COMSATS UNIVERSITY ISLAMABAD

Attock Campus

Department Of Computer Science

Course	Information Security
Instructor	Ms. Ambreen Gul
Terminal Exam	LAB

Submitted From:

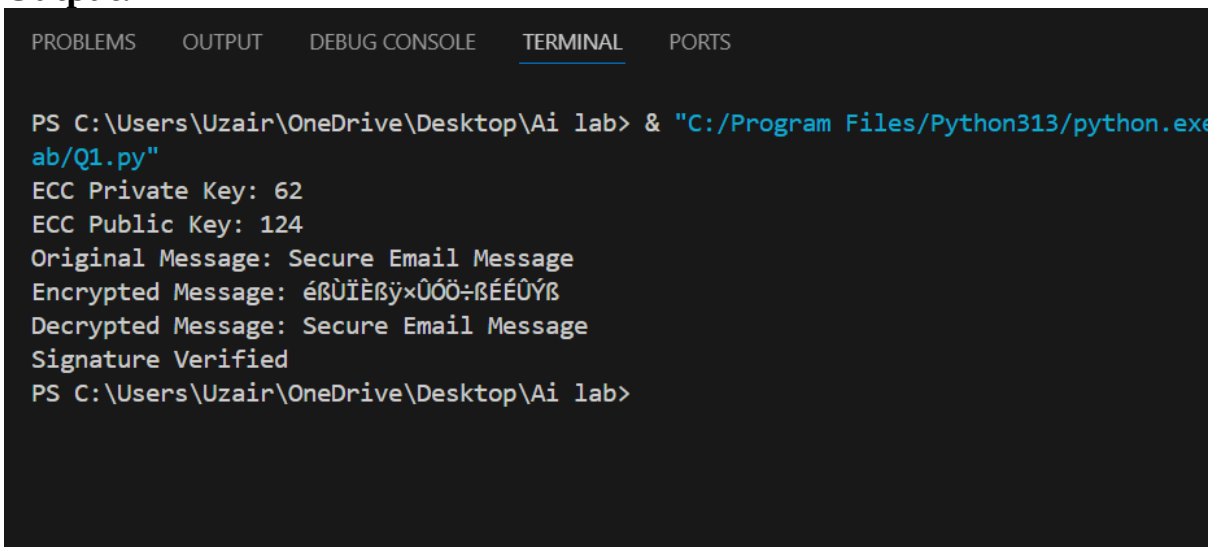
Registration No	**Name**
SP24-BSE-014	Uzair Khan

Q1. Scenario: You are designing a secure email communication system that ensures confidentiality, integrity, and authenticity of messages. The system uses Elliptic Curve Cryptography (ECC) for encryption and the Digital Signature Algorithm (DSA) for signing messages.
Tasks:
1. Key Generation:
2. Encryption/Decryption using ECC:
3. Digital Signature and Verification using DSA

Answer:

```
import hashlib
import random

private_key = random.randint(1, 100)
public_key = private_key * 2

print("ECC Private Key:", private_key)
print("ECC Public Key:", public_key)

message = "Secure Email Message"

shared_secret = private_key + public_key
encrypted = "".join(chr(ord(c) ^ shared_secret) for c in message)

decrypted = "".join(chr(ord(c) ^ shared_secret) for c in encrypted)

print("Original Message:", message)
print("Encrypted Message:", encrypted)
print("Decrypted Message:", decrypted)

dsa_private_key = random.randint(100, 200)
dsa_public_key = dsa_private_key * 3

signature = hashlib.sha256((message +
str(dsa_private_key)).encode()).hexdigest()

verify = hashlib.sha256((message + str(dsa_private_key)).encode()).hexdigest()

if signature == verify:
    print("Signature Verified ✔")
else:
    print("Signature Invalid ✖")
```

Output:



Code Explanation:

1. Key Generation

Public and private keys are generated for both ECC and DSA. The private key is kept secret, while the public key is shared with the receiver. These keys are used to perform secure encryption and digital signing.

2. Encryption/Decryption using ECC

ECC is used to create a shared secret key between sender and receiver.
The message is encrypted using this shared key to ensure confidentiality.
The receiver uses the same key to decrypt the message and obtain the original data.

3. Digital Signature and Verification using DSA

DSA is used to generate a digital signature for the message using the sender's private key. This signature ensures message integrity and authenticity. The receiver verifies the signature using the sender's public key to confirm that the message was not altered.

Q2. You have developed a project during this course as your final submission. Using that same project:

1. Justify your security method: Why is it suitable or better than other possible methods for your type of project?

Answer:

In my project AES (Advanced Encryption Standard) is used to secure user passwords in a file-based login system. AES is suitable because it is a strong and fast symmetric encryption algorithm that efficiently protects sensitive data like passwords. Compared to plain-text storage or basic hashing, AES ensures confidentiality by encrypting passwords before saving them in the file. This makes the system more secure for small-scale and offline applications where a database is not required.

2.Identify one possible vulnerability or weakness in your current system. How could an attacker misuse it?

Answer:

One possible vulnerability in the system is AES key management. If the master key or passphrase is exposed, an attacker can decrypt all stored passwords from the users.txt file. This could allow unauthorized access to user accounts and compromise the entire system.

3.Suggest one realistic improvement to enhance the security of your project. Briefly explain how it would work.

Answer:

One realistic improvement is to use authenticated encryption such as AES-GCM instead of AES-CBC. AES-GCM provides both encryption and integrity, which means it can detect if the encrypted file has been modified. This would protect the system from tampering attacks and further enhance overall security.