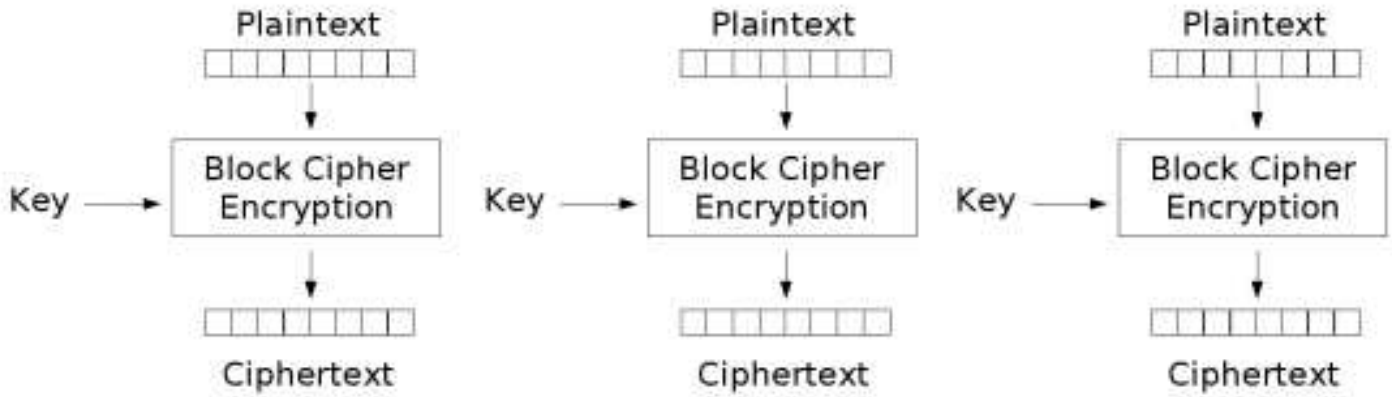
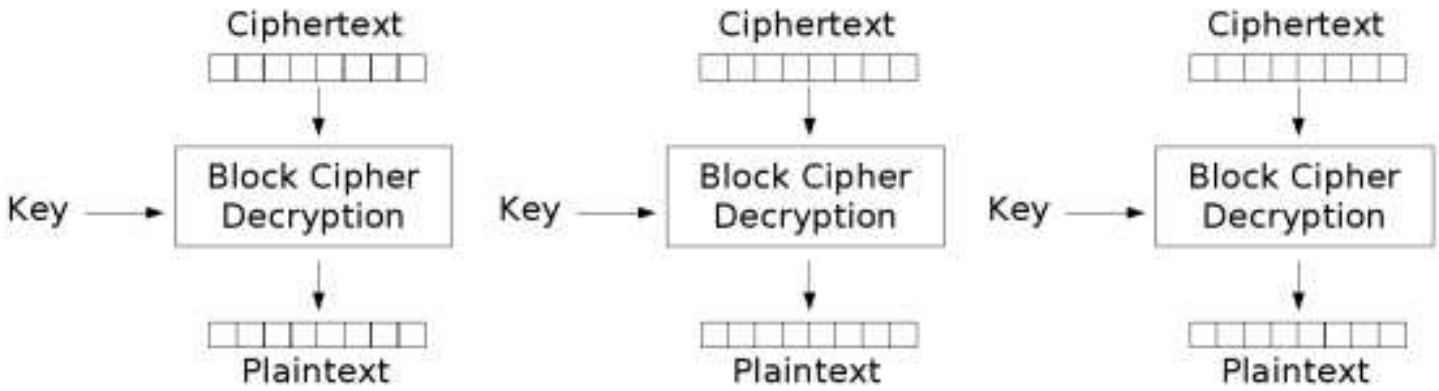
Cryptography, winter 2014/15

