**Cyber security Internship Report**

**Prepared By**

**Haifa Sidani**

**Supervised By**

**Ibrahim Fleifel**

# Acknowledgments

I would like to express my sincere gratitude to XpertBot Academy for giving me the opportunity to undertake my internship in cybersecurity field. This experience has greatly enriched my practical knowledge and professional skills.

I am especially thankful to my supervisor Mr. Ibrahim Fleifel for the continuous guidance, support and encouragement throughout the internship. The feedback and mentoring helped me understand real world applications of the concept I learned academically.

Table of Contents

[Acknowledgments 2](#_Toc210061680)

[General Introduction 4](#_Toc210061681)

[CIA Triad 5](#_Toc210061682)

[Symmetric Encryption 5](#_Toc210061682)

[Asymmetric Encryption 6](#_Toc210061683)

[Digital Signatures 7](#_Toc210061683)

[Network Security Basics 8](#_Toc210061684)

[List of Figures 9](#_Toc210061685)

[Summary 9](#_Toc210061685)

# 

# General Introduction

Cybersecurity has become an essential aspect of modern technology, as organizations rely heavily on digital systems to store, process, and transmit information. Protecting these systems from threats, vulnerabilities, and unauthorized access is crucial to ensure data integrity, confidentiality, and availability.

During my internship at **XpertBot**, I had the opportunity to gain hands-on experience in various cybersecurity practices, including **encryption, digital signatures, network security, and the CIA triad**. This internship allowed me to apply theoretical knowledge in real-world scenarios, understand practical challenges, and develop skills necessary to safeguard digital information. This report documents the tasks I performed, the concepts I learned, and the insights I gained in the field of cybersecurity, highlighting how this experience contributed to my professional and personal growth.

# CIA Triad

The CIA Triad is a fundamental model in cybersecurity that guides how to protect data and systems. It stands for Confidentiality, Integrity, and Availability.

**Confidentiality**: Ensuring that sensitive information is only accessible to authorized people.

**Example:**

In BabiBeauty, only authorized users can access their secret product formulas, no one else can see them or have access.

**Integrity:** Ensuring that information is accurate, complete, and not tampered with.

**Example:**

In BabiBeauty, the product ingredients listed on the packaging should match the ingredients in the bottle.

**Availability:** Ensuring that data and systems are accessible when needed.

**Example:**

BabiBeauty manufacturing systems must always be available so that brands can place orders, track production, and ensure products are delivered on time.

**Symmetric Encryption:**

Symmetric encryption is a way to keep data secret by using one same key for both encryption and decryption, only people with the key can read the message.

The public key used in BabiBeauty should be sent encrypted using symmetric encryption for extra security.

**Common symmetric Encryption Algorithms:**

**AES:** Advanced Encryption Standard is very secure and widely used.

**DES:** Data Encryption Standard is older and less secure.

**3DES:** Triple DES is stronger than DES but slower.

**Blowfish:** Fast and good for smaller devices.

**Python script:**

from cryptography.fernet import Fernet

key = Fernet.generate\_key()

cipher = Fernet(key)

message = "BabiBeauty message encryption".encode()

encrypted\_message = cipher.encrypt(message)

print("Encrypted:", encrypted\_message)

decrypted\_message = cipher.decrypt(encrypted\_message)

print("Decrypted:", decrypted\_message.decode())

# Asymmetric Encryption

Asymmetric encryption is a method of protecting data using two different keys:

1. A public key shared with everyone to encrypt information.
2. A private key is kept secret to decrypt information.

Only the person who have the private key can read the message.

The BabiBeauty server create two keys:

Public key shared with the browser, and private key only on the BabiBeauty server. When the user login on the website, the browser encrypts the login credentials (email, password) using the public key, the encrypted data is sent to the server. On the server side, the server uses the private key to decrypt the message and read the credentials securely.

**Common Asymmetric encryption algorithm:**

**RSA:** Rivest Shamir Adleman is widely used for secure communication and digital signatures.

**ECC:** Elliptic Curve Cryptography is smaller keys, faster than RSA and is used in modern systems.

**DSA:** Digital Signature Algorithm mainly used for digital signatures.

**Python script:**

from Cryptodome.PublicKey import RSA

from Cryptodome.Cipher import PKCS1\_OAEP

key\_pair = RSA.generate(2048)

private\_key = key\_pair.export\_key()

public\_key = key\_pair.publickey().export\_key()

message = b"BabiBeauty confidential data"

cipher\_encrypt = PKCS1\_OAEP.new(RSA.import\_key(public\_key))

encrypted\_message = cipher\_encrypt.encrypt(message)

print("Encrypted Message:", encrypted\_message[:60], "...")

cipher\_decrypt = PKCS1\_OAEP.new(RSA.import\_key(private\_key))

decrypted\_message = cipher\_decrypt.decrypt(encrypted\_message)

print("Decrypted Message:", decrypted\_message.decode())

**Digital Signatures:**

A digital signature is like a secure fingerprint attached to a digital message or file, it ensures integrity and authenticity of digital data and proves that the message or file is real and hasn’t been changed. The digital signature works when the sender creates a hash of the message, then it signs the hash with its private key and sends both the message and the signature, then the receiver uses the sender’s public key to verify the signature.

