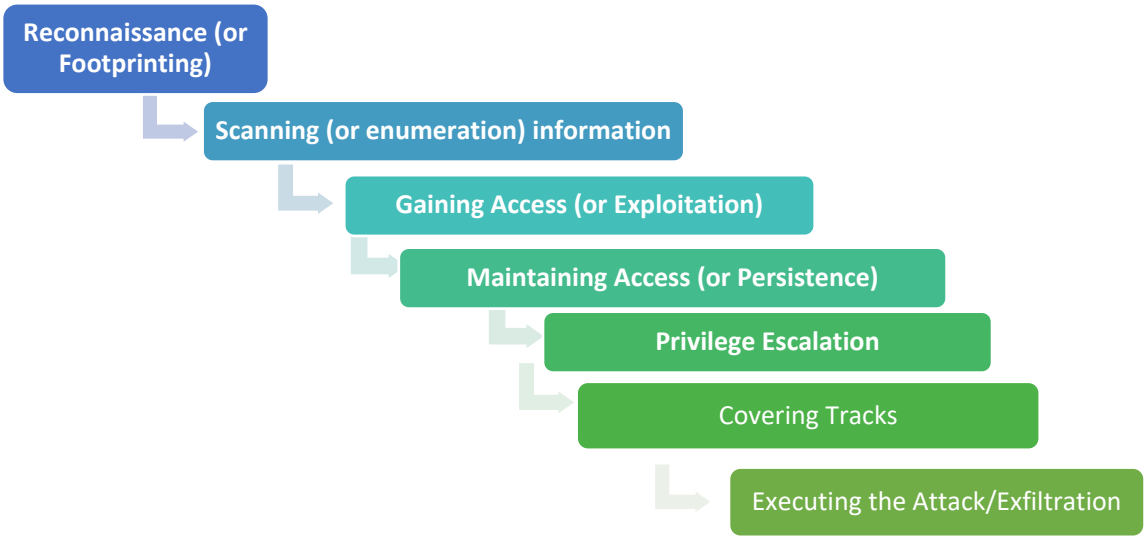
Replay: This type of attack consists of capturing a transmitted message (passive attack), then retransmitting it later to produce an unauthorized effect,

Message Modification: This attack allows modifying the content of the message or reordering messages to produce an unauthorized effect,

Denial of Service: The principle of this attack is to disrupt or interrupt the service of a network. Its goal is to saturate the service with useless messages to degrade the performance of the service or cause the loss of messages.

1.5.2. Steps of an Attack

To proceed with an attack on a network or service, the attacker generally follows a seven-step



1.6. Applications of Security:

- Equipment security
- Software application security
- Data security
- Telecommunications network security

Chapter 2: Concepts of Cryptography and Cryptanalysis

2.1. Introduction

Cryptography is a technique of writing where an encrypted message is written using secret codes or encryption keys. It is the practice of protecting information considered confidential through the use of encoded algorithms. The information can be at rest, in transit, or in use. Cryptography has four main objectives: Confidentiality, Integrity, Non-repudiation, and Authentication.

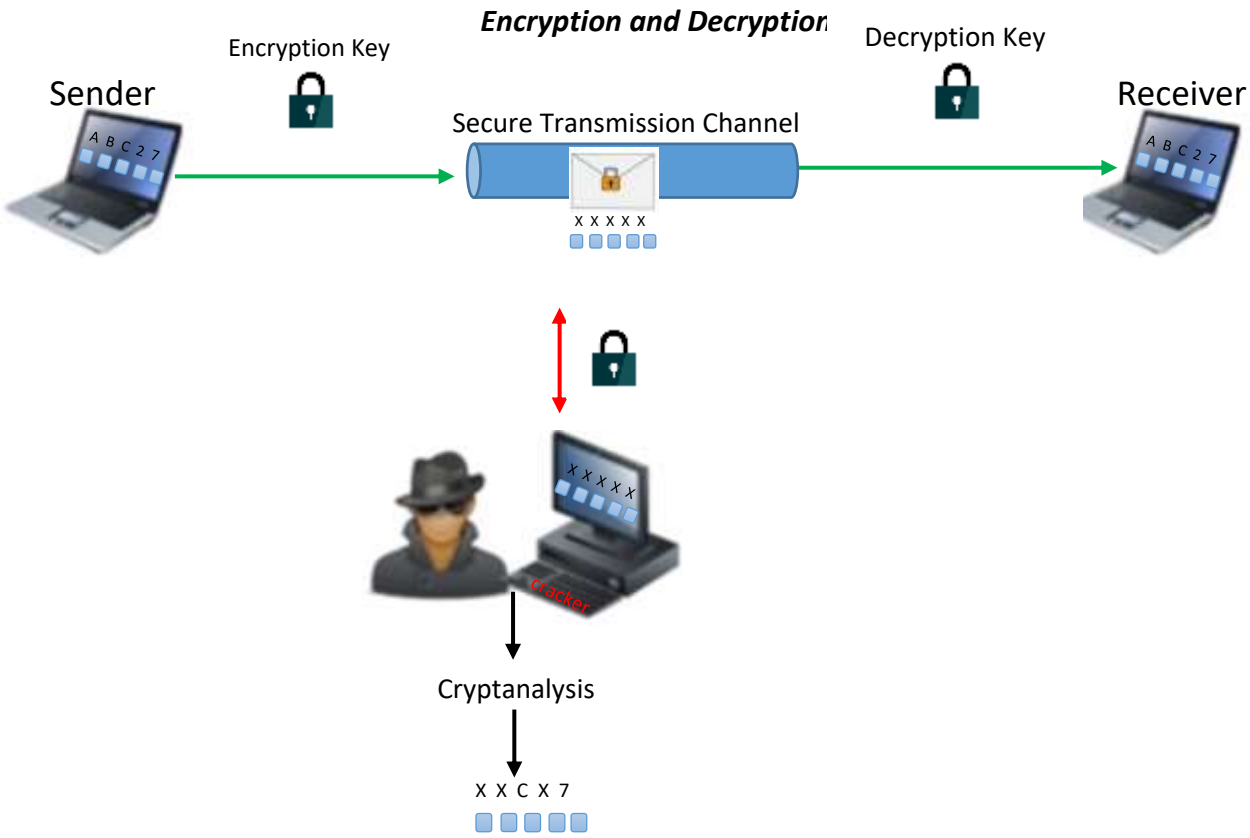


Figure 1: Encryption Diagram

2.2. Definitions and Terminology

- **Plaintext** : This is the information that a sender wants to transmit to a receiver.

- **Cryptology** : The mathematical science of secret messages, encompassing both cryptanalysis and cryptography.
- **Cryptography** : The study of the art of encryption. From the Greek: hidden and writing, cryptography is the study of methods that enable the sending of data confidentially (encrypted) over a given medium.
- **Encrypt** : Synonym of "encipher."
- **Cryptanalysis** : The science of analyzing cryptograms to decrypt them. It is the art for an unauthorized person to decrypt, decode, or decipher a message.
- **Cryptogram** : An encrypted message.
- **Cryptosystem** : An encryption algorithm.
- **Cryptolect** : A vocabulary used by a group of individuals using cryptography.
- **Decrypt** : To recover the plaintext message from the encrypted message without knowing the key.
- **Encryption (Cipher)** : It involves transforming data (text, message, etc.) to make it incomprehensible to an unauthorized person.
- **Key** : This is the parameter involved in and authorizing encryption and/or decryption operations.
- **Code** : The use of substitution at the level of words or phrases to encode.

2.3. Principles of Operation

A sender Youcef wants to send a message to a recipient Nada while avoiding the eavesdropping of Ikram and the malicious attacks of Abbassi. To do this, Youcef agrees with Nada on the cryptosystem they will use. This choice does not need to be secret, in accordance with Kerckhoffs' principle .

- **Encryption (Cipher**) : The message (information) that **Youcef** wants to transmit to **Nada** is the **plaintext**. The process of transforming information (message), **M** , is called encryption (**Cipher**) or encoding. It becomes incomprehensible to **Ikram** . This generates an encrypted message, **C** , (**Ciphertext**) obtained through an encryption function, **E** .

$$C = E(M)$$

- Decryption : The process of reconstructing the plaintext message from the encrypted message is called decryption or decoding and uses a decryption function, **D** . It is required that for any plaintext message **M** :

$$D(C) = D\big(E(M)\big) = M$$

✓ **Fundamental Relationship**

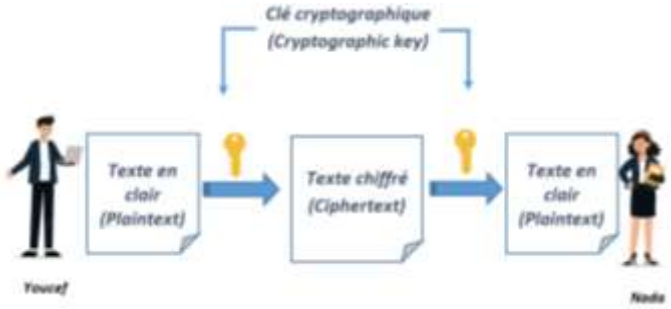
- In practice: **E** and **D** are parameterized by keys **Ke** and **Kd**:

$$C = E_{Ke}(M)$$
$$D_{Kd}(C) = M$$

- **Ke** and **Kd** ∈ key space.
- Defines two categories of cryptographic systems:

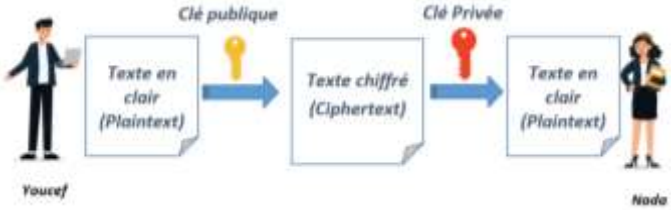
Secret Key Systems (or Symmetric)

