Lab 1: Basic Cryptography - AES, RSA and Kyber

Hrishikesh Nikam - 002315477
Computer Hardware and System Security (EECE5699)
Instructor: Yunsi Fei TA: Venkatesh Arumugam

September 29, 2025

Question 1: Performance Comparison

First compare the performance of RSA, AES-128, and Kyber512 (on the same size of plaintext - 16 bytes). Choose the appropriate key size for RSA to achieve the same security level as AES- 128. How much slower is RSA/Kyber than AES? With this implementation cost, discuss what scenarios RSA, AES, and Kyber are mainly used for, respectively. Why would someone want to use Kyber rather than RSA?

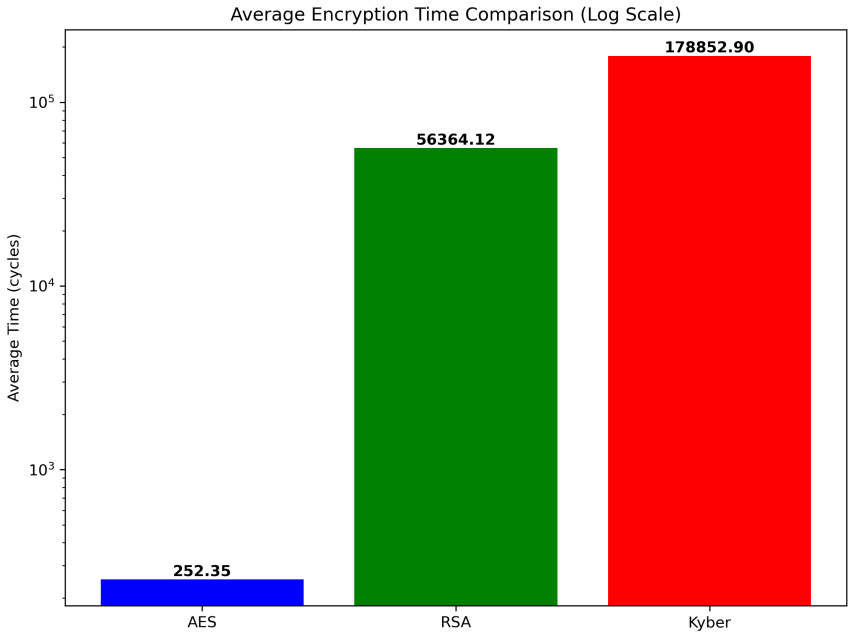

Figure 1: Performance comparison of AES, RSA, and Kyber (log scale).

We compared the performance of AES-128, RSA-2048, and Kyber512 on a fixed plaintext size of 16 bytes. Our implementation measured CPU cycles for one million AES iterations and one thousand iterations each for RSA and Kyber.

Results:

- AES mean cycles: **252.35**
- RSA mean cycles: **56364.12**
- Kyber mean cycles: **178852.90**

Discussion: AES-128 is the fastest since it is a symmetric cipher optimized for bulk data encryption. RSA, being asymmetric with large key sizes, is significantly slower. Kyber, a lattice-based post-quantum scheme, is the slowest but provides quantum resistance.

Appropriate RSA key size to match AES-128's security is **RSA-3072**, which is even slower than RSA-2048. From our results:

- RSA is roughly x slower than AES.
- Kyber is roughly 700x slower than AES.

Use cases:

- AES: Bulk data encryption, TLS/SSL, VPN, WiFi security.
- RSA: Key exchange, digital signatures, certificates, email encryption.
- Kyber: Post-quantum secure key encapsulation and future-proof systems.

Question 2: ECB vs CBC Encryption Modes

Compare these two encrypted images and comment on the security. What is the downside of CBC mode in terms of performance? Suggest one operation mode you think is the best and give your reason.

We encrypted the penguin image using AES-128 in both ECB and CBC modes.

- In ECB, identical plaintext blocks map to identical ciphertext blocks. The encrypted image still revealed the penguin structure.
- In CBC, each block depends on the previous one, removing visible patterns and providing stronger security.

Downside of CBC: CBC mode is slower because each block depends on the previous block. This introduces sequential dependencies and reduces performance.

Best Mode: CBC (or modern alternatives like CTR/GCM) is preferable due to stronger security, even at the cost of performance.

