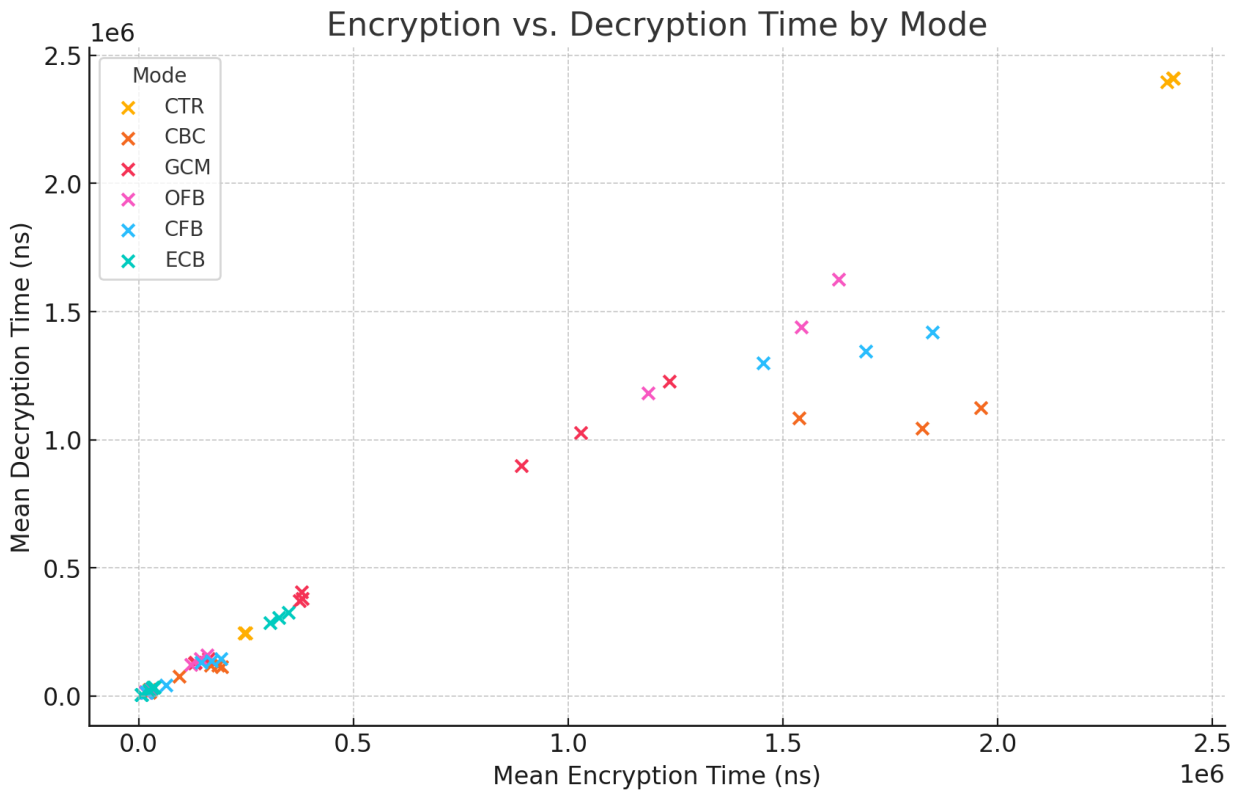
CYBR 372 Applications of Cryptography

- **Name:** Hamish Burke
- **Student ID:** 300601632
- View the raw data in `/src/part4/results.csv`

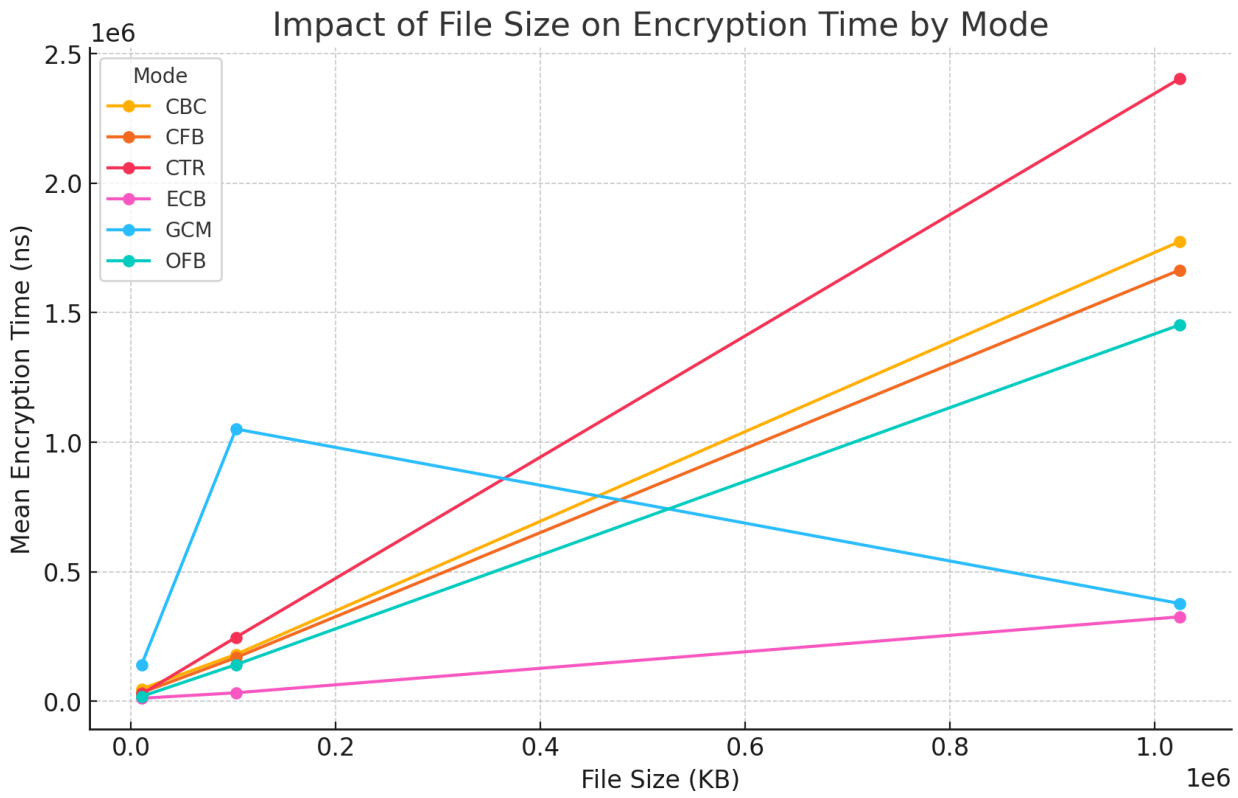
Part 3: Evaluation of Parameters on Performance

