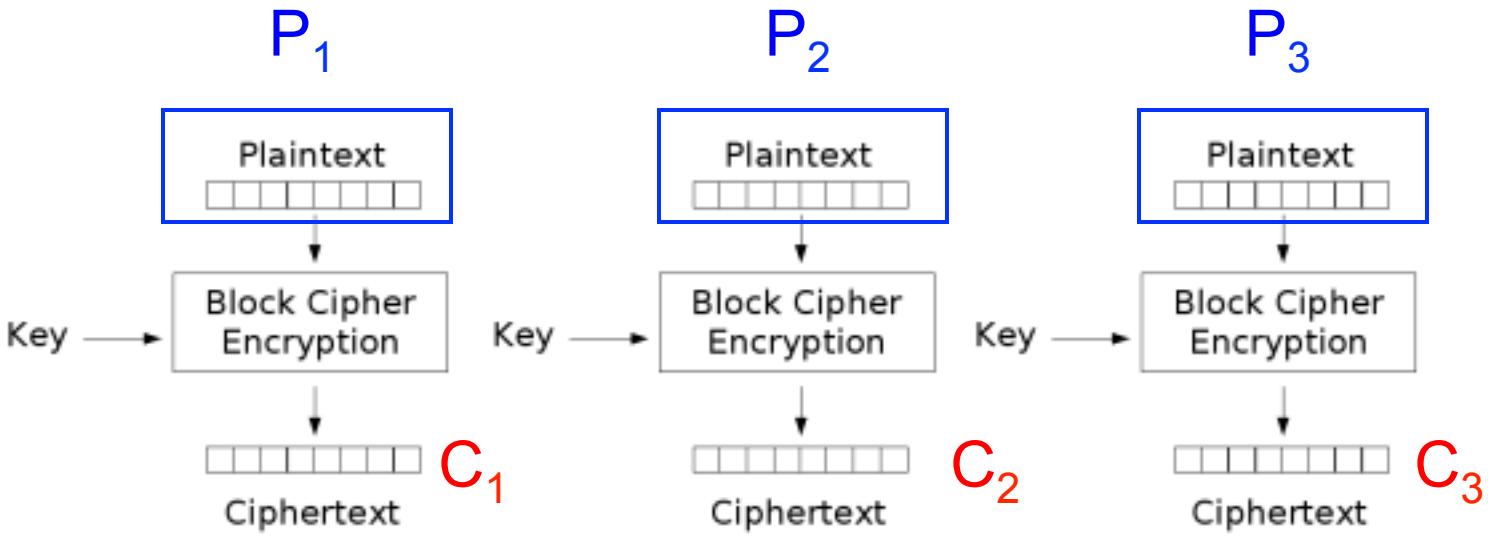
Symmetric-Key Cryptography

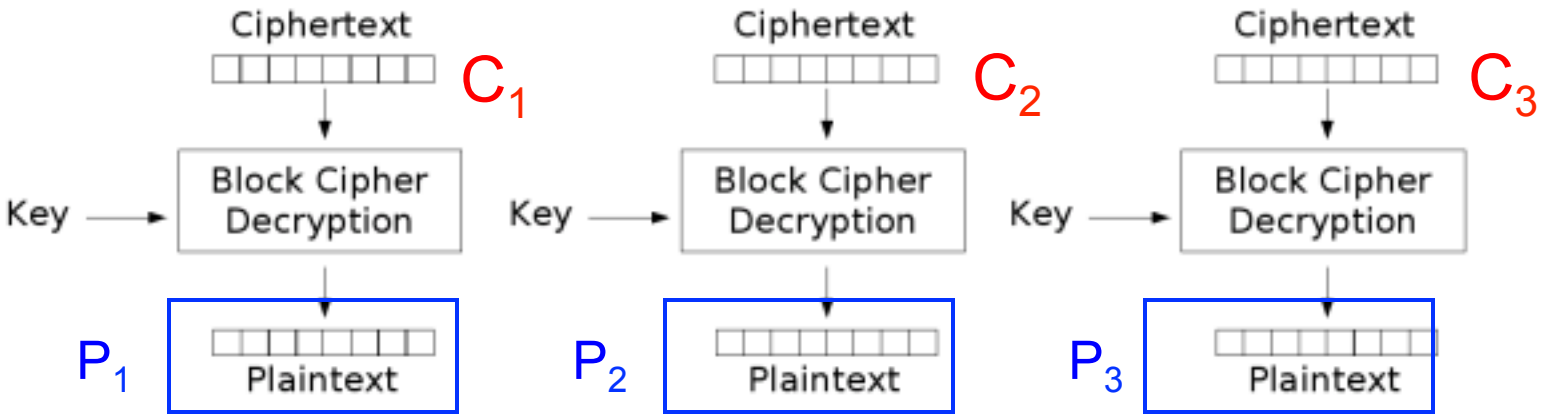
CS 161: Computer Security