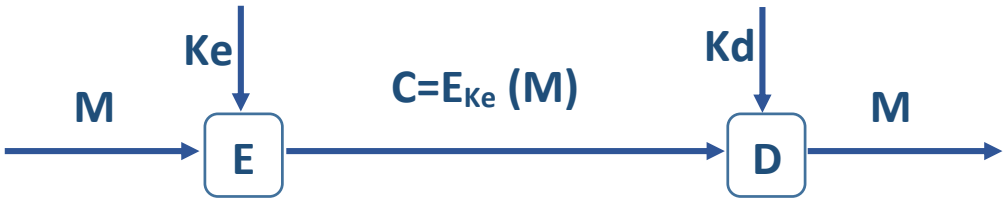
$(Ke = Kd = K)$

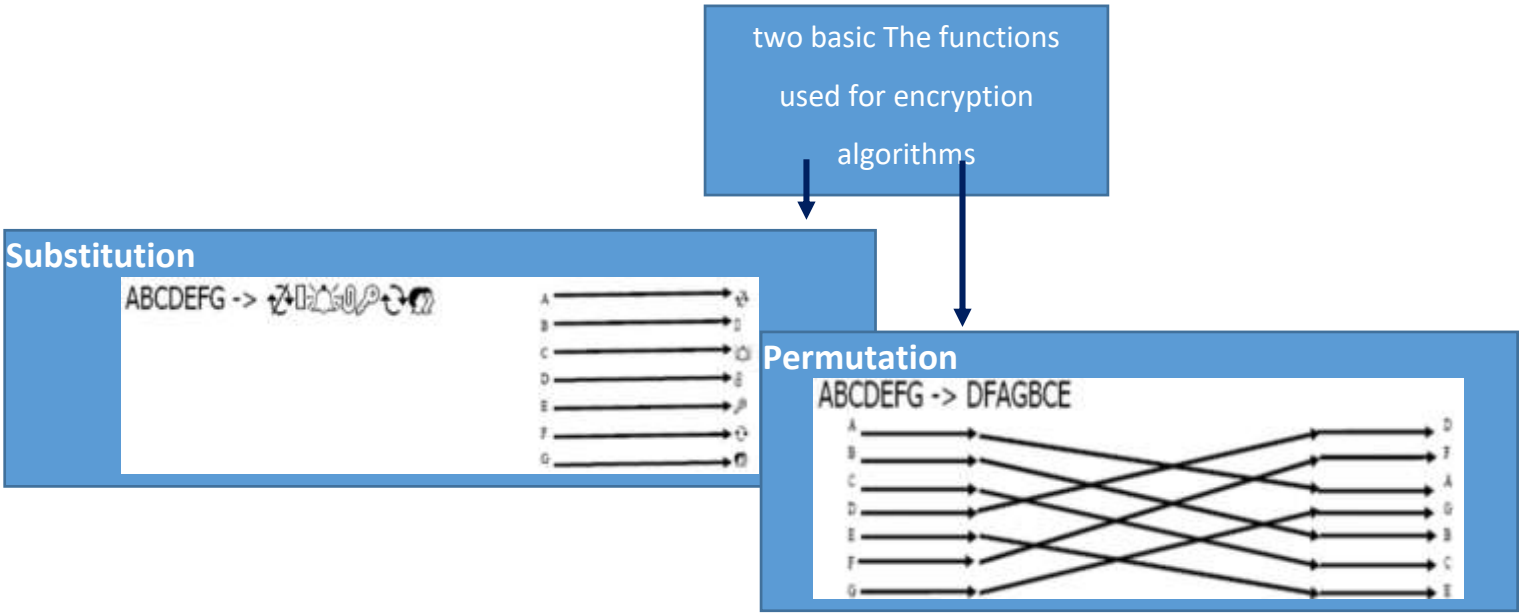


Public Key Systems (or Asymmetric)

$(Ke \neq Kd)$







2.4. Substitution Algorithms

Substitution encryption, or simple encryption, consists of replacing one or more entities in a message with one or more other entities. An entity can be a letter, a byte, or a binary sequence. Several types of substitution encryption exist, including:

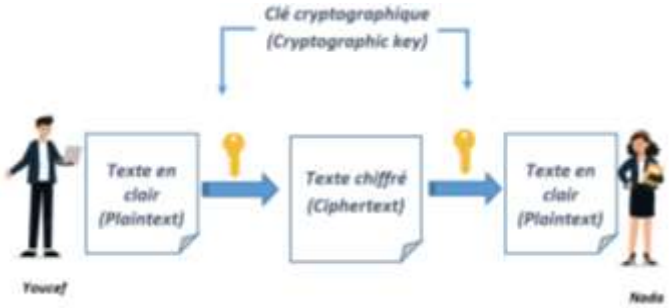
Mono-alphabetic Encryption : Consisting of replacing each character in the message with another character, e.g., Caesar Cipher (Annex A)

Poly-alphabetic Encryption : Using a sequence of mono-alphabetic ciphers reused periodically, e.g., Vigenère Cipher (Annex A)

Homophonic Encryption : Allowing each character in the message to correspond to a possible set of other character groups, e.g., A (23, 9, 33), C (45, 20, 10), C (45, 20, 10)

Polygram Encryption : Consisting of substituting a group of characters in the message with another group. Examples: Playfair Cipher, Hill Cipher, Vigenère Cipher, etc. (Annex A)

2.5. Symmetric Cryptography



Secret Key (or Symmetric) Systems
$(Ke = Kd = K)$

Symmetric encryption algorithms are mainly classified into two categories:

Block cipher

This type of algorithm operates on the plaintext message in blocks of n bits, meaning it takes n bits as input and encrypts them into n bits of output. Typically, data is split into blocks of a fixed size. This size is between 32 and 512 bits, but since 2000, the standard has been 128 bits.

Stream cipher

Stream encryption encrypts variable-length messages and does not need to split them into blocks. Indeed, messages are processed bit by bit based on the Vernam cipher model. The most common algorithms are: RC4, A5/1, and RC5.

The main advantage of symmetric encryption algorithms is their computation time, which is significantly shorter compared to their counterparts (asymmetric encryption algorithms). However, they have the following limitations:

- **Secret Key Length:** According to Shannon (1940), symmetric encryption systems must use keys with a length at least equal to that of the message to be encrypted, to resist all brute-force attacks;

- **Secret Key Exchange:** Symmetric encryption requires having a secure channel for key exchange, which seriously diminishes the interest of such an encryption system;
- **Number of Keys:** Knowing that one key is needed for each exchange, for a group of N users exchanging among themselves, it is necessary to securely distribute N*(N-1)/2 secret keys.

2.5.1. AES Encryption

Advanced Encryption Standard or AES, also known as Rijndael, is a symmetric encryption algorithm and it is the encryption standard for United States government organizations. It was approved by the NSA (National Security Agency).

Key Lengths	n_r (Rounds)
128 bits	10
192 bits	12
256 bits	14

For K a key length of 128 bits

Message (Plaintext) hexadécimale

A_0	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8	A_9	A_{10}	A_{11}	A_{12}	A_{13}	A_{14}	A_{15}

Key

K_0	K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_8	K_9	K_{10}	K_{11}	K_{12}	K_{13}	K_{14}	K_{15}

Stat Matrix

Message

A_0	A_4	A_8	A_{12}
A_1	A_5	A_9	A_{13}
A_2	A_6	A_{10}	A_{14}
A_3	A_7	A_{11}	A_{15}

Cipher Key

K_0	K_4	K_8	K_{12}
K_1	K_5	K_9	K_{13}
K_2	K_6	K_{10}	K_{14}
K_3	K_7	K_{11}	K_{15}

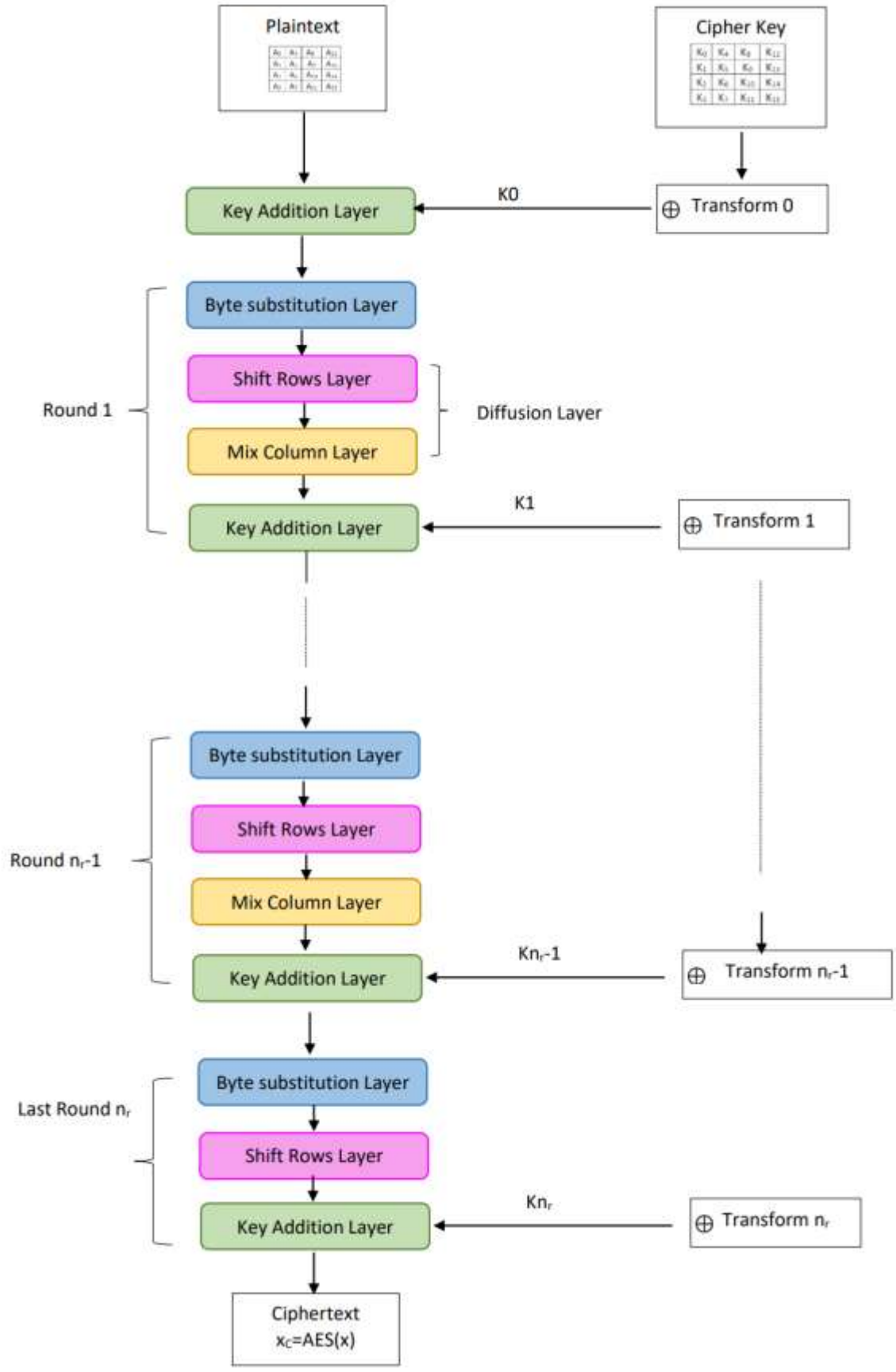


Figure : Block diagram of AES encryption

- **Key Addition Layer**

  - A 128-bit round key, or sub-key, which was derived from the main key in the key schedule, is **XOR** ⊕)with the state.