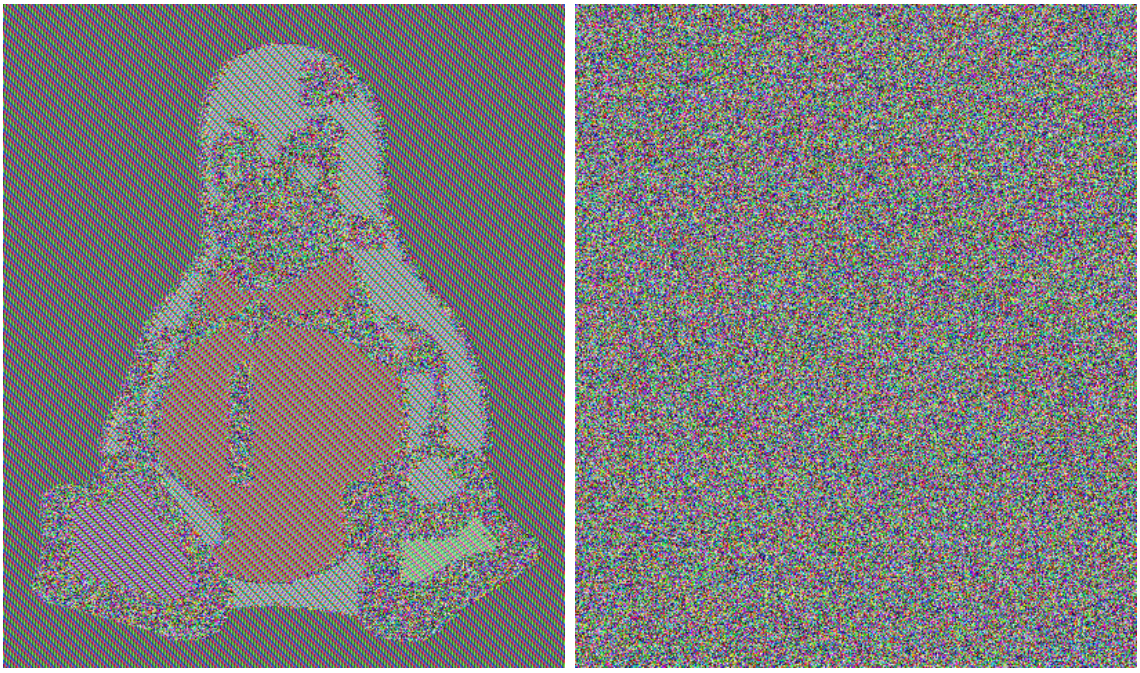

Figure 2: Comparison of ECB (left) vs CBC (right) encrypted images.

Module 3: Secure Communication with RSA

- The client generated an AES key and encrypted it with the server's RSA public key.
- The server decrypted the AES key with its private key, then encrypted the secret message with AES.
- The client decrypted the AES-encrypted secret message.

Output: The client successfully decrypted the server's secret:

```
Welcome to 5699!
```

The message was saved into `secret.txt`. This shows the RSA key exchange worked correctly.

Module 3: Quantum-Secure Communication with Kyber

- The client generated a Kyber keypair and sent its public key to the server.
- The server encapsulated a shared secret into a ciphertext and sent it back.
- The client decapsulated the ciphertext to derive the shared secret.
- AES was used with the derived key to decrypt the final secret message.

Output: The client decrypted the message as:

```
KyberPostQuantum
```

The message was saved into `secret_kyber.txt`. This confirms Kyber + AES communication works securely.

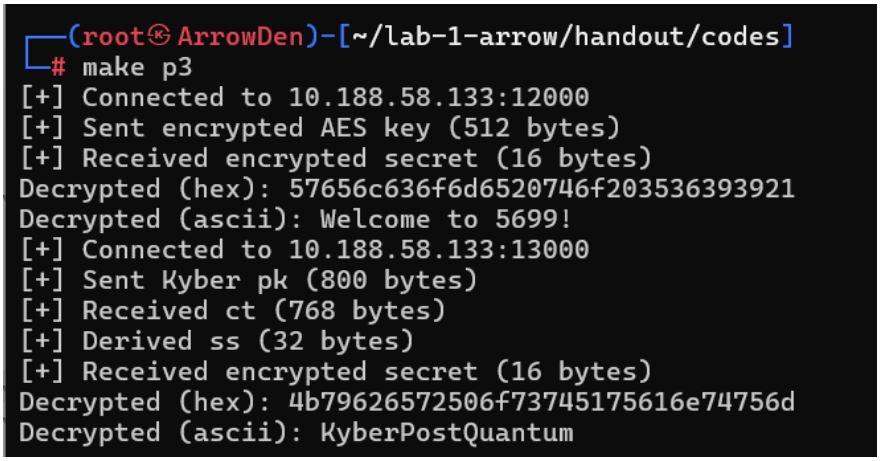

Figure 3: Secret Message

Conclusion

This lab demonstrated:

- AES is the fastest and best for bulk data.
- RSA provides asymmetric security but is slower.
- Kyber is quantum-resistant, slower than RSA, but future-proof.
- CBC masks patterns better than ECB at a small performance cost.
- Secure client-server communication was achieved using both RSA and Kyber.