Prof. David Wagner

March 12, 2013

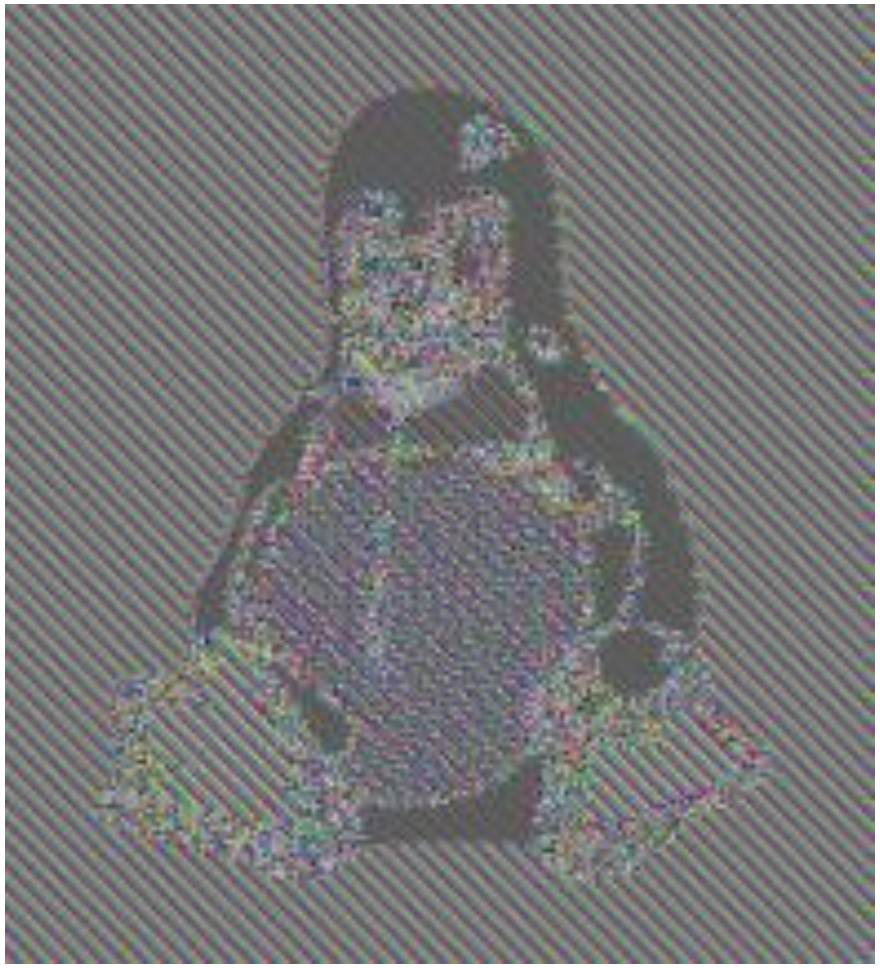


Electronic Codebook (ECB) mode encryption

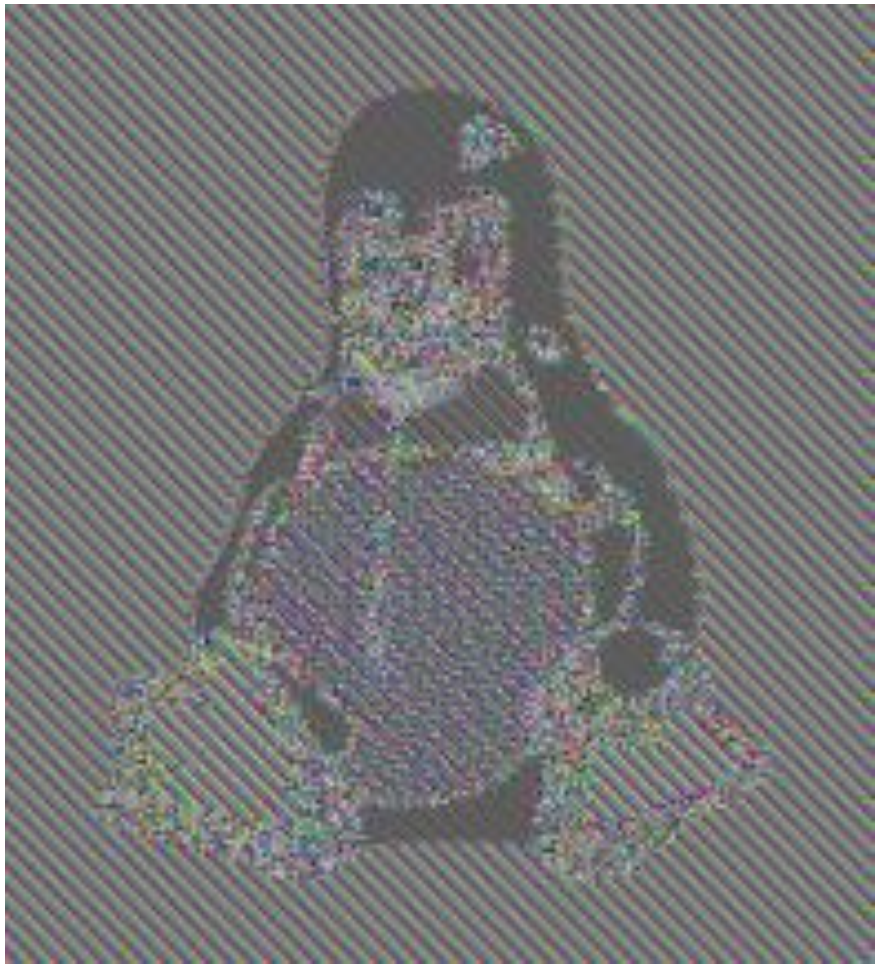