Modes of operation

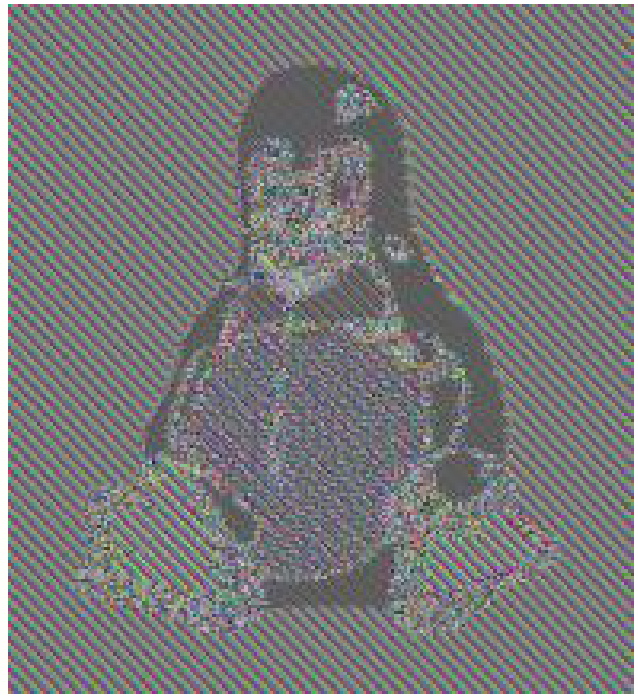
Dr. Daniel Loebenberger

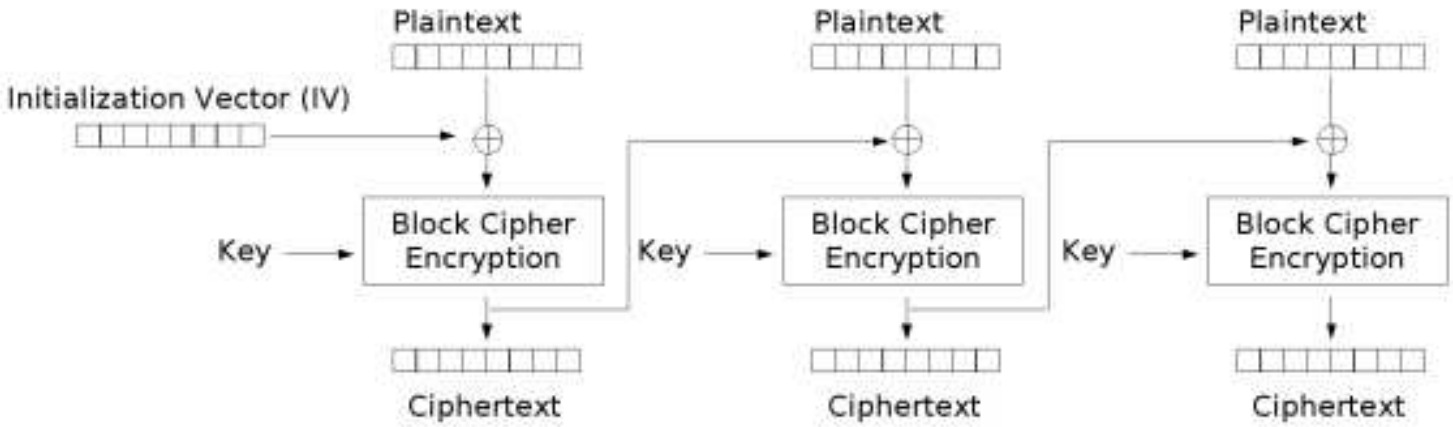


Electronic Codebook (ECB) mode encryption

