Task 7 Analysis Report

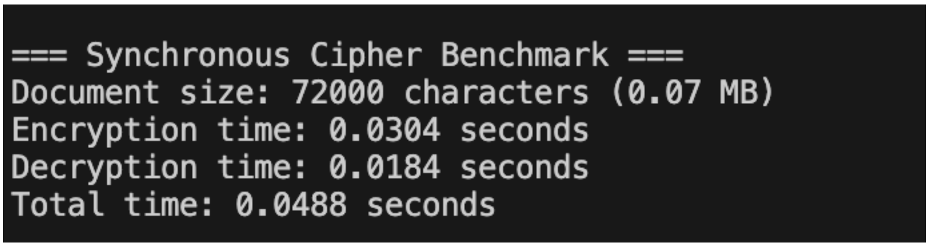
This report shows the implementation and analysis of a combination encryption system between 1-Bit CFB mode with synchronous stream cipher. The combination approach applies different encryption methods based on character position

- Odd position characters use 1-Bit CFB with TEA encryption
- Even position characters use synchronous cipher

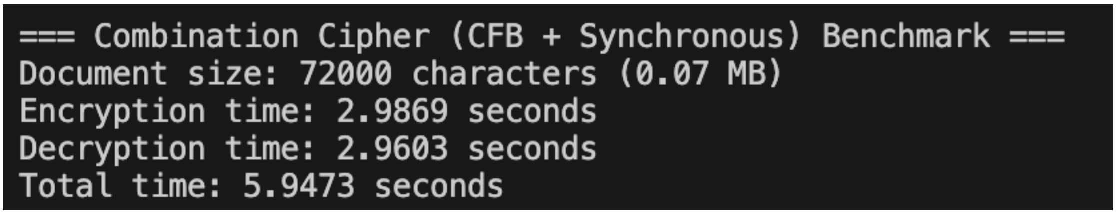
Implementation overview

1. Modified 1-Bit CFB Implementation
   The 1-Bit CFB mode was implemented using TEA as the underlying block cipher.
   - Block Size: 64 bits (8 bytes)
   - Key Size: 128 bits (16 bytes)
   - Operation: Processes 1 bit at a time
   - Shift Register: Updated with each ciphertext bit
   - Initialization vector: 8-byte IV for initial shift register state
2. Synchronous cipher implementation
   Based on algorithm from Task 6.
3. Combination cipher architecture
   - Even position: 1-Bit CFB with TEA
   - Odd position: Synchronous stream cipher
   - Character encoding: 5-bit representation for CFB mode
   - Synchronization: Independent keystreams for each cipher mode

Performance analysis



```
=== Synchronous Cipher Benchmark ===
Document size: 72000 characters (0.07 MB)
Encryption time: 0.0304 seconds
Decryption time: 0.0184 seconds
Total time: 0.0488 seconds
```



```
=== Combination Cipher (CFB + Synchronous) Benchmark ===
Document size: 72000 characters (0.07 MB)
Encryption time: 2.9869 seconds
Decryption time: 2.9603 seconds
Total time: 5.9473 seconds
```

Analysis and Justification

1. Computational Complexity Mismatch
   - Synchronous cipher: O(1) operations per character
   - CFB Mode: O(n) where n = 32 TEA rounds * 5 bits per character = 160 operations per character
   - Impact: 160x computational difference per CFB-encrypted character

2. Cryptographic Algorithm Overhead
   - TEA complexity: 32 rounds of Feistel network operations
   - Key scheduling: Multiple XOR, shift, and addition operations per round
   - State Management: Shift register updates for every bit processed

Conclusion

The combination cipher implementation demonstrates the significant performance trade off in combining different cryptographic approaches. The 73x performance degradation observed is primarily due to the computational intensity of 1-Bit CFB mode using TEA encryption which overwhelms the efficiency of synchronous cipher.