MODULE 1

Performance Comparison

AES-128: Fastest because it's optimized for symmetric key encryption.

- RSA: Slower than AES because of its asymmetric nature and larger key size (3072 bits to match AES-128 security).
- Kyber512: Its slower than both AES and RSA. Kyber is designed to be quantum resistant, which adds lots of computational.

Discussion of Cipher Use Cases

- AES: Best for encrypting large amounts of data quickly, commonly used in applications like VPNs, file encryption, and HTTPS.
- RSA: Mainly used for key exchange, digital signatures, and other scenarios where asymmetric encryption is needed.
- Kyber: Post-quantum cryptography, designed to resist quantum attacks. It will be used in future encryption standards where quantum security is required.

Why choose Kyber over RSA?

Kyber is designed to withstand quantum computers, which could break RSA in the future due to its high computation ability. It will also be used for secure communications that will last for decades.

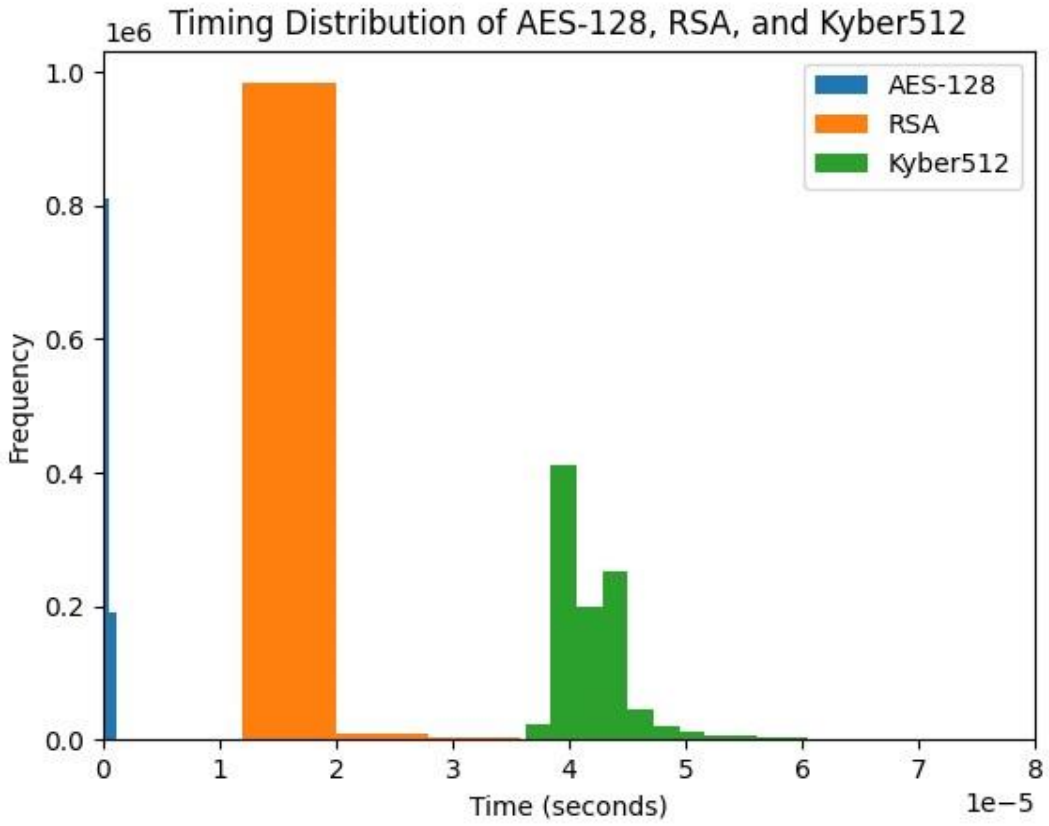
Timing Distribution of AES-128, RSA, and Kyber512
1e6
1.0
0.8
0.6
0.4
0.2
0.0
Frequency
AES-128
RSA
Kyber512
0
1
2
3
4
5
6
7
8
Time (seconds)
1e−5