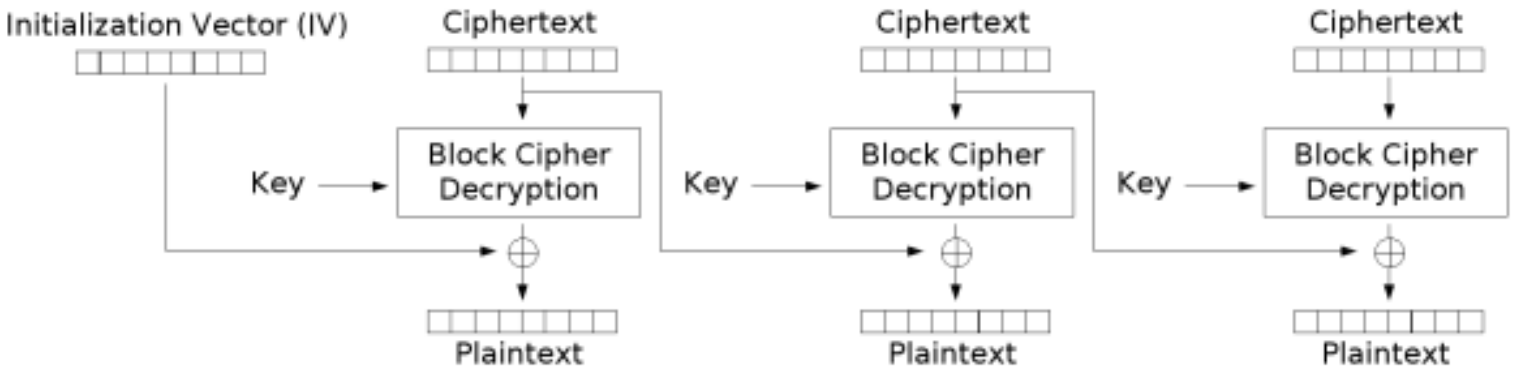


Electronic Codebook (ECB) mode decryption

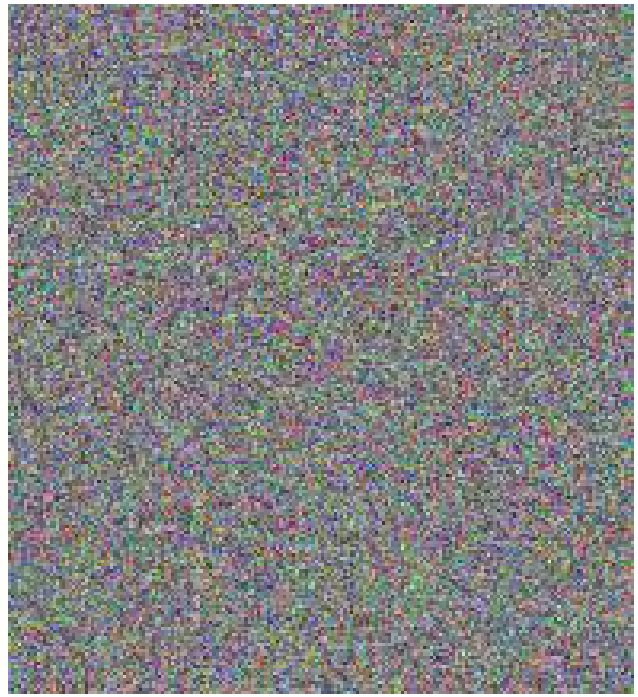


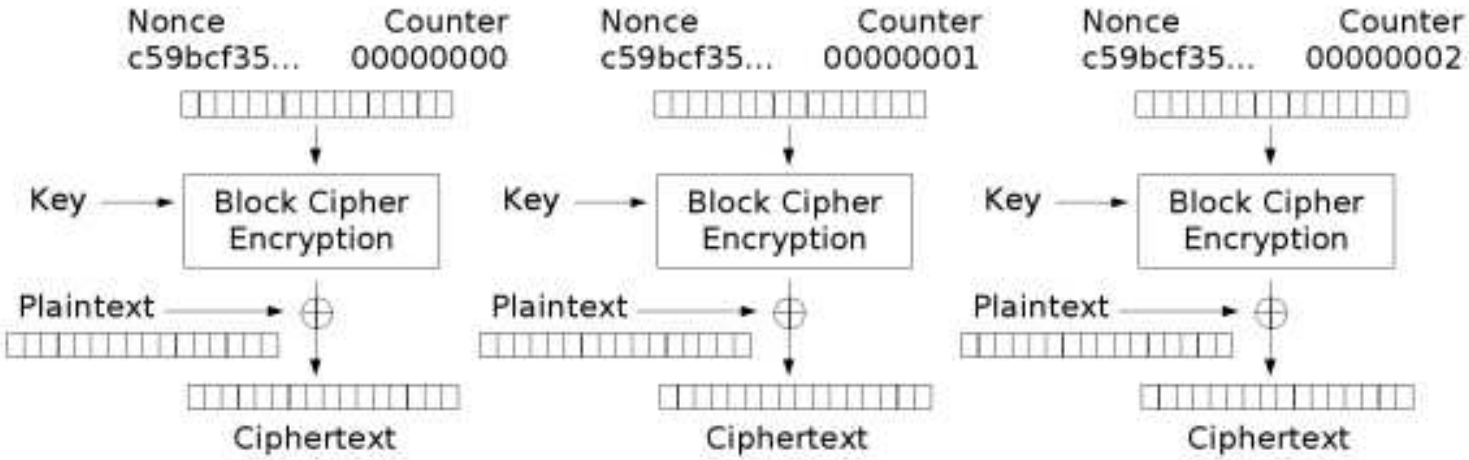


