Task 5 Report

Student Number: 670182

This report presents the implementation and performance comparison of 5-bit CFB TEA and 3-bit CFB TEA algorithms. The student number 670182 was used as test data and timing analysis was conducted to evaluate the computational efficiency of different feedback bit sizes.

5-bit CFB TEA Algorithm Implementation

The 5-bit CFB TEA was implemented with the following features:

* Block cipher: TEA with 64-bit blocks and 128-bit keys
* Mode of operation: CFB with 5-bit feedback segments
* Shift register: 64-bit register updated with 5-bit ciphertext feedback
* Processing: Data processed in 5-bit chunks with TEA keystream generation

Technical implementation details

* TEA uses 32 cycles (64 rounds) with delta constant 0x9e3779b9
* Shift register initialized with 64-bit initialization vector
* Each iteration: encrypt shift register -> extract 5 leftmost bits -> XOR with plaintext -> feedback to register
* Bit-level processing with proper padding for incomplete chunks

**Performance Comparison Results**

5 Bit CFB TEA timing: 0.000366 seconds

3 Bit CFB TEA timing: 0.000528 seconds

5-bit CFB TEA is 1.44x faster than 3-bit CFB

Analysis and explanation

The timing comparison reveals that 3-bit CFB TEA is slower than 5-bit CFB TEA due to several factors:

1. Iteration Frequency

* 5-bit CFB: 10 iterations for 48-bit data
* 3-bit CFB: 16 iterations for 48-bit data
* 60% more iterations are required for 3-bit processing

1. TEA Encryption Overhead

* Each iteration requires a full TEA encryption of the 64-bit shift register
* More iterations mean more TEA encryptions which also mean higher computational cost
* TEA encryption is the most expensive operation in the algorithm

1. Register Management Overhead

* More frequent shift register updates
* More bit manipulation operations
* Higher per-bit processing overhead

1. Memory Access Patterns

* Smaller chunks require more memory access
* Less efficient cache utilization
* Higher instruction overhead per bit processed

Conclusions

* Both 5 Bit and 3 Bit CFB TEA algorithms were successfully implemented and verified through encryption and decryption testing.
* Smaller feedback sizes (5 bit and 3 bit) result in worse performance because they require more computational power
* Due to the reasons stated above, it is observed that 3-bit CFB TEA algorithm will take longer than 5-bit CFB TEA algorithm.