Lab 4 exercises

June 25, 2024

1. Use source files from aes to implement a chipher with commands for encryption and decryption.

   The AES algorithm works on blocks of 16 bytes (input/output): Data must be sliced into 16 byte chunks.

2. Implement CBC mode of operation.

   CBC mode of operation use diffusion to break patterns in encrypted data. each encrypted data block is XORed with next plain data block before encryption. For first block an IV (initialization vector) is used. Encrypt the message below.

   ```
   See you at 13 o'clock in class, do not be late!!!
   ```

   Modify input data for decryption algorithm in such way the decrypted text still appears valid.

   !Hint if you change one byte from IV only corresponding byte from first block will be altered.

3. Implement CBC MAC

   CBC MAC is MAC algorithm based on block cipher CBC mode allways using IV set with 0.

4. Implement CTR mode of operation.

   CTR mode use a counter. the algoritm encrypt the counter and the XOR te output with plain text.

   Then the counter is incremented and the process is repeated until all data are encrypted.