Electronic Codebook (ECB) mode decryption

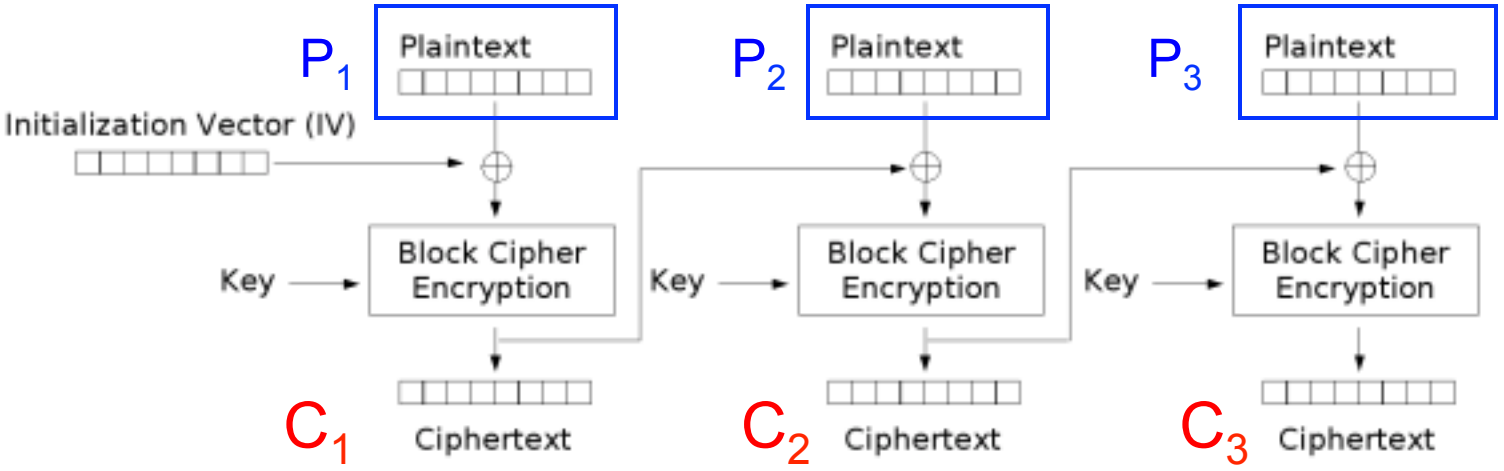
Original image



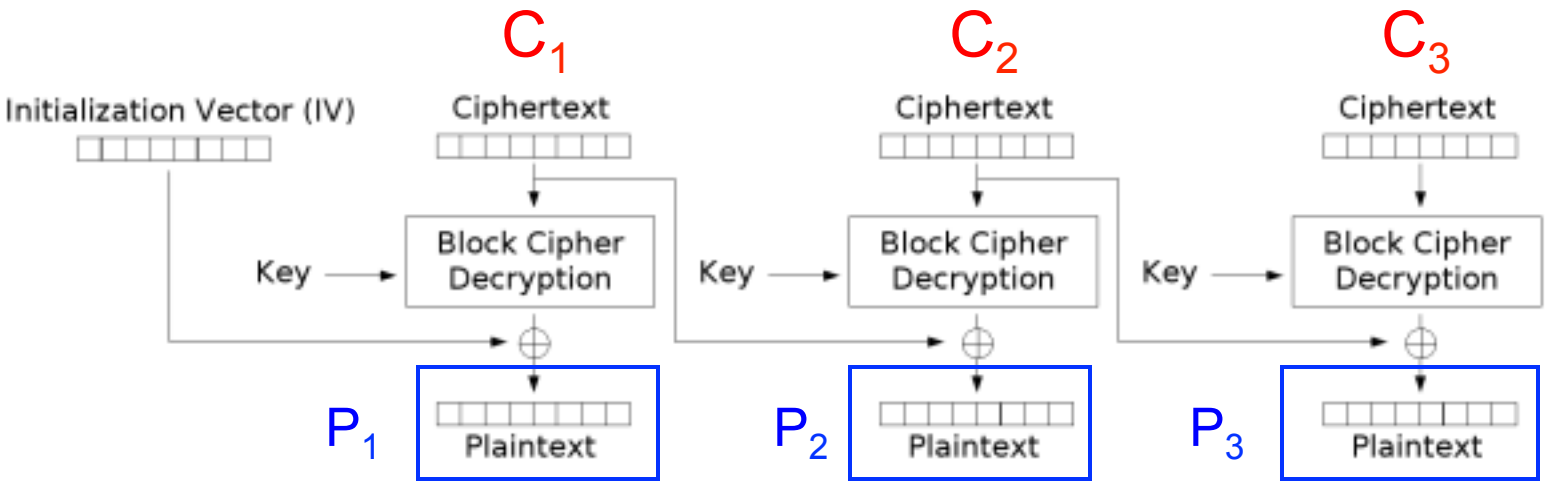
