Cybersecurity Internship

Prepared by:

Mariam Srour

For: Abidjan.ai

September 30, 2025

Introduction: This internship report summarizes my learning journey in cybersecurity. The purpose of the project was to explore essential security principles and practices, including
the CIA Triad, encryption methods, digital signatures, and network security fundamentals. By completing these tasks, I was able to strengthen my theoretical understanding and gain hands-on
experience with practical tools and coding demonstrations. This report not only reflects technical
outcomes but also shows how these concepts are interconnected and applied in real-world cybersecurity.

Task 1: CIA Triad Documentation

Confidentiality, Integrity, and Availability (CIA Triad):

- **Confidentiality** → Ensures that sensitive information is accessible only to authorized individuals

Example: Using a password to log in to your email.

- **Integrity** → Ensures that information is accurate and not modified by unauthorized users.

Example: A bank ensuring that when you transfer $100, the system does not change it to $1,000.

- **Availability** → Ensures that systems and data are accessible when needed.

Example: A hospital's patient records system must always be online so doctors can access it during emergencies.

Task 2: Symmetric Encryption (Theory + Demo)

Theory: - Symmetric encryption uses the same secret key for encryption and decryption. - Common algorithms: AES, DES, 3DES, Blowfish, ChaCha20.

Python Demo (AES):

```
from cryptography.fernet import Fernet

key = Fernet.generate_key()
cipher = Fernet(key)

msg = b"Hello Cyber Security!"
enc = cipher.encrypt(msg)
dec = cipher.decrypt(enc)

print("Encrypted:", enc)
print("Decrypted:", dec.decode())
```

Task 3: Asymmetric Encryption (Theory + Demo)

Theory: - Asymmetric encryption uses two keys: - Public key (encrypts) - Private key (decrypts) - Common algorithms: RSA, ECC, ElGamal.

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

```
private = rsa.generate_private_key(public_exponent=65537,
key_size=2048)
public = private.public_key()


msg = b"Hello Asymmetric!"
enc = public.encrypt(msg,
padding.OAEP(mgf=padding.MGF1(hashes.SHA256()),
algorithm=hashes.SHA256(), label=None))
dec = private.decrypt(enc,
padding.OAEP(mgf=padding.MGF1(hashes.SHA256()),
algorithm=hashes.SHA256(), label=None))


print("Decrypted:", dec.decode())
```

Task 4: Digital Signatures

Digital signatures ensure integrity and authentication.

They use private keys to sign and public keys to verify. Example (Python):

```
from cryptography.hazmat.primitives import hashes
from cryptography.hazmat.primitives.asymmetric import padding

msg = b"Verify this message!"
sig = private.sign(msg,
padding.PSS(mgf=padding.MGF1(hashes.SHA256()),
salt_length=padding.PSS.MAX_LENGTH), hashes.SHA256())
public.verify(sig, msg,
padding.PSS(mgf=padding.MGF1(hashes.SHA256()),
salt_length=padding.PSS.MAX_LENGTH), hashes.SHA256())
print("Signature verified")
```

Task 5: Network Security Basics

Basic Concepts:

1. Firewalls → Block/allow traffic based on rules (e.g., Windows Firewall).
2. VPNs→ Encrypt internet traffic and hide IP.
3. HTTPS → Secure communication between browsers and servers using TLS.
4. Port Scanning → Checking open ports (tool: Nmap).

Demo Commands:

-ping google.com (connectivity check)

-nmap -sV scanme.nmap.org (scan open ports)

Task 6: Final Summary

In this internship project, I learned about the CIA Triad, encryption (symmetric & asymmetric), digital signatures, and network security basics. These concepts are interconnected: CIA provides the foundation of security principles, encryption ensures confidentiality, digital signatures guarantee integrity, and network security protects systems from attacks.

Task 7 (Bonus): Cyber Hygiene Poster

5 Tips for Staying Safe Online:

1. Use strong, unique passwords.
2. Enable two-factor authentication.
3. Avoid clicking suspicious links or attachments.
4. Keep software and antivirus updated.
5. Use a VPN on public Wi-Fi.

Personal Reflection:

This internship was an enriching experience that enhanced both my technical and professional skills. I learned how the CIA Triad serves as the foundation of security, how encryption ensures confidentiality, and how digital signatures provide trust and authenticity. Working with practical demos in Python and exploring tools like Nmap gave me confidence in applying theory to practice. Beyond technical knowledge, I also developed discipline, problem-solving skills, and a deeper appreciation for cybersecurity's role in protecting organizations. I am motivated to continue learning and to contribute meaningfully to the field in my future career.