Plaintext

A_0	A_4	A_8	A_{12}
A_1	A_5	A_9	A_{13}
A_2	A_6	A_{10}	A_{14}
A_3	A_7	A_{11}	A_{15}

⊕

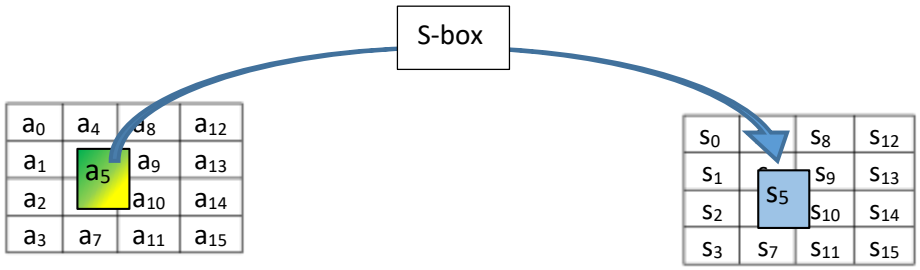
Cipher Key

K_0	K_4	K_8	K_{12}
K_1	K_5	K_9	K_{13}
K_2	K_6	K_{10}	K_{14}
K_3	K_7	K_{11}	K_{15}

=

a_0	a_4	a_8	a_{12}
a_1	a_5	a_9	a_{13}
a_2	a_6	a_{10}	a_{14}
a_3	a_7	a_{11}	a_{15}

- **Byte substitution Layer (S-box):** A non-linear transformation applied independently to each byte of the state using a substitution table (S-box).



Example : for a_5 = {6e}

S_5= SubBytes(a_5) = {9f}

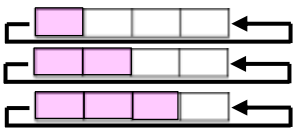
	Y															
	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
X 8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
a	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
b	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
c	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
d	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
e	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
f	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

AES S-box

➢ Shift Rows Layer

Cyclic permutation of the bytes in the rows of the state. The byte shift corresponds to the index of the row considered ($0 \leq r < 4$). The goal of the ShiftRow transformation is to increase the diffusion properties of AES. If the input to the ShiftRows sub-layer is given as a state matrix S_0.....S_{15}:

S_0	S_4	S_8	S_{12}
S_1	S_5	S_9	S_{13}
S_2	S_6	S_{10}	S_{14}
S_3	S_7	S_{11}	S_{15}



Sans décalage

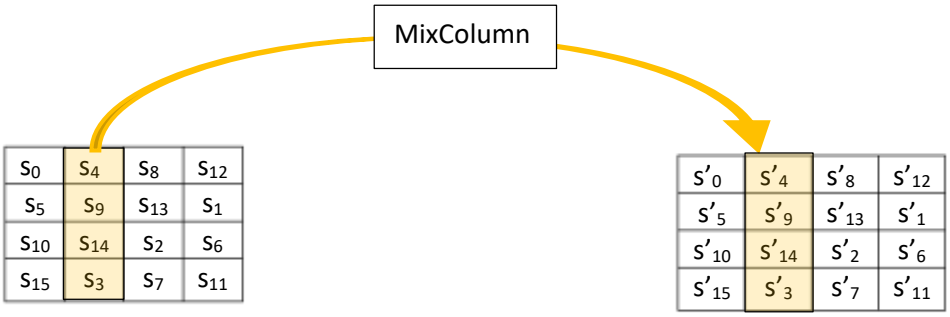
Décalage une position à gauche

Décalage deux positions à gauche

Décalage trois positions à gauche

S_0	S_4	S_8	S_{12}
S_5	S_9	S_{13}	S_1
S_{10}	S_{14}	S_2	S_6
S_{15}	S_3	S_7	S_{11}

- **Mix Column Layer:** This is a linear transformation: a matrix product using the 4 bytes of a column. Columns are treated as polynomials in GF(2^8) and multiplied modulo $x^4 + 1$ with fixed polynomials given in the following figure:



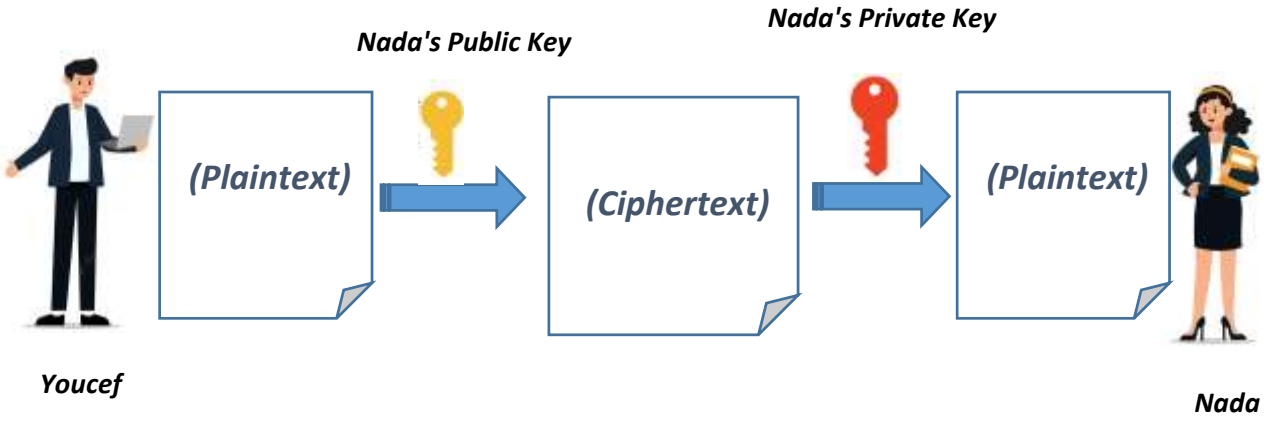
$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_4 \\ s_9 \\ s_{14} \\ s_3 \end{bmatrix} = \begin{bmatrix} s'_4 \\ s'_9 \\ s'_{14} \\ s'_3 \end{bmatrix}$$

2.6. Asymmetric Cryptography

Asymmetric cryptography, or public key cryptography (**PKC**), is based on the existence of one-way functions. It refers to a cryptographic algorithm that requires two distinct keys, one of which is secret (or private, **SK**) and the other public (**PK**). In reality, asymmetric cryptography uses one-way functions with a secret trapdoor. Such a function is difficult to invert unless one possesses specific, secret information called the private key. Asymmetric cryptography appeared in 1976 with the publication of the work on cryptography by Whitfield Diffie and Martin Hellman. It has the following characteristics:

- ✓ A public key PK (symbolized by the vertical key);
- ✓ A secret private key SK (symbolized by the horizontal key);
- ✓ Property: Knowing PK does not allow one to deduce SK;

$$D_{SK}(E_{PK}(M)) = M ;$$



2.6.1. RSA (Rivet Shamir Adelman)

Considered the first asymmetric cryptography algorithm (1978), RSA is named after its creators, Ronald Rivest, Adi Shamir, and Leonard Adleman. Currently, RSA is the most widely used cryptographic system today, having survived all attacks for over a quarter of a century. The reliability of this algorithm is based on the difficulty of solving a very complex mathematical problem, known as factorization, which requires many operations and a large memory space.

The RSA algorithm is based on three steps:

1) Key Generation (by the same person, Nada)
2) Message Encryption
3) Message Decryption

RSA

Key Generation

Nada performs the following operations:

- Choose two distinct prime numbers **p** and **q**

-Calculate $n = p\,x\,q$

- Calculate $\varphi(n) = (p-1) \times (q-1)$

- Choose an encryption exponent, a natural integer **e**, coprime with$\varphi(n)$ et $e < \varphi(n)$ such that $pgcd(\mathrm{e}, \varphi(n)) = 1$

- Calculate the integer **d**, a decryption exponent, the inverse of **e** modulo$\varphi(n)$ et $d < \varphi(n)$; d can be calculated efficiently using the extended Euclidean algorithm.. $d \times e \equiv 1 mod(\varphi(n))$

The pair (**n, e**) is the public encryption key, the number **d** is her private key (Nada keeps the private key for herself).

Message Encryption

- Youcef wants to send a secret message to Nada
- If **M** is the message to send$0 \leq M < \mathrm{n}$, M=10
- The encrypted message to transmit will be $C \equiv M^e mod(n)$

Message Decryption

- To decrypt C, one uses d, and finds the plaintext message M: $M \equiv C^d mod(n)$

Example:

Bob wants to send a message M=10 to Alice. Alice has chosen p=5 and q=17 as the two prime numbers for RSA encryption.

- Give the public key ''(n, e)'' calculated by Alice
- Give the private key ''d'' calculated by Alice
- Give the message transmitted by Bob

SOLUTION

$n = p \times q$=85 $\varphi(n) = (p-1) \times (q-1) = 64$

$$e = 5 \ tel\ que\ pgcd((5,64) = 1$$

$$d \times e \equiv 1 mod\Big(\varphi(n)\Big), 13 \times 5 \equiv 1 mod(64)$$

$$PK = (85,5) \quad PS = 13$$

Exemple $M = 10$

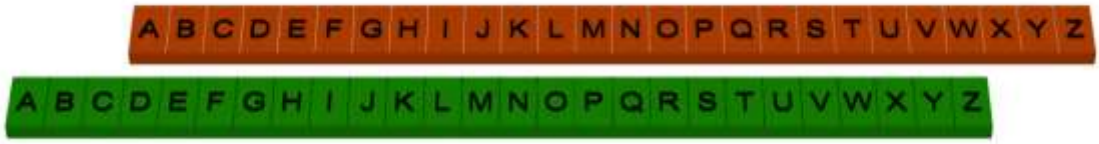
$C \equiv 10^5 mod(85) \quad \overset{1}{\Rightarrow} 10^5 \equiv C\ mod(85)$

$\overset{1}{\Rightarrow} C = 85k + 10^5 \ \overset{1}{\Rightarrow} k\ entier\ si\ on\ suppose \quad \overset{1}{\Rightarrow} 10^5 = 85k + C \overset{1}{\Rightarrow} 10^5 - 85k = C\ ,\ C = 40$

ANNEX A

1- The Caesar Cipher

Here is a figure with the original alphabet on top in **red**, corresponding to the encryption alphabet below in **green**.



