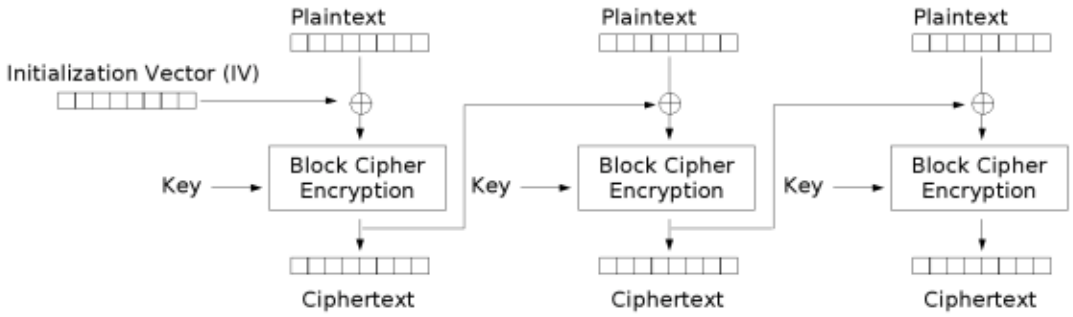
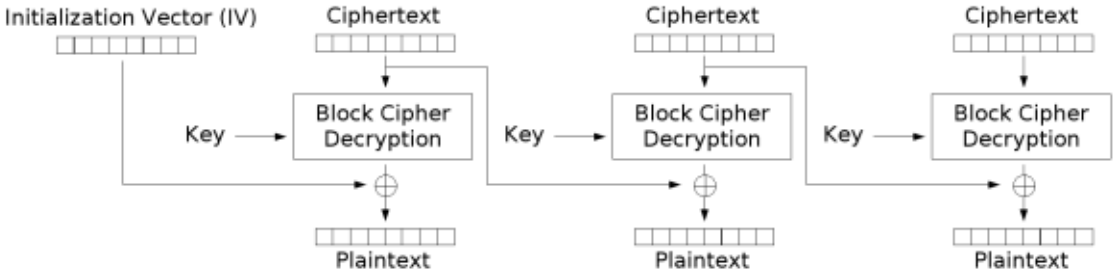
Cipher Block Chaining (CBC)

The S-DES algorithm is a block cypher (block size is one byte). The following describes the algorithm for Cipher Block Chaining (CBC). The information is taken from Wikipedia (http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation).

IBM invented the cipher-block chaining (CBC) mode of operation in 1976. In CBC mode, each block of plaintext is XOR'd with the previous ciphertext block before being encrypted. This way, each ciphertext block depends on all plaintext blocks processed up to that point. To make each message unique, an initialization vector must be used in the first block.



Cipher Block Chaining (CBC) mode encryption



Cipher Block Chaining (CBC) mode decryption