Suppose BabiBeauty sends discount codes to loyal customers, but it wants to make sure that hackers don’t send fake discount codes pretending to be BabiBeauty, and customers can verify the code really came from BabiBeauty. They create a digital signature using their private key and send the discount code and when the customers receive the code they uses the BabiBeauty public key to check the signature. If the signature is valid this means that the code is real, and if it’s invalid this means that the code was changed by hacker or is fake.

**Python script:**

from cryptography.hazmat.primitives.asymmetric import rsa, padding

from cryptography.hazmat.primitives import hashes

private\_key=rsa.generate\_private\_key(public\_exponent=65537,key\_size=2048)

public\_key=private\_key.public\_key()

message=b"This is a secure message."

signature=private\_key.sign(message,padding.PSS(mgf=padding.MGF1(hashes.SHA256()),salt\_length=padding.PSS.MAX\_LENGTH),hashes.SHA256())

print("Signature is created successfully!\n")

try:

public\_key.verify(signature,message,padding.PSS(mgf=padding.MGF1(hashes.SHA256()),salt\_length=padding.PSS.MAX\_LENGTH),hashes.SHA256())

print("Signature is valid.")

except Exception:

print("Signature is invalid or message was tampered with.")

# Network Security Basics

Network security is about protecting data as it travels across networks and ensuring safe communication between devices. Below are some core concepts:

**Firewalls:**

A Firewall is a network filter that allows and blocks traffic based on rules such as IP, port, protocol, and application. It is used to prevent unauthorized access, limits attack surface, and enforces network policy.

**Types:**

Hardware Firewalls: Built into routers or network appliances.

Software Firewalls: installed on computer/servers.

**Virtual Private Network (VPN):**

A VPN creates an encrypted tunnel between endpoints over public networks. It is used to protect the confidentiality and integrity of traffic, allows secure remote access to internal resources. It is used as a remote employee access, site-to-site tunnels between branch offices, and protecting traffic on untrusted Wi-Fi.

**HTTPS (Hypertext Transfer Protocol Secure)**

HTTPS is the secure version of a website. You know it’s secure when you see a lock in the browser, it protects your data from being read or changed.

It uses TLS/SSL encryption to ensure:

Confidentiality: Attackers can’t read your traffic.

Integrity: Attackers can’t alter the content.

Authentication: Verifies you’re really connected to the website.

**Port Scanning:**

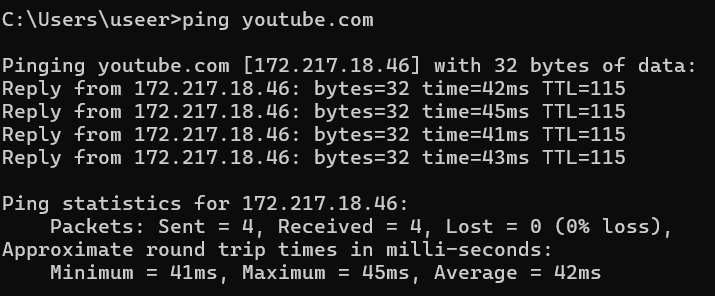
Port scanning is probing a host to see which ports or services are listening, it’s useful for inventorying services, finding misconfigurations, and attack surface analysis for defenders. Port scanning scan only systems you have an explicit permission to test, unauthorized scanning may be illegal and can trigger alarms.

Example tool: Nmap.

nmap scanme.nmap.org (it finds open ports on the test server)

nmap -p 1-1000 192.168.1.1(scan ports 1-1000 on a device at IP 192.168.1.1)

**Ping Test:** ping youtube.com sends test packets to see if a host is reachable, if it replies, the connection works.



*Figure 1: Ping Youtube*



*Figure 2: Tips for Staying Safe Online*

# Summary

During this internship, I learned about several core security concepts and how they are connected. Each concept plays a role in protecting data, systems and users.

Confidentiality, integrity and availability keep the data secret and not changed without permission and making sure the system is always accessible.

We have two types of encryption; symmetric that use one shared key for encryption and decryption, and asymmetric that use two keys (private/public) key to secure information’s.

Digital signature is an electronic proof that a message is authentic and hasn’t been changed, like a secure digital fingerprint.

Network security basics are the essential tools and practices used to protect computers, networks and data. Some tools are: firewalls, VPNs, HTTPS, Port scanning.

All these concepts work together to protect BabiBeauty or any system from cyber threats. They ensure that data is secure and available for users at all time.