Experiment 2

Information Security: Encryption/Decryption

Part 1:

1. Caesar Cipher: The C code exp2.c has been compiled with gcc compiler with the command gcc exp2.c -o encrypt\_decrypt. The code has been run with the key input range -26 to 26. The plain text should have all English capital letters.

2. Advanced Encryption Standard (AES): The given codes have been compiled and observed the output according to the given instruction.

Caeser Cipher : The output:

A screen shot of a computer

Description automatically generated

AES: The screenshot for AES step 5 is given below.A screen shot of a computer code

Description automatically generated

AES: The screenshot for AES step 6 is given below

A black screen with white text

Description automatically generated

AES: The screenshot for AES step 9 is given below:

A screen shot of a computer

Description automatically generated

Summary:  
This hardware security lesson focuses on two encryption techniques: the Caesar Cipher and the Advanced Encryption Standard (AES). The Caesar Cipher is a simple substitution cipher where each letter in the plaintext is shifted a certain number of positions up or down the alphabet. The lesson includes a programming the Caesar Cipher in C, emphasizing case sensitivity and ignoring non-letter characters.

The second part of the lesson provides information on AES, a more sophisticated encryption method based on a substitution-permutation network. Unlike its predecessor DES, AES operates on a fixed block size of 128 bits and allows for key sizes of 128, 192, or 256 bits. The practical exercises involve compiling and running AES encryption code, modifying input messages, and analyzing the resultant ciphertext.