**Description for: CS 492 Homework 2**

Symmetric Cryptography

Complete the problems below and submit this word document with the solution to the questions here. Also submit the source code **you** created to solve problem 2

Name: Christopher Kareem Schmitt  
  
**Problem 1 Stream encryption (30 pts):**

You have a 4 bit LFSR with tap sequence [3,2,0] your initial key is 1011 encrypt the message “1001” and enter it below.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Bit 0 | Bit 1 | Bit 2 | Bit 3 | Key stream | Encrypted message |
| 1 | 0 | 1 | 1 |  |  |
| 1 | 1 | 0 | 1 | 1 | 0 |
| 0 | 1 | 1 | 0 | 1 | 1 |
| 1 | 0 | 1 | 1 | 0 | 0 |
| 1 | 1 | 0 | 1 | 1 | 0 |

**Problem 2 Block encryption (40 pts):**

**YOU** implement the Tiny Encryption Algorithm (TEA) in either Java or C++. There are many implementations out there, but make sure this implementation is **completely your own**. Your understanding of the details of how the bit operations matter is critical to your understanding of the intricacies of implementing computer security.

In addition to submitting this word document you need to submit your source code.

**Part 1:** Use your TEA algorithm to encrypt the 64-bit plaintext block:

0x01CA45670CABCDEF

Using 128 bit key:

0xAF6BABCDEF00F000FEAFFFAFABCDEF01

Enter your cipher text here:

0xCCC662540BCBF1A1

**Part 2:** Implement decryption and verify that you obtain the original plain text

**Part 3:** In comments in your code explain how you would make your code encode/decode a longer set of plaintext (i.e. multiple blocks) using CBC. You do not need to code this, but your explanation should be detailed related to your implementation.

**Problem 3 Chain block encryption (30 pts)**

Given the following message and a block size of 2 bits, encode it using ECB, CBC, and CTR (make sure to indicate which is which)

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Use the following substitution cipher | | | | Plain | 00 | 01 | 10 | 11 |
|  |  |  |  | Encoded | 11 | 10 | 00 | 01 |
| IV | 00 |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| Message | 01 | 00 | 11 |  |  |  |  |  |

ECB:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Ciphertext | 10 | 11 | 01 |  |  |  |  |  |

CBC:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Plaintext | 01 | 00 | 11 |  |  |  |  |  |
| XOR | 01 | 10 | 11 |  |  |  |  |  |
| Ciphertext | 10 | 00 | 01 |  |  |  |  |  |

CTR:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Plaintext | 01 | 00 | 11 |  |  |  |  |  |
| XOR | 01 | 01 | 01 |  |  |  |  |  |
| Ciphertext | 10 | 10 | 10 |  |  |  |  |  |