We will adopt the following convention: in **green** is the part of the message that everyone has access to (or that could be intercepted), so it is the encrypted message. Whereas in **red** is the confidential part of the message, it is the plaintext message.

(plaintext) : ''hello'' with key K=3

$$hello \rightarrow khoor$$

$C(h) \rightarrow k$,$C(e) \rightarrow h$, $C(l) \rightarrow o$, $C(l) \rightarrow o$, $C(o) \rightarrow r$

To also account for the last letters of the alphabet, it is more appropriate to represent the alphabet on a ring. This shift is a circular shift on the letters of the alphabet.

There are 26 possible keys.

To also account for the last letters of the alphabet, it is more appropriate to represent the alphabet on a ring. This shift is a circular shift on the letters of the alphabet.

Mono-alphabetic substitution

We now associate each letter with another letter (without a fixed order or general rule).

Here K is composed of 26 letters.

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

There is $26! = 1 \times 2 \times 3 \times \ldots\ldots \times 26$ possible keys

2- Vigenère Cipher

We group the letters of our text into blocks, for example here into blocks of length 3:

To encrypt the message:

For a key of length k, there are k 26^K possible keys

3- Playfair Cipher

The Playfair algorithm uses a 5x5 matrix constructed using the secret key. This matrix is filled with the letters of the key, excluding duplicates (example: 'informatique' becomes 'informatque'), from left to right and top to bottom. The remaining cells of the matrix are filled with the remaining letters in alphabetical order (the letters I and J count as a single letter). Example (Playfair matrix with the key 'informatique') :

key = **CIPHER** , the message (plain text)**logger** , the digramme is **log x ge rx**

- Repeated letters in the same digram are separated by a null, usually X: **logger lo gx ge rx**
- Two letters in the same row are each replaced by the one to the right: DF becomes FR
- Two letters in the same column are each replaced by the one below: AQ becomes KW
- Otherwise, each digram is encrypted according to their row and column:
  LO becomes GS and GE becomes NC

- To encrypt the message: **logger** the bigrams are **lo gx ge rx**

The encrypted message is then: GS LV NC BV

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

ANNEX B

Caesar's cipher with Python

Program

```
def caesar_cipher(text, shift, mode='encrypt'):
    """
    Enhanced Caesar cipher with mode selection.

    Args:
        text: Input message
        shift: Shift value (1-25 recommended)
        mode: 'encrypt' or 'decrypt'

    Returns:
        Processed message
    """
    if mode == 'decrypt':
        shift = -shift

    result = []

    for char in text:
        if char.isalpha():
            # Determine base ASCII value
            base = ord('A') if char.isupper() else ord('a')
            # Apply shift with wrapping
            shifted = (ord(char) - base + shift) % 26
            result.append(chr(base + shifted))
        else:
            result.append(char)
```

```
    return ''.join(result)


# Demonstration
message = "All the tasks of the mission are completed"
shift = 5

encrypted = caesar_cipher(message, shift, 'encrypt')
decrypted = caesar_cipher(encrypted, shift, 'decrypt')

print(f"Original: {message}")
print(f"Encrypted: {encrypted}")
print(f"Decrypted: {decrypted}")
```

Chapter 3: Firewall Security

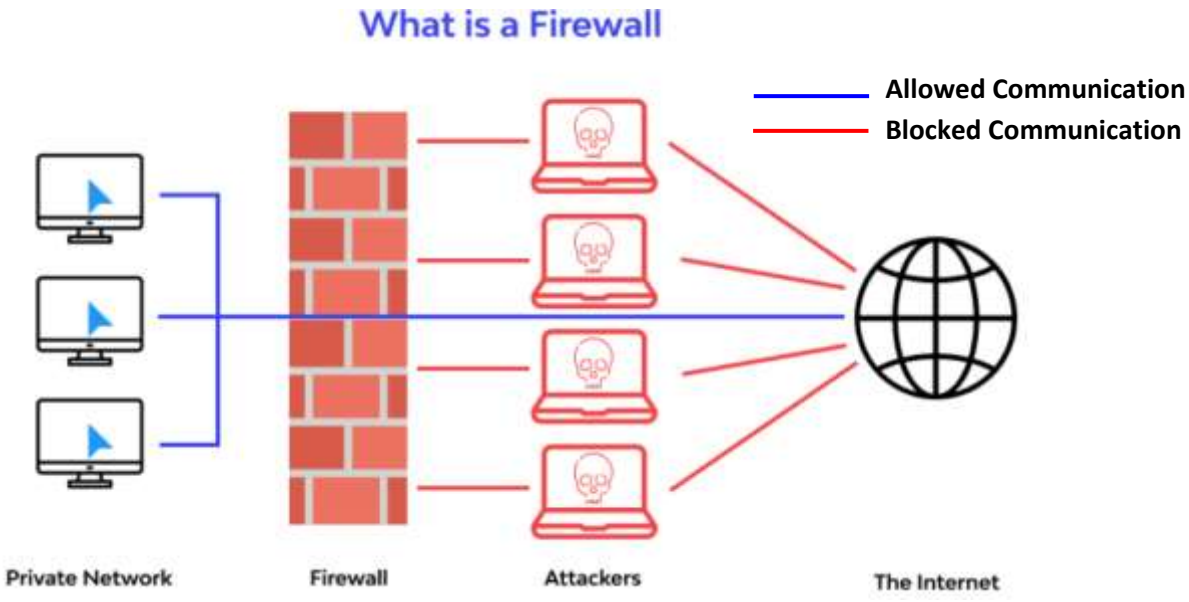
3.1. Introduction

A **firewall** is a software or hardware system installed on a machine or router that controls communications passing through a given network. This mechanism protects a private network from certain intrusions originating from an external network (e.g., the internet), such as outgoing communications triggered by installed malware. Furthermore, its function is to enforce the network security policy, which defines which communications are allowed or prohibited.

It is essentially a filtering gateway that includes at least the following network interfaces:

- An interface for the network to be protected (internal network);
- An interface for the external network.

-



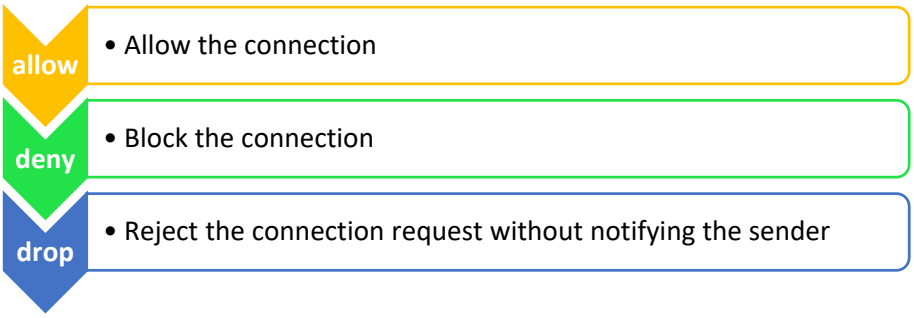
It is possible to set up a firewall system on any machine and with any operating system provided that:

- The machine is powerful enough to handle the traffic;
- The system is secure;

- No service other than packet filtering is running on the server. When the firewall system is provided as a "turnkey" black box, the term "Appliance" is used.

3.2. How a Firewall System Works

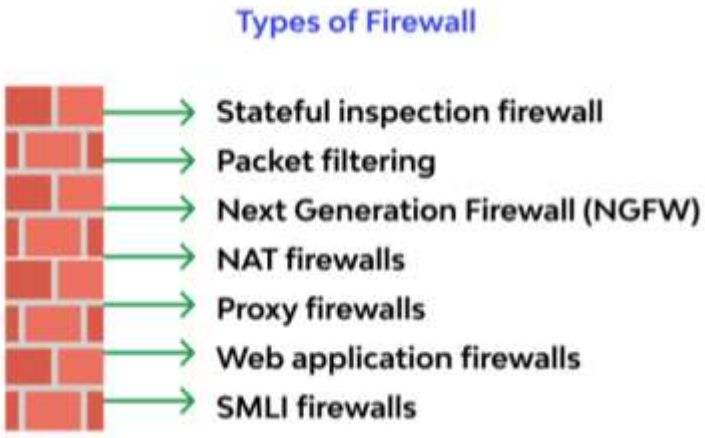
A firewall system contains a set of predefined rules that allow it to:



3.3. Principle

The firewall acts as a filter and can therefore operate at various levels of the OSI model. There are three main types of firewalls:

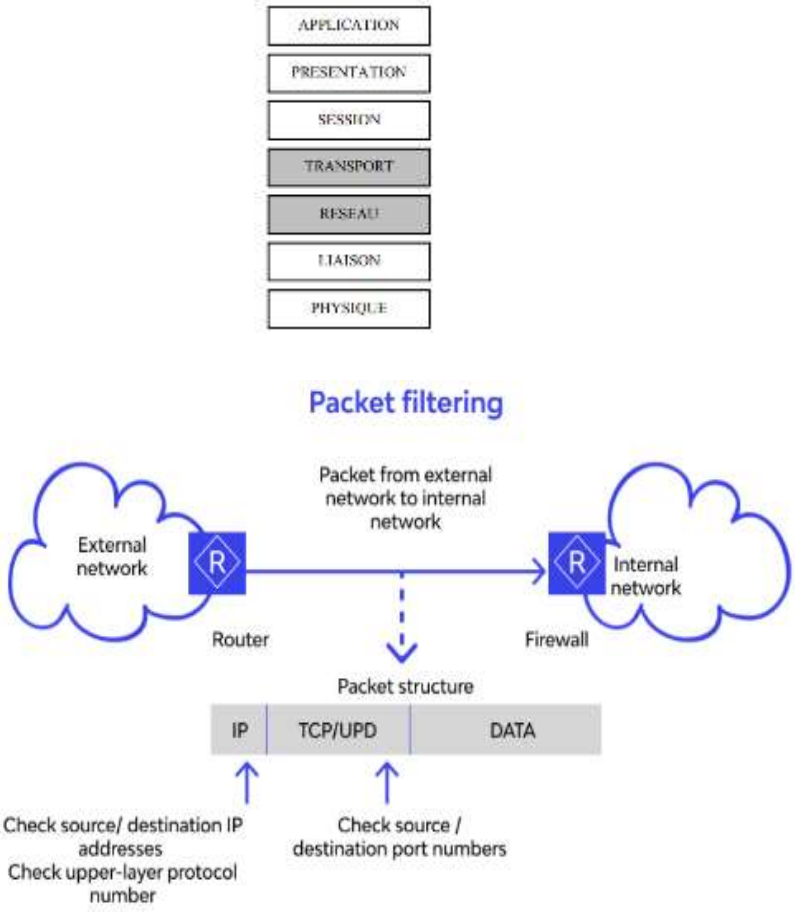
- Packet filtering
- Stateful packet filtering (stateful firewall)
- Proxy