Encrypted with ECB



Later (identical) message again encrypted with ECB

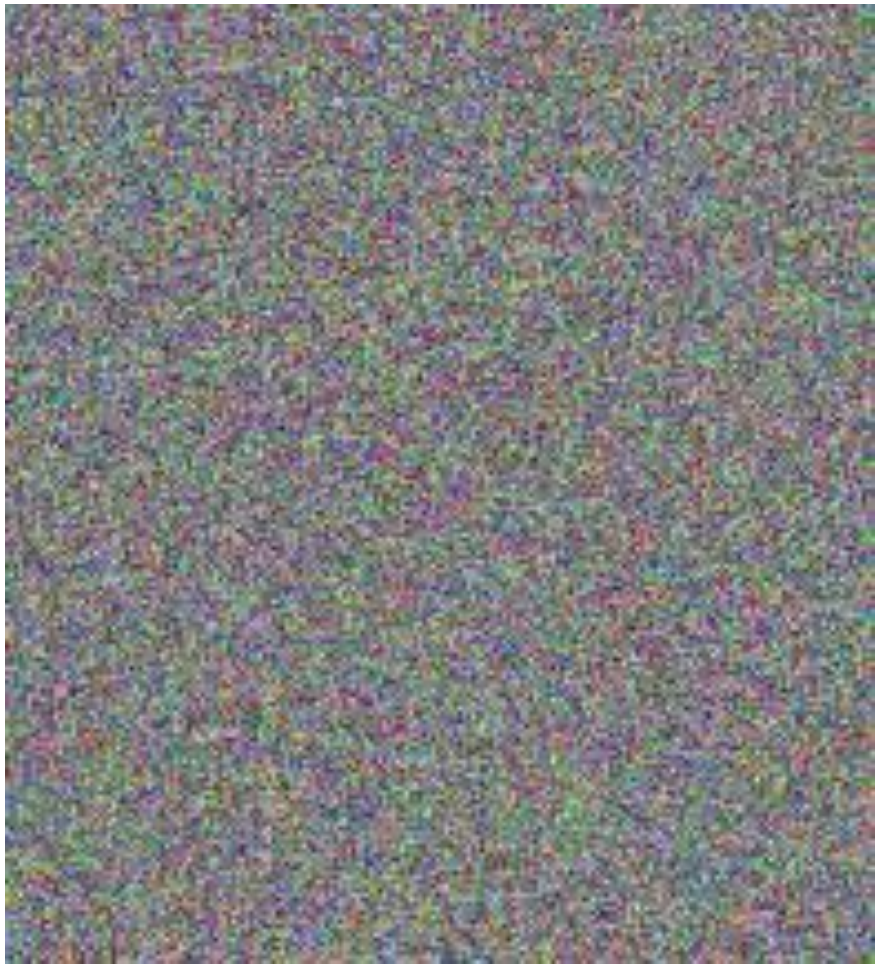


