Name: Rhea D'Souza **UID:** dsouzrhea CYBR372_Assignment 1

Introduction

This report presents the findings of encryption and decryption performance measurements across different AES modes of operation, key sizes, and file sizes. The performance was evaluated based on the average time taken for encryption and decryption operations over 100 iterations, with results captured in seconds. The following sections describe the observed patterns and provide key takeaways from the data.

Encryption Performance Analysis

1. Impact of Cipher Mode:

- Across all file sizes and key sizes, the Cipher Block Chaining (CBC) and Galois/Counter Mode (GCM) on average show higher encryption times compared to the other modes like Cipher Feedback (CFB), Output Feedback (OFB), and Electronic Codebook (ECB).
- GCM mode on average consistently shows slightly lower performance than CBC, with encryption times close to or exceeding CBC times.

2. Impact of File Size:

- For smaller files (128 bits), the variation in encryption time is more visible across different key sizes and modes, with the longest duration observed in CBC mode for a 128-bit key (76.14 seconds) and the shortest in CFB mode for a 256-bit key (20.97 seconds).
- For larger files (512 bits), encryption times are more consistent across different key sizes and modes. The difference between the fastest (CFB with 25.07 seconds) and slowest (ECB with 27.79 seconds) modes is minimal.

3. Impact of Key Size:

- Increasing the key size generally decreases the encryption time for smaller files (128 bits). For instance, CBC mode sees a reduction from 76.14 seconds for a 128-bit key to 23.25 seconds for a 256-bit key.
- However, for larger files (512 bits), the key size has a less pronounced impact on encryption time, with only minor differences observed between different key sizes.

Decryption Performance Analysis

1. Impact of Cipher Mode:

- Decryption times are consistently lower than encryption times across all modes, key sizes, and file sizes.
- Similar to encryption, CBC and GCM modes tend to show higher decryption times than other modes.

2. Impact of File Size:

- For smaller files (128 bits), the variation in decryption times is significant, with GCM mode showing the highest decryption time (28.64 seconds) for a 128-bit key and OFB mode showing the lowest time (0.62 seconds) for a 256-bit key.
- For larger files (512 bits), decryption times are more uniform across different key sizes and modes, with the highest time observed in GCM mode (4.94 seconds) for a 192-bit key and the lowest in OFB mode (0.61 seconds) for a 256-bit key

3. Impact of Key Size:

- Similar to encryption, increasing the key size generally reduces decryption times for smaller files (128 bits), but the impact is less pronounced for larger files (512 bits).

Discussion

Performance Implications of Mode Selection:

GCM and CBC modes offer better security but at the cost of higher encryption and decryption times, particularly for smaller files. CFB and OFB modes provide faster processing, making them suitable for scenarios where performance is critical.

File Size Considerations:

As file size increases, the differences in performance between different key sizes and modes become less significant. This suggests that for larger files, the choice of mode and key size may be driven more by security requirements than by performance concerns.

Optimization Opportunities:

For applications requiring quick encryption/decryption of small files, using CFB or OFB modes with higher key sizes (256-bit) can significantly reduce processing time while maintaining a reasonable level of security.

Conclusion

This report highlights the trade-offs between encryption/decryption performance and the choice of AES modes and key sizes. While CBC and GCM modes provide robust security, they incur higher processing costs, especially for smaller files. Optimizing for performance without compromising security requires careful consideration of the specific use case, file size, and security requirements.