3.3.1 Packet Filtering

Packet-filtering firewalls are typically routers that grant or deny access based on the following elements:

- Source address
- Destination address
- Protocol
- Port number



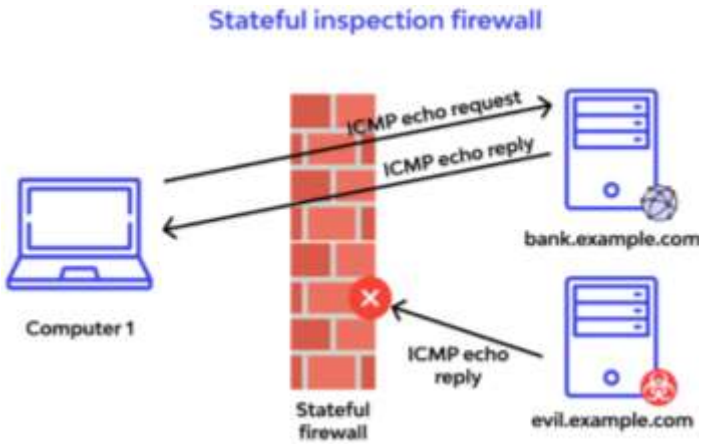
A packet-filtering firewall inspects each data packet the moment it passes through. It checks the packet's source and destination addresses, as well as its source and destination port numbers. If the packet does not comply with the firewall's rule set, it is dropped—meaning it is not forwarded to its intended destination.

For example, a firewall configured to block Telnet access will drop all packets destined for Transmission Control Protocol (TCP) port 23, which is the default port used by Telnet server applications.

This type of firewall operates primarily at the network layer (Layer 3) of the OSI model, but it also utilizes the transport layer (Layer 4) to acquire the port numbers. It examines each packet in isolation and has no awareness of whether it is part of an existing connection or traffic stream.

3.3.2 Stateful Firewall

Stateful technology is one of two possible responses to the limitations of packet filtering. A stateful firewall includes all the functionalities of a packet filter and adds the ability to keep track of sessions and connections in internal state tables. Any data exchange is subject to its approval, and it adapts its behavior based on states. This technique is suitable for connection-oriented protocols (TCP). Some protocols (UDP and ICMP) pose an additional challenge: they have no inherent connection concept. The firewall must therefore examine the packets and can only manage timeouts, often around one minute.



Stateful inspection firewalls—also referred to as dynamic packet-filtering firewalls—monitor communication packets over time and examine both incoming and outgoing traffic.

This type of firewall maintains a state table that tracks all active connections. When a new packet arrives, it compares the information in the packet's header to its state table—a log of legitimate connections—to determine if the packet is part of an established session. If it is, the packet is allowed to pass without further analysis. If the packet does not correspond to an existing connection, it is evaluated against the firewall's rule set for new connection requests.

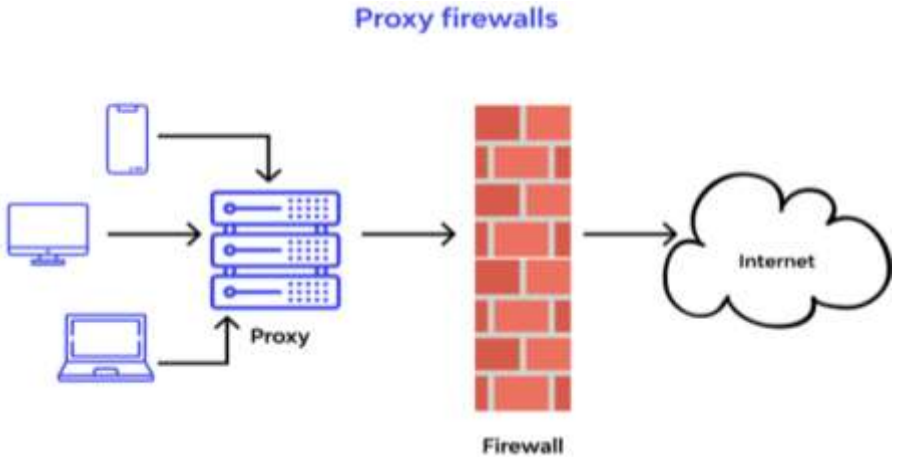
Although stateful inspection firewalls are highly effective, they can be vulnerable to Denial-of-Service (DoS) attacks. Such attacks exploit the trust this firewall type places in established connections that it assumes are legitimate.

3.3.3 Proxy

Application proxy firewalls (or application gateways) aim to address the problems raised by packet filters and stateful firewalls. These systems act on behalf of the server or client they are tasked with protecting by:

- Processing requests and responses instead of the system to be protected,
- Transmitting them after possible modifications,
- Or blocking them.

Firewalls of this type act as a channel and interpreter by operating on Application layer protocols. This approach, in principle, allows for the highest level of security.



3.3.4 Other Firewall Capabilities

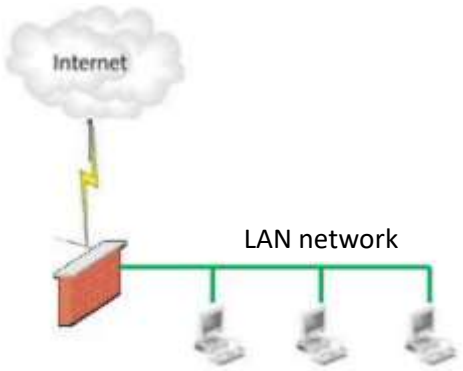
Firewall manufacturers tend to integrate a maximum number of functionalities:

- **Content filtering** (URL, spam emails, ActiveX code, Java applets, ...)
- **Virtual Private Network (VPN)**: VPNs allow secure traffic to be channeled from one point to another across typically hostile networks (e.g., the Internet). Checkpoint and Cisco integrate VPN services into their firewall offerings.
- **Network Address Translation (NAT)**: This service allows the mapping of reserved or illegal addresses to valid addresses. The first NAT devices that appeared in enterprises were often firewall products.

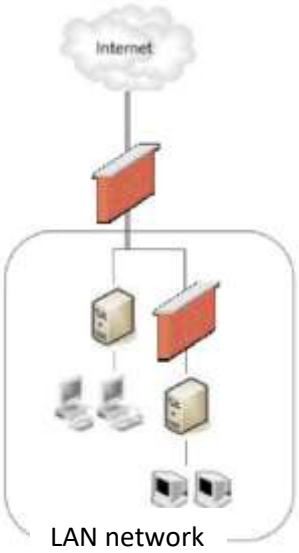
- **Load balancing**: Allows traffic to be segmented in a distributed manner (e.g., directing Web and FTP traffic).
- **Fault tolerance**: Some firewalls, such as CISCO/PIX or Nokia/Checkpoint, support these functionalities (usually with firewalls deployed in pairs to enable high availability (HA)).
- **Intrusion Detection System (IDS)**: A new and trendy service!

3.4 Different Firewall Architecture Types

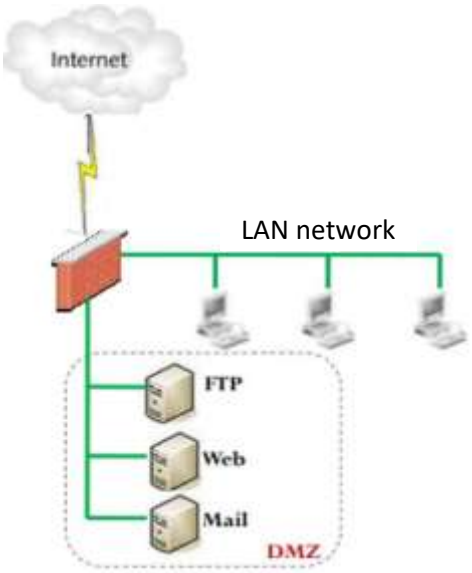
Architecture with a single central firewall: In this architecture, the firewall is positioned between the LAN and the WAN. Filtering is done only at Layer 3 (IP filtering) and Layer 4 (port filtering).



Architecture with multiple firewalls: In this architecture, in addition to the firewall between the LAN and the WAN, another firewall can be added between two internal networks. This can protect a sensitive internal network from attacks originating from another internal network within the company.



Architecture with a Demilitarized Zone (DMZ): If a company needs one of its servers to be accessible from the Internet but wants to protect its internal network, the first step is to divide the company's network into several segments: the internal network part and the part containing servers accessible from the Internet, called the Demilitarized Zone (DMZ).



Chapter 4: Virtual Private Networks (VPN)

4.1 Introduction

VPN stands for Virtual Private Network. It is a technology that allows data to be sent between computers belonging to distant sites, via a public Internet in the same way as if it were a private point-to-point link. It is important to understand this model: a private network is built using software on top of a public infrastructure (the Internet or an operator's network).