Key Findings



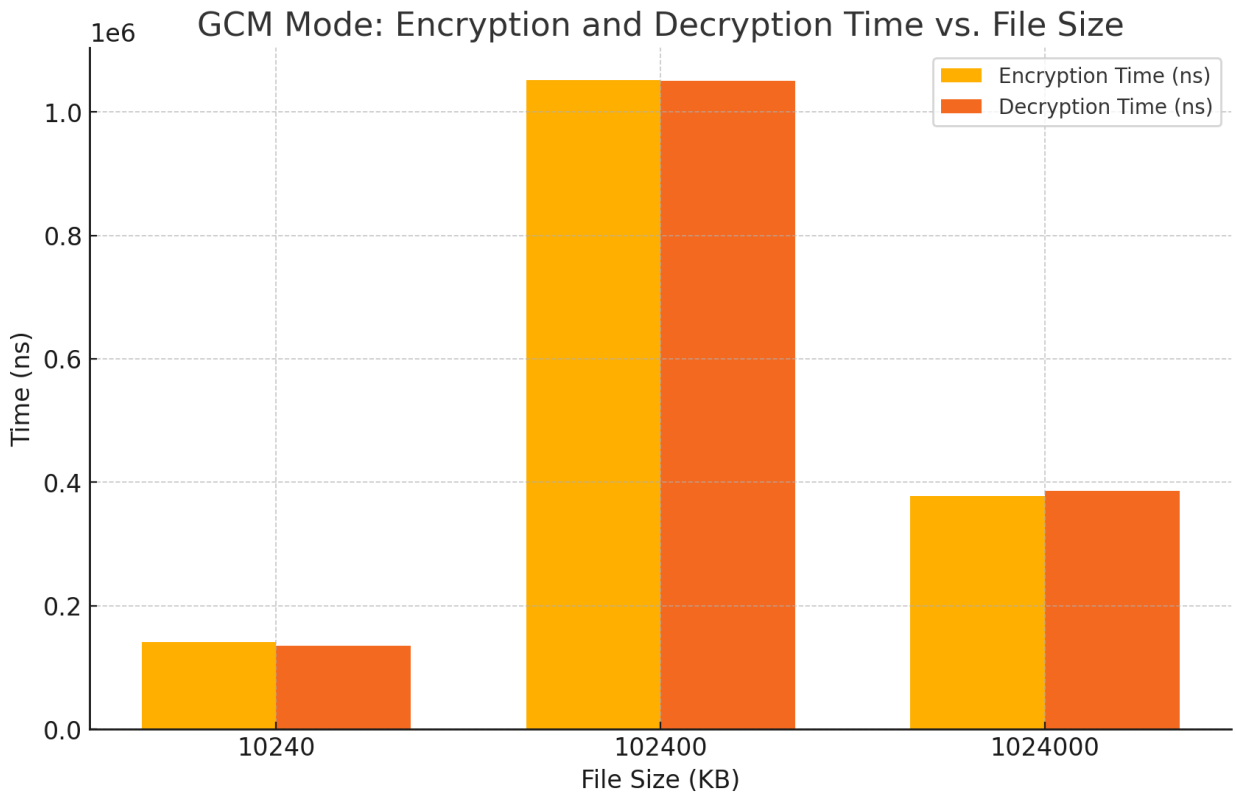
Encryption vs. Decryption Time (Scatter Plot):

- The scatter plot shows a strong correlation between encryption and decryption times across different modes. Modes like **CTR** exhibit higher encryption and decryption times, while **ECB** shows consistently lower times. This indicates that while some modes offer better performance, others like **CTR** may require more processing time due to their complexity.



