CENG 471 HW1 REPORT

- These two block ciphers and stream ciphers are the methods used for converting the plain text into ciphertext. Block ciphers turn plain text into cipher text one block at a time, which is the primary distinction between them and stream ciphers. Stream cipher, on the other hand, converts plain text into cipher text by taking 1 byte at a time. When the security is more important than performance Block cipher should be used otherwise Stream cipher should be used. AES and DES are examples of Block cipher. RC4 and SALSA20 are examples of Stream cipher.
- In CBC mode, the IV used in the first block of encryption is not a secret value. Encryption of the IV value might be solution for this situation.
- Some researches say that it is not secure. But it depends on design of encryption. There are few other modes that can be used for encryption instead of CBC (CFB and OFB). These modes use IV in different ways for encryption.