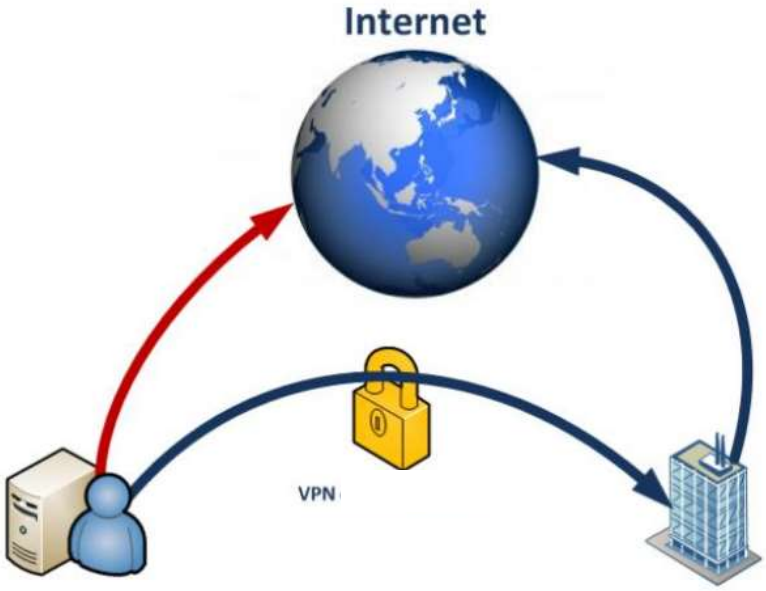
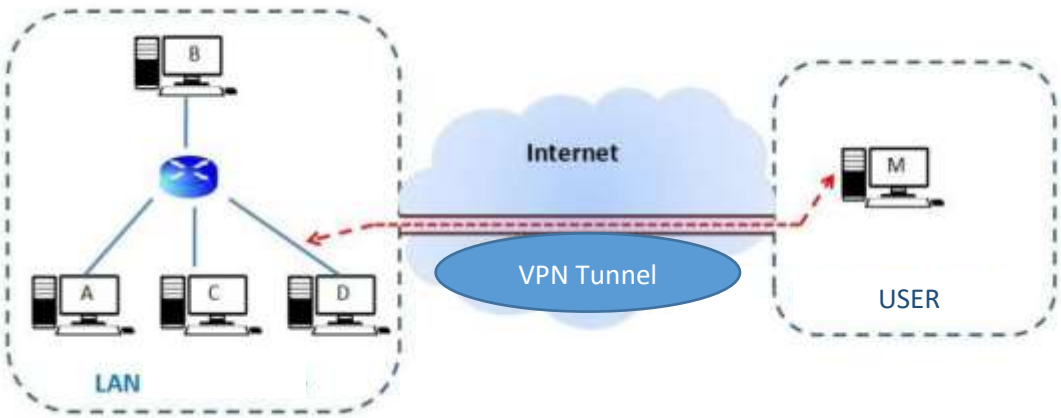


Fig.1 principle of a VPN

To make a private network "virtual" within the Internet, a VPN creates what is called a "tunnel".



The VPN tunnel must be able to meet the following points:

- **Authentication:** Only authorized persons can connect to the VPN (identity verification using a unique code, for example).
- **Integrity:** Data traveling through the tunnel must arrive at the destination as they were sent, without loss or modification.
- **Data Security:** Only authorized persons can read the packets transiting through the tunnel. Data must be protected by encryption.

In addition to the points above that a tunnel must ensure, a VPN service must be able to manage encryption keys between the client and the server and must support the most commonly used protocols on public networks, such as the IP protocol.

4.2 Modes of VPN Use

A virtual private network can be used in two ways:

- **Intranet or Extranet VPN (LAN-to-LAN):** Allows two LANs to be connected. The extranet allows, for example, a company to connect with its partners or clients. As for the intranet VPN, it allows, for example, two remote servers of the same company to be connected securely.
- **Access VPN (Host-to-LAN):** Allows, for example, a remote worker to connect to their company's local network remotely to work, access private data, or communicate with their colleagues who may also be connected via VPN. Requires an access code for each VPN connection.

4.3 Operating Principle

A VPN network is based on a protocol called a "tunneling protocol". This protocol allows company information to flow encrypted from one end of the tunnel to the other. Thus, users feel as if they are connecting directly to their company's network.

The tunneling principle involves building a virtual path after identifying the sender and the recipient. Subsequently, the source encrypts the data and routes it using this virtual path. To provide easy and low-cost access to corporate intranets or extranets, access virtual private networks simulate a private network, while they actually use a shared access infrastructure, such as the Internet.

The data to be transmitted can be handled by a protocol other than IP. In this case, the tunneling protocol encapsulates the data by adding a header. Tunneling is the set of encapsulation, transmission, and decapsulation processes.

4.4 Functionalities

A secure VPN system must be able to implement the following functionalities:

– User Authentication: Only authorized users should be able to identify themselves on the virtual network. A history of connections and actions performed on the network can be defined and kept. Conversely, the client may also need to authenticate the server to protect itself from fake VPN servers.

– Address Management: Each client on the network has a private and confidential address. A new client must be able to connect easily to the network and receive an address.

– Data Encryption: During their transport over the public network, data must be protected by effective encryption.

– Key Management: Encryption keys for the client and server must be able to be generated and regenerated.

– Multiprotocol Support: The VPN solution must support the most commonly used protocols on public networks, particularly IP.

4.5 VPN Protocols

a) **Layer 2 Protocols:** PPTP, L2TP both encapsulate the payload data in a PPP frame which will be transmitted across the Internet.

FIg.2 Client Configuration on Windows 7

- The tunnel is similar to a session.
- The two ends of the tunnel must agree and must negotiate configuration variables, address assignment, encryption and/or compression parameters.
- A mechanism for tunnel management and maintenance.

b) **Layer 3 Protocols:** IPSec encapsulates IP packets within another IP packet before sending it over the Internet.

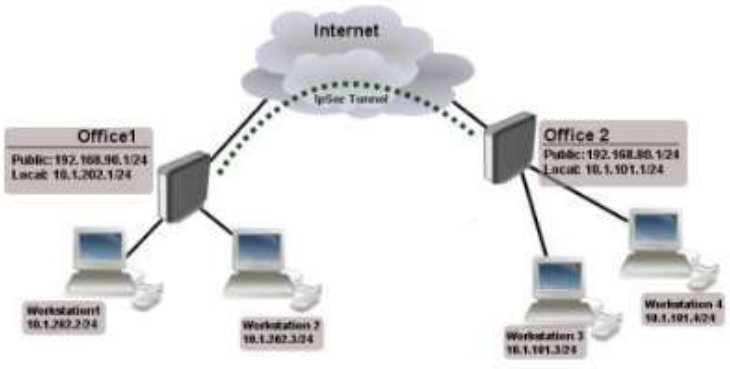


Fig. 3 – IPSEC Tunnel

- The variables are pre-configured.
- No tunnel maintenance phase.

c) **Layer 4 Protocols:** Uses TLS/SSL to secure exchanges at the Transport layer.

4.6 Advantages of a VPN

The VPN service offers several advantages. The first advantage is to ensure secure and encrypted communication between multiple sites. The second advantage concerns the simplicity of its use. Indeed, the VPN uses the circuits of existing public telecommunication networks. The third advantage is its cost of use. Since the VPN uses the Internet as a transport mode, this avoids additional costs for creating a dedicated line.

Chapter 5: Switch Security

(*Concepts of VLANs, Attacks, and Data Link Layer Responses)*

This chapter provides a deep dive into the security of switched networks at the Data Link Layer . Students will learn that network security is not solely an IP-based concern. The module covers the fundamental concepts of VLANs for segmentation, explores inherent vulnerabilities in Layer 2 protocols, and details common attacks such as MAC table flooding, VLAN hopping, ARP poisoning, and STP manipulation. A strong emphasis is placed on practical mitigation techniques and best practices to harden network infrastructure.

5.1. Introduction

In modern computer networks, **switches** play a critical role in enabling efficient data transmission at the **data link layer (Layer 2)** of the OSI model. While switches increase performance and segment traffic effectively, they are not immune to security threats. As networks grow in complexity, **securing switches** becomes essential to protect data integrity, confidentiality, and availability.

This chapter explores the fundamental concepts of **switch security**, focusing on **Virtual Local Area Networks (VLANs)**, common **Layer 2 attacks**, and the corresponding **defensive mechanisms** that can be employed to mitigate these threats. VLANs are widely used to logically segment network traffic for performance, management, and security benefits. However, misconfigurations and vulnerabilities in VLAN implementations can lead to severe security breaches, including **VLAN hopping**, **MAC flooding**, and **ARP spoofing**.

To address these challenges, network administrators must implement **Layer 2 security best practices** such as port security, dynamic ARP inspection, and VLAN pruning. Additionally, understanding the underlying principles of how these attacks operate enables proactive network defense.

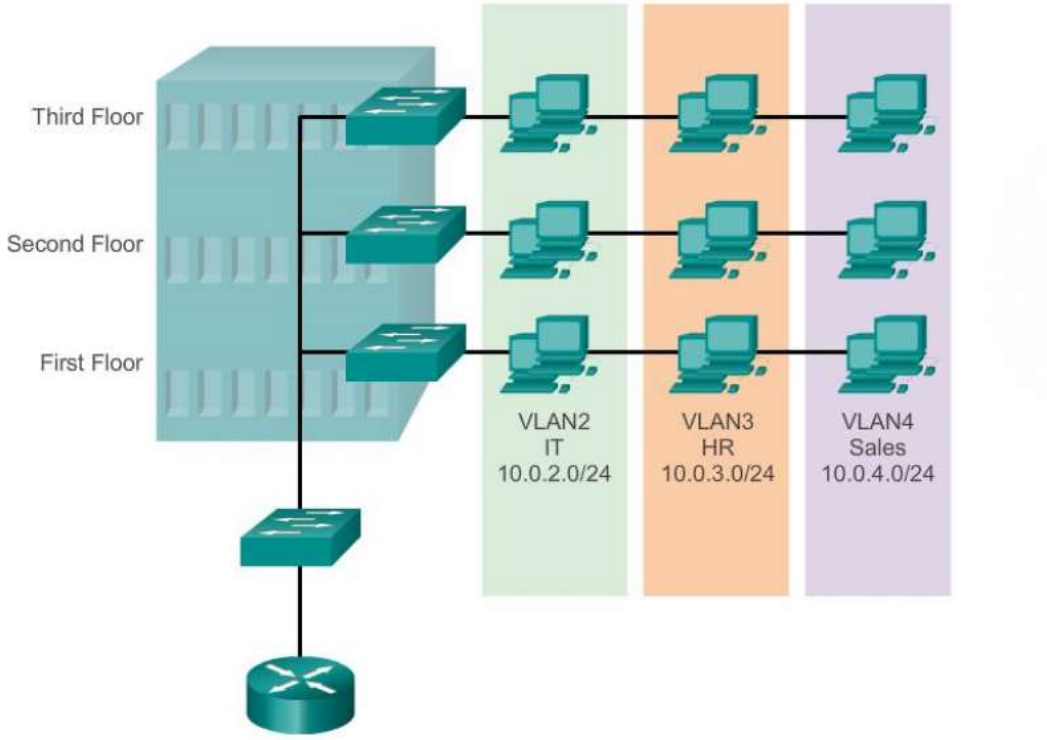
By the end of this chapter, readers will gain a clear understanding of how switches can be both a **target and tool** in network security, and how **data link layer responses** play a critical role in maintaining a secure and resilient network infrastructure.