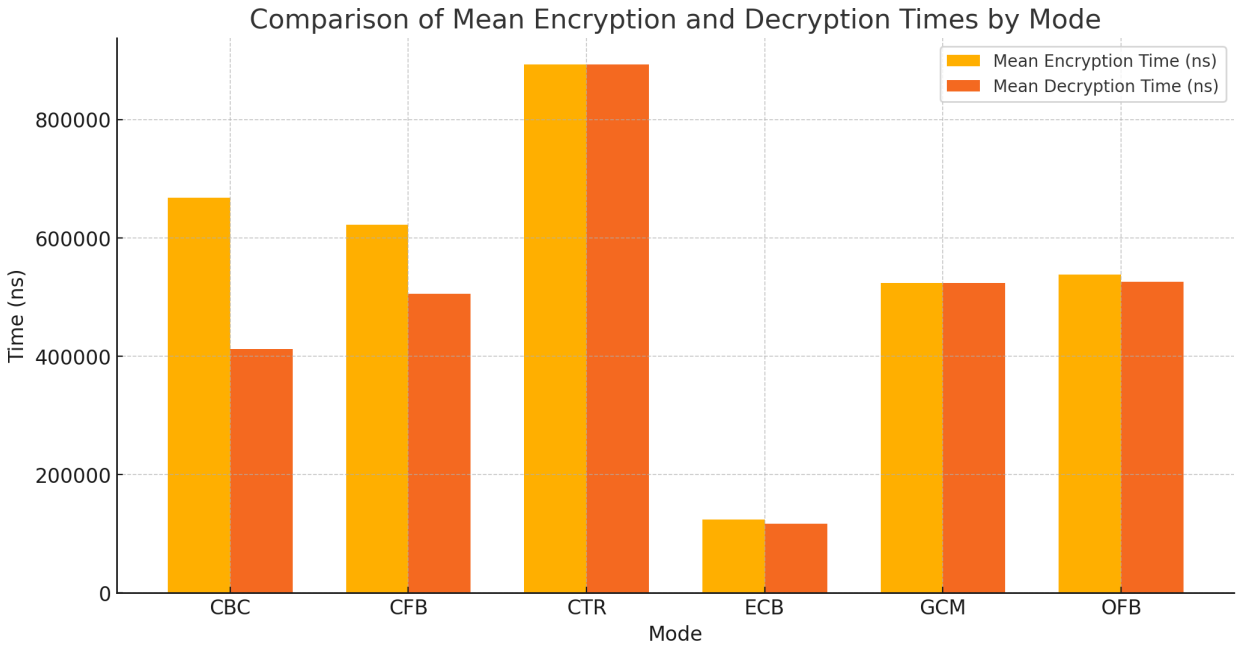
Impact of File Size on Encryption Time by Mode (Line Graph):

- The line graph above highlights how encryption times scale with file size for each mode. **CTR** and **CBC** modes show significant increases in time with larger files, while **ECB** remains relatively stable. **GCM** displays an unusual pattern (going up then down), which may indicate inconsistency in how it handles different file sizes.



GCM Mode: Encryption and Decryption Time vs. File Size (Bar Graph):

- The bar graph specifically for **GCM Mode** shows that both encryption and decryption times increase with file size, but interestingly, for the largest file size, the time decreases slightly. This suggests that **GCM Mode** may have optimisations or efficiencies that manifest at certain thresholds.



Comparison of Mean Encryption and Decryption Times by Mode (Bar Graph):

- This comparison bar graph clearly shows that **CTR** mode has the highest mean encryption and decryption times among all modes. **OFB** and **GCM** are more consistent, while **ECB** has the shortest times, reaffirming its efficiency but also its vulnerability.

Recommendations

For High Performance:

- **ECB Mode** is the most efficient and offers the fastest encryption and decryption times. However, due to its vulnerabilities, it should only be used when security is less of a concern, such as in controlled environments where the data pattern is not an issue.
- **OFB Mode** is recommended when a balance of speed and security is required, as it shows consistent performance across different file sizes.

For High Security:

- **GCM Mode** is the best option for scenarios requiring authenticated encryption, despite its higher processing times. Its relatively stable performance across different file sizes makes it reliable for secure applications.
- **CTR Mode** should be considered when encryption security is critical, but be aware of its higher time costs, especially with larger file sizes.

Balanced Approach:

- **CBC Mode** offers a good balance between security and performance but becomes less efficient as file sizes grow. It can be a good choice for medium-sized files where moderate security is needed.

Conclusion

The visualisations clearly show the trade-offs between encryption modes in terms of performance and security. **ECB Mode** offers the fastest times but at the cost of security, making it suitable only in specific, low-risk scenarios. **GCM Mode** delivers robust security with relatively stable performance, making it ideal for high-security needs. **OFB** and **CBC Modes** provide a middle ground, with **OFB** offering consistency and **CBC** balancing security and speed. **CTR Mode** should be used when security is a priority, but its higher processing times must be considered.