Image 1.1

MODULE 2

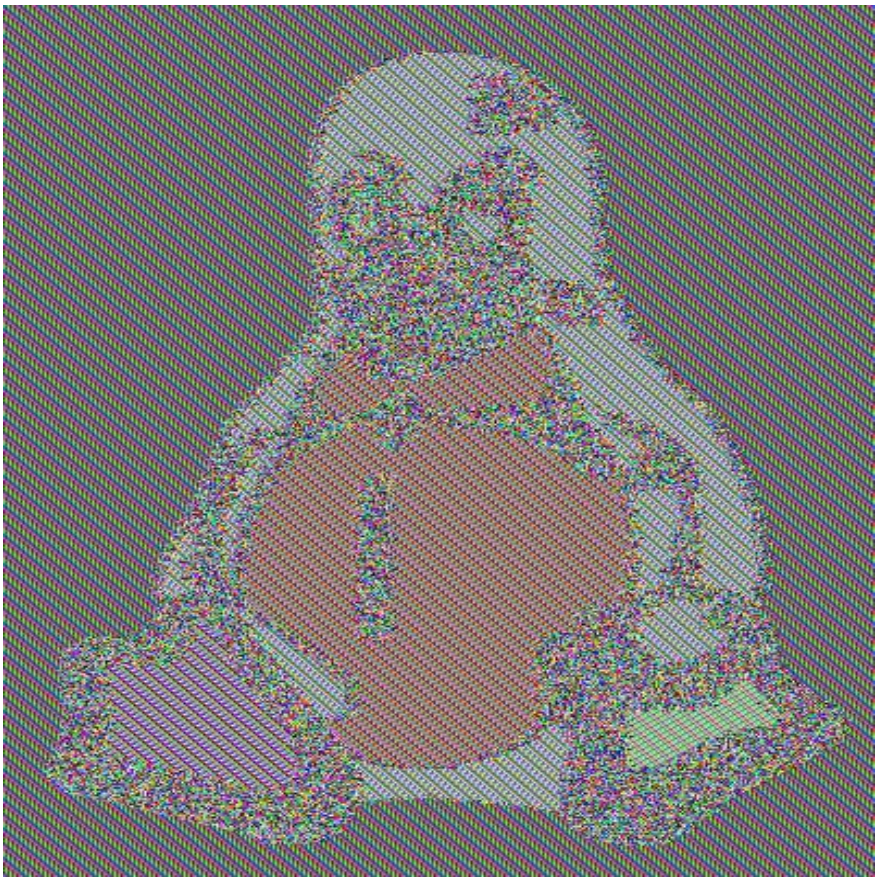

IMAGE 2.1 - ECB mode for Penguin

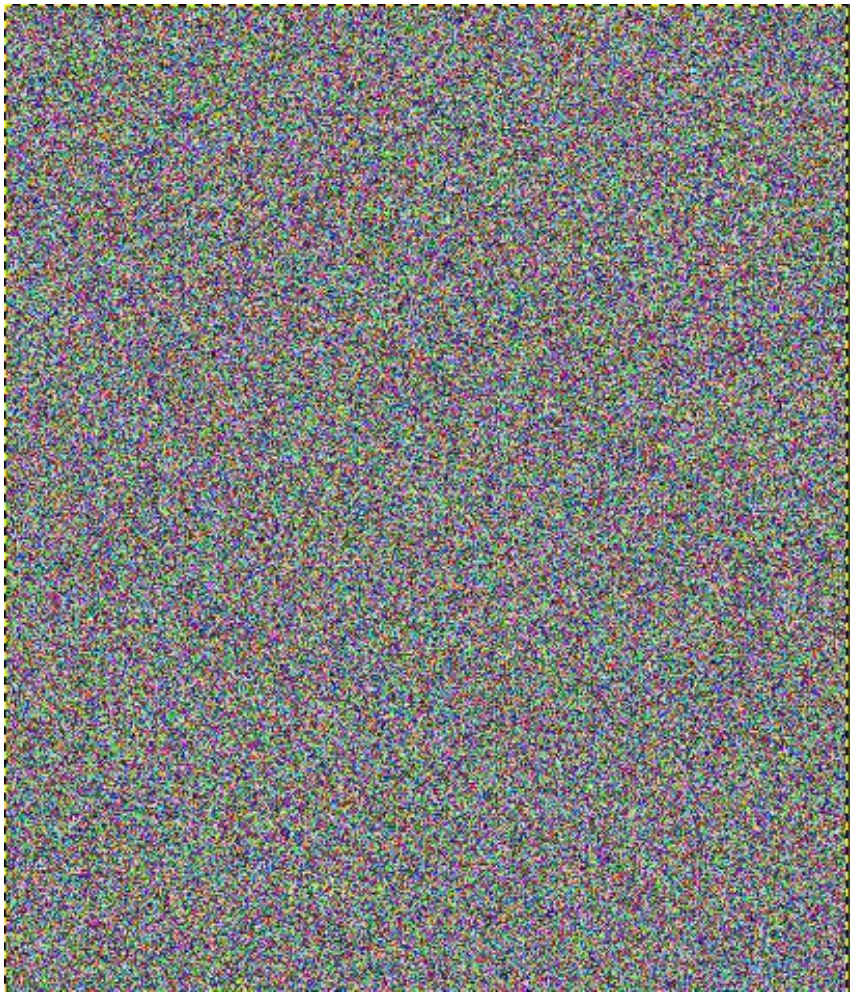

Image 2.2 - CBC mode for both Puppy and Penguin

Image 2.3 - ECB mode for Puppy

Visual Comparison

ECB Mode:
The encrypted image shows patterns from the original image, although it looks scrambled. We can look at the images 2.1 and 2,3 above.

CBC Mode:
The encrypted image appears much more randomized, with no discernible patterns from the original. We can look at image 2.2 above from the original penguin and puppy.

Security Preference:
From the images above we can conclude that ECB is not the best for encrypting images due to its vulnerability to pattern detection, hence CBC provides stronger encryption by chaining blocks together, making it harder for attackers to infer any patterns.

Performance Consideration:
ECB Mode is faster and allows parallel processing because blocks are encrypted independently while in CBC Mode each block depends on the encryption of the previous block, adding overhead.

MODULE 3

Secret message received:

NäU¬ç?y—£j„Ø ž¶