5.2. VLAN and Segmentation

5.2.1. Virtual Local Area Network (VLAN): is a logical subdivision of a physical network. VLANs allow network administrators to segment traffic, improve security, and optimize performance by grouping devices—even if they are not physically located on the same switch—into a single broadcast domain.

VLAN Definitions

- VLAN (virtual LAN) is a logical partition of a layer 2 network.
- Multiple partition can be created, allowing for multiple VLANs to co-exist.
- Each VLAN is a broadcast domain, usually with its own IP network.
- VLANs are mutually isolated and packets can only pass between them through a router.
- The partitioning of the layer 2 network takes inside a layer 2 device, usually a switch.
- The hosts grouped within a VLAN are unaware of the VLAN's existence.



5.2.2. Benefits of VLANs: VLANs allow network administrators to:

- ✓ Improve **security** by isolating groups of users.
- ✓ Reduce **broadcast traffic**.
- ✓ Simplify **management** of devices and policies.
- ✓ Support **multi-tenancy** and scalability.
- ✓ **Cost** reduction

- ✓ Better **performance**
- ✓ Improved **IT staff efficiency**

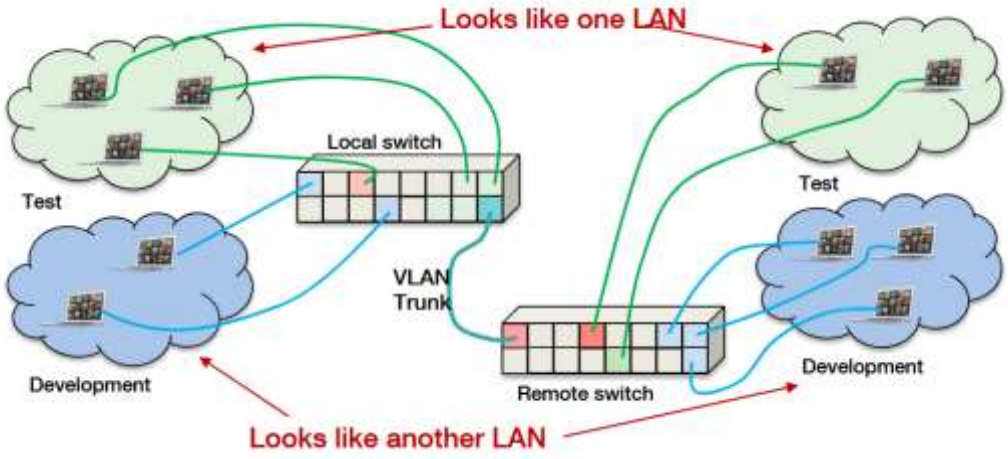
5.2.3. VLAN Characteristics

- Devices in the same VLAN behave as if they are connected to the same physical switch, even if they are on different switches.
- VLAN membership can be assigned by:
  - ✓ **Port-based VLANs** – a switch port is mapped to a VLAN.
  - ✓ **MAC-based VLANs** – assignment by device MAC address.
  - ✓ **Protocol/Policy-based VLANs** – using higher-layer rules.

5.2.4. VLAN Tagging and Trunking

- **IEEE 802.1Q** tagging adds a VLAN ID into Ethernet frames.
- **Access Port:** Belongs to one VLAN; untagged traffic only.
- **Trunk Port:** Carries multiple VLANs using tagging.

VLAN Trunking: a single connection between two VLAN-enabled switches carries all traffic for all VLANs



5.2.5. Types of VLANs

- Data VLAN
- Default VLAN
- Voice VLAN
- Native VLAN
- Management VLAN

VLAN 1

```
Switch# show vlan brief

VLAN Name                Status    Ports
---- ------------------- --------- -------------------------
1    default             active    Fa0/1,  Fa0/2,  Fa0/3,  Fa0/4
                                   Fa0/5,  Fa0/6,  Fa0/7,  Fa0/8
                                   Fa0/9,  Fa0/10, Fa0/11, Fa0/12
                                   Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                   Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                   Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                   Gi0/1,  Gi0/2
1002 fddi-default        act/unsup
1003 token-ring-default  act/unsup
1004 fddinet-default     act/unsup
1005 trnet-default       act/unsup
```

- All ports assigned to VLAN 1 to forward data by default.
- Native VLAN is VLAN 1 by default.
- Management VLAN is VLAN 1 by default.
- VLAN 1 cannot be renamed or deleted.

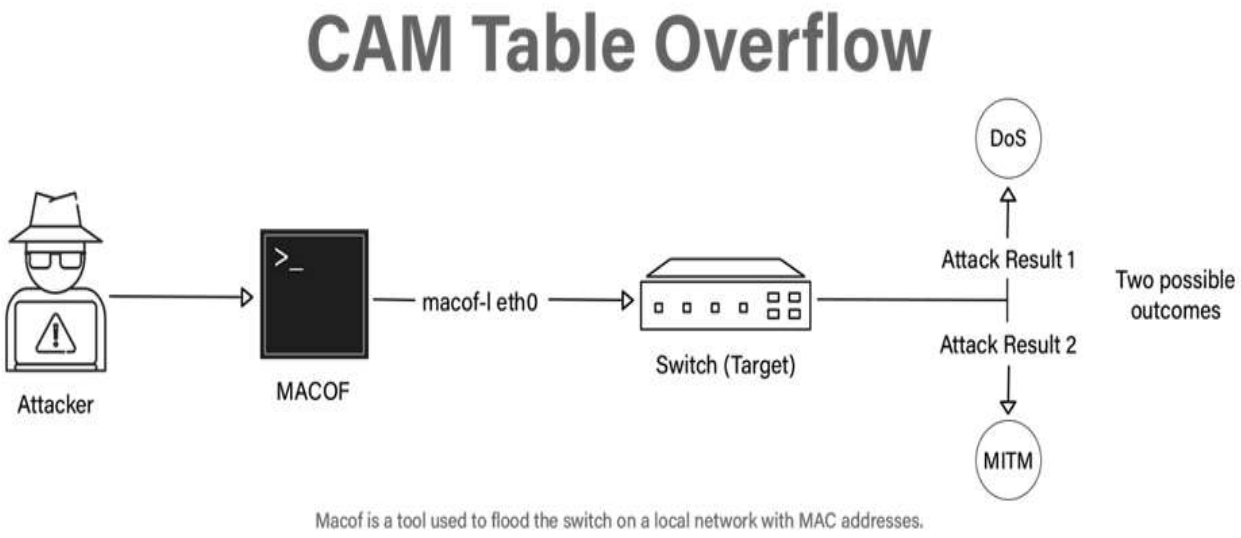
5.3. Layer 2 Attacks and Mitigations

Layer 2 (Data Link Layer) is vulnerable to several security threats because Ethernet and switches were originally designed for performance, not security.

5.3.1. Common Layer 2 Attacks

1. **MAC Flooding**

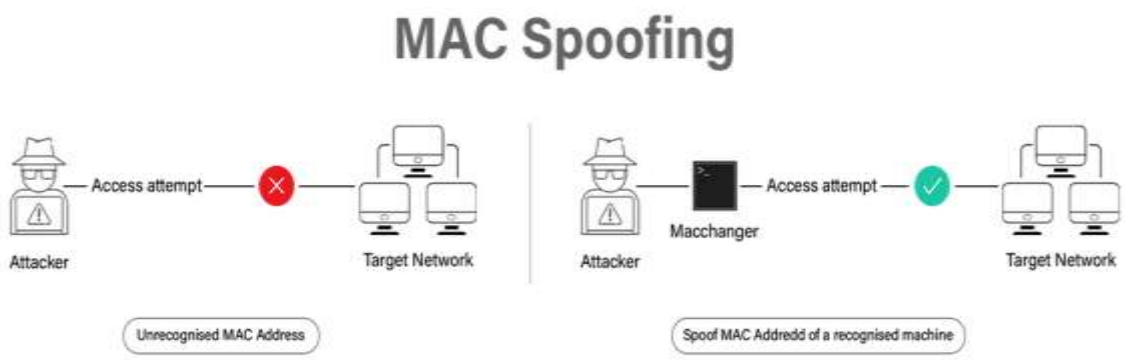
   - Attacker floods switch CAM table with fake MAC addresses.
   - Switch fails open → behaves like a hub → sends frames to all ports (data sniffing).



Mechanism of a CAM Table Overflow Attack :A CAM Table Overflow attack exploits the limited memory allocated for a switch's Content Addressable Memory (CAM) table. In this attack, a malicious actor floods the switch with a high volume of Ethernet frames, each containing a forged source MAC address. The switch, designed to learn and record each new source address, attempts to populate its CAM table with these fictitious entries. Once the table's capacity is exhausted, the switch can no longer learn legitimate MAC addresses. This condition forces the switch to fail-open, meaning it reverts to hub-like behavior. In this state, instead of forwarding frames intelligently only to the correct port, the switch broadcasts incoming traffic out of all ports within the same VLAN. This loss of segmentation enables the attacker to intercept data intended for other hosts, facilitating eavesdropping and man-in-the-middle (MITM) attacks.

2. **ARP Spoofing/Poisoning**

- Attacker sends fake ARP replies.
- Can redirect traffic (MITM) or cause DoS.



MAC Spoofing: Mechanism and Mitigation : MAC spoofing is a network attack that exploits the inherent trust model of the MAC (Media Access Control) layer. It involves an attacker altering the factory-assigned MAC address of their network interface to impersonate an authorized device on the network. This attack subverts network access control mechanisms that rely solely on MAC address filtering for authentication, a method known as MAC Authentication Bypass (MAB).

The feasibility of MAC spoofing stems from the fact that a MAC address is a configurable software value, not a immutable hardware fixture. This allows an attacker to easily change their device's MAC address to match that of a trusted target. A successful spoof can enable a range of threats, including the establishment of rogue access points or the simulation of a legitimate wireless network to harvest user credentials through eavesdropping and man-in-the-middle attacks.