Cipher Block Chaining (CBC) mode encryption

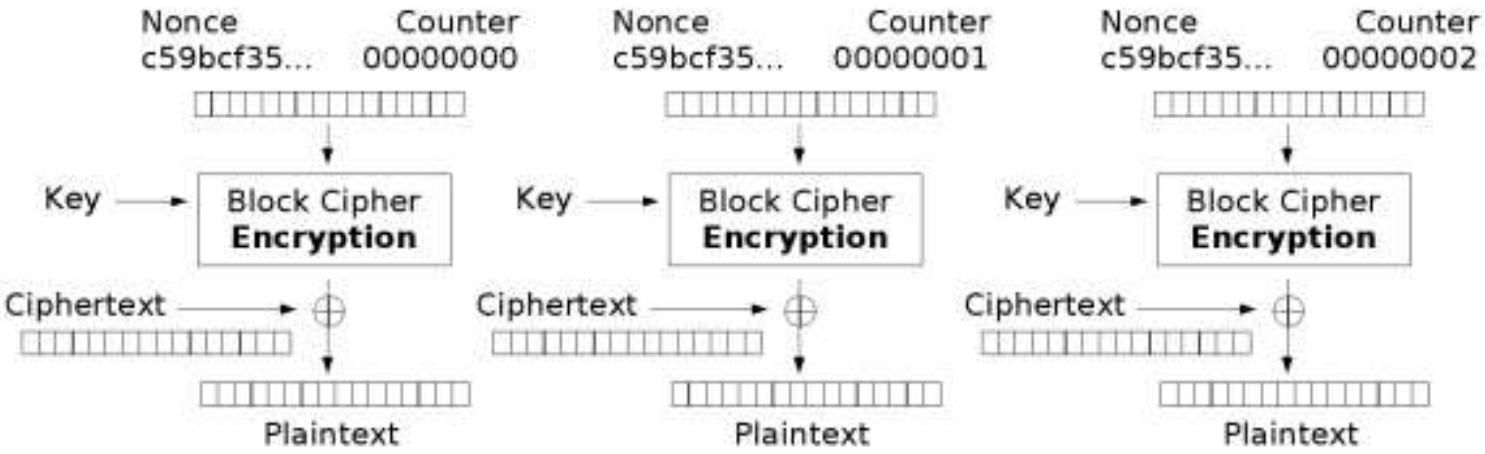


Cipher Block Chaining (CBC) mode decryption





Counter (CTR) mode encryption



Counter (CTR) mode decryption