Lab 4 exercises

June 22, 2024

1. Implement the Caesar cipher using a TLV enconding on UART. Have separate commands for encryption and decryption. Shift by 3 characters.

2. Implement the Caesar cipher with shift as an input. Use the first byte from value(the V in TLV) for the shift value(value can be only positive).

3. Implement the Kamasutra cipher Implement the Caesar cipher using a TLV enconding on UART. Have separate commands for encryption and decryption.

4. Implement the encryption scheme for a simple XOR cipher with padding and block chaining. Key is a 8 byte input(can be any random value). Message can be any length between 1 and 32 bytes. Message needs to be padded if length is not multiple of 8.

   The XOR cipher algorithm is as follows:

   - If message is not multiple of 8 we will pad the message with 0s until it is a multiple of 8
   - We consider 8 bytes as the block of this cipher
   - We xor the first block(8 bytes) of the padded message with the key
   - If the padded message is longer than 1 block(8 bytes) for the subsequent n blocks the encryption will be the padded message xored with the key and xored with the ciphertext of the previous block

   The encryption algorithm above in our case is still XOR Key will be hardcoded in the program with: `uint8_t key[]={0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07, 0x08};` For an input of 10 bytes: `{F0}{F0}{00}{00}{00}{00}{00}{00}{08}{08}` We should receive: `{F1}{F2}{03}{04}{05}{06}{07}{08}{F8}{F8}{00}{00}{00}{00}{00}{00}`