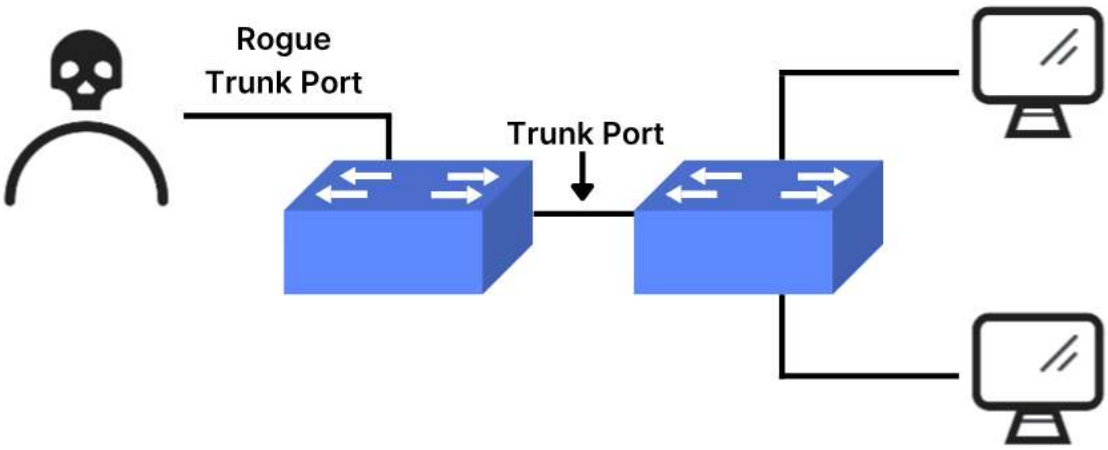
The compromise of a single device via MAC spoofing can serve as a pivot point, potentially allowing the attacker to gain a foothold and move laterally to compromise other systems within the network. To mitigate this risk, a defense-in-depth strategy is essential. Key measures include:

- Disabling unused switch ports to reduce the attack surface.
- Implementing port security features that enforce allowed MAC addresses and limit their number.

- Augmenting or replacing weak authentication like MAB with more robust methods, such as 802.1X, Multi-Factor Authentication (MFA), and digital certificates.

3. **VLAN Hopping**

   - Attacker sends double-tagged packets to escape their VLAN.
   - Gaining unauthorized access to other VLANs.

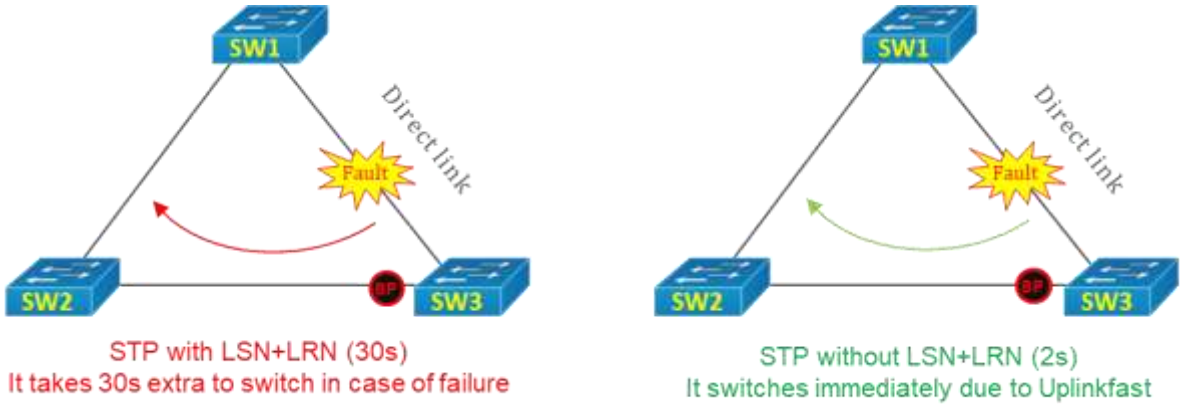


4. **DHCP Attacks**

   - **Rogue DHCP Server:** Provides malicious IP/gateway.
   - **DHCP Starvation:** Exhausts pool of IPs.

5. **STP (Spanning Tree Protocol) Manipulation**

- Attacker sends BPDU messages to become root bridge, controlling traffic paths.



Mechanism of a Spanning Tree Protocol (STP) Attack : Spanning Tree Protocol (STP) is designed to prevent Layer 2 bridging loops in a switched network by logically disabling redundant paths, thereby eliminating the risk of broadcast storms.

The protocol establishes a hierarchical topology by electing a single root bridge, which serves as the central reference point for all path calculations. This election is based on a combination of bridge priority and MAC address, with the lowest value winning. An STP attack occurs when a malicious actor introduces a rogue switch into the network, configured to pose as the root bridge. This is achieved by advertising Bridge Protocol Data Units (BPDUs) with a bridge priority superior to (lower than) that of the legitimate root bridge. Upon receiving these forged BPDUs, other switches in the network trigger a Topology Change Notification (TCN), forcing a full STP recalculation to converge on the new, illegitimate root. This malicious recalculation causes significant network disruption.

During the convergence process, which can take 30-50 seconds, all user traffic is typically blocked on affected ports. Furthermore, the attacker's switch is placed at the center of the new topology, potentially allowing it to intercept a vast portion of the network's traffic for man-in-the-middle attacks.

5.3.2. Mitigations

- **For MAC Flooding:**
  - Enable **Port Security** (limit number of MACs per port).
  - Use **sticky MACs** to bind known addresses.

- **For ARP Spoofing:**
  - Use **Dynamic ARP Inspection (DAI)**.
  - Implement **static ARP entries** for critical systems.
- **For VLAN Hopping:**
  - Disable **unused switch ports**.
  - Set unused ports as **access ports in an unused VLAN**.
  - Disable **DTP (Dynamic Trunking Protocol)**.
- **For DHCP Attacks:**
  - Enable **DHCP Snooping**.
  - Trust only legitimate DHCP servers.
- **For STP Manipulation:**
  - Enable **Root Guard**.
  - Enable **BPDU Guard**.

Chapter 6:

Wireless Network Security

Why Wireless is Insecure?

The Lack of a Physical Boundary, Eavesdropping is Passive and Undetectable,The Shared Medium, Historical and Protocol Weaknesses

- Channel: Broadcast ⇒ Eavesdropping, Jamming, Active attacks on protocols
- Mobility: Portable devices ⇒ Not physically secured Resources: Limited memory and processing resources ⇒ Need simpler security
- Accessibility: May be left unattended
-

Unlike wired networks, where physical access control is a primary layer of defense, wireless networks transmit data using radio frequencies. This broadcast nature makes them inherently accessible to anyone within range, including malicious actors. Therefore, securing wireless communications is not an optional add-on but a fundamental requirement for any telecommunication system. This chapter explores the principles, protocols, and practices designed to protect the confidentiality, integrity, and availability of data transmitted over wireless networks.

6.1. Fundamental Concepts of Wireless Security

6.1.1 The Broadcast Nature of Wireless Communications: Every transmission from an access point or a client device can potentially be intercepted by any other device listening on the same frequency. This fundamental characteristic is the root cause of most wireless security challenges.

Types of Wireless Communication

6.1.2 Key Security Objectives: Confidentiality, Integrity, Availability (CIA)

- ✓ **Confidentiality:** Ensuring that data is only readable by the intended recipient. This is achieved through strong encryption.
- ✓ **Integrity:** Guaranteeing that data has not been altered in transit.
- ✓ **Availability:** Ensuring that the wireless network and its services are accessible to authorized users when needed.

6.1.3. Authentication, Authorization, and Accounting (AAA)

- ✓ **Authentication:** Verifying the identity of a user or device before granting network access (e.g., using a pre-shared key or a username/password).
- ✓ **Authorization:** Determining what resources and services an authenticated user/device is permitted to access.
- ✓ **Accounting:** Tracking the consumption of network resources by users (e.g., for billing or auditing purposes).

6.2. Security Protocols

- Wired Equivalent Privacy (WEP): An older standard that provided minimal security. It is largely outdated due to known vulnerabilities.
- Wi-Fi Protected Access (WPA): An improvement over WEP, offering better data encryption through the Temporal Key Integrity Protocol (TKIP).

- Wi-Fi Protected Access II (WPA2): Utilizes the Advanced Encryption Standard (AES) for stronger security and is widely recommended for current networks.
- Wi-Fi Protected Access III (WPA3): The latest standard offering improved security features like Enhanced Open and 192-bit security suite.

6.3. Cellular Network Security

6. 3. 1. Security Architecture in 4G/LTE : 4G/LTE introduced a major security overhaul from 3G. Key features include:

Mutual Authentication: Both the user device (UE) and the network authenticate each other using the **AKA (Authentication and Key Agreement)** protocol.

Strong Encryption and Integrity Protection: Uses algorithms based on AES and SNOW 3G for the air interface between the device and the base station (eNodeB).

Network Domain Security (NDS): Secures the core network interfaces (e.g., between MME, HSS, S-GW).

6. 3. 2. Enhanced Security in 5G Networks : 5G builds upon 4G security and adds new capabilities:

Enhanced Subscriber Privacy: Protects the long-term identity (IMSI) of the user from eavesdropping.

Service-Based Architecture (SBA) Security: Uses HTTP/2 with TLS to secure communication within the 5G core.

Slicing Security: Provides isolation and security between different network slices.

6.4. Common Attack Vectors and Threats

- **Eavesdropping:** Simply listening to wireless transmissions to capture data.
- **Rogue Access Point / Evil Twin:** An unauthorized access point set up to mimic a legitimate one, tricking users into connecting.

- **Denial-of-Service (DoS):** Flooding a wireless channel or an access point with traffic to make it unavailable to legitimate users.
- **Man-in-the-Middle (MitM):** Intercepting and potentially altering the communication between two parties without their knowledge.

6.5. Best Practices for Securing Wireless Networks

- ✓ Use the latest security protocol (preferably **WPA3**, or WPA2 with AES).
- ✓ Use strong, complex Pre-Shared Keys (for personal use) or implement an 802.1X/EAP framework for enterprise environments (WPA2/3-Enterprise).
- ✓ Disable legacy protocols (WEP, WPA(TKIP)).
- ✓ Segment the network using VLANs (e.g., a separate VLAN for guest users).
- ✓ Regularly update firmware on access points and client devices.
- ✓ Perform regular wireless security assessments and penetration tests.