Cipher Block Chaining (CBC) mode encryption

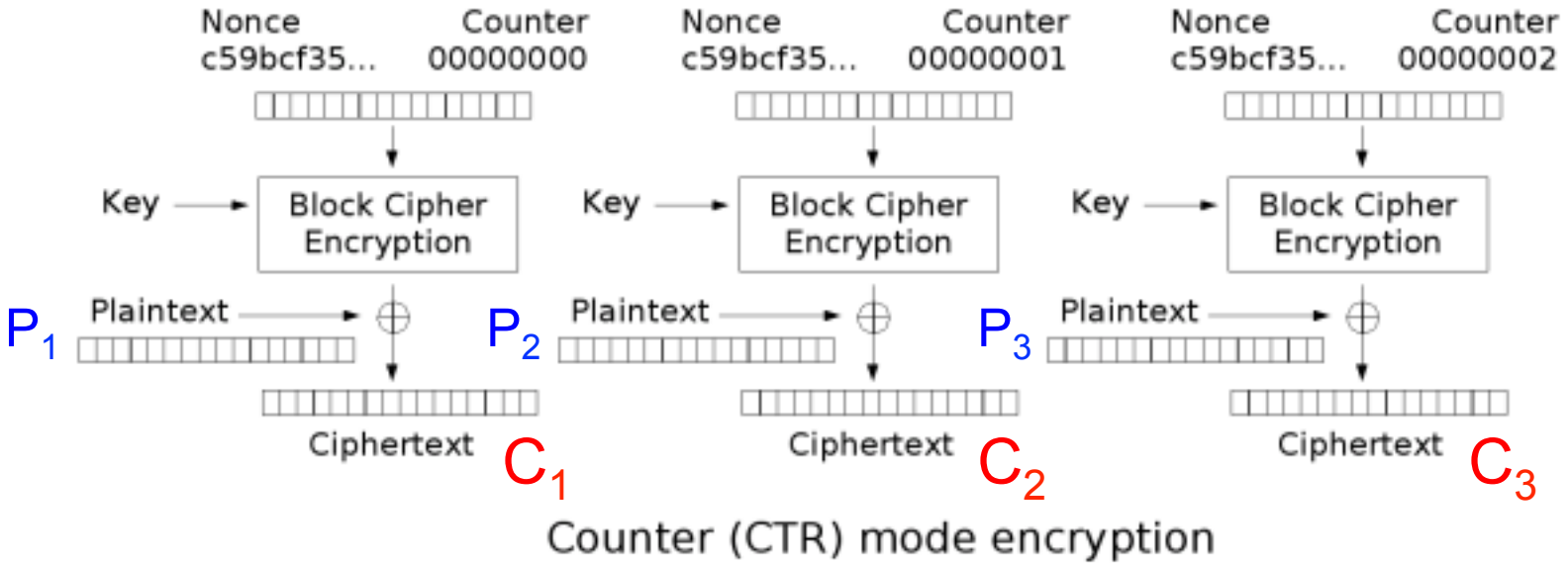


Cipher Block Chaining (CBC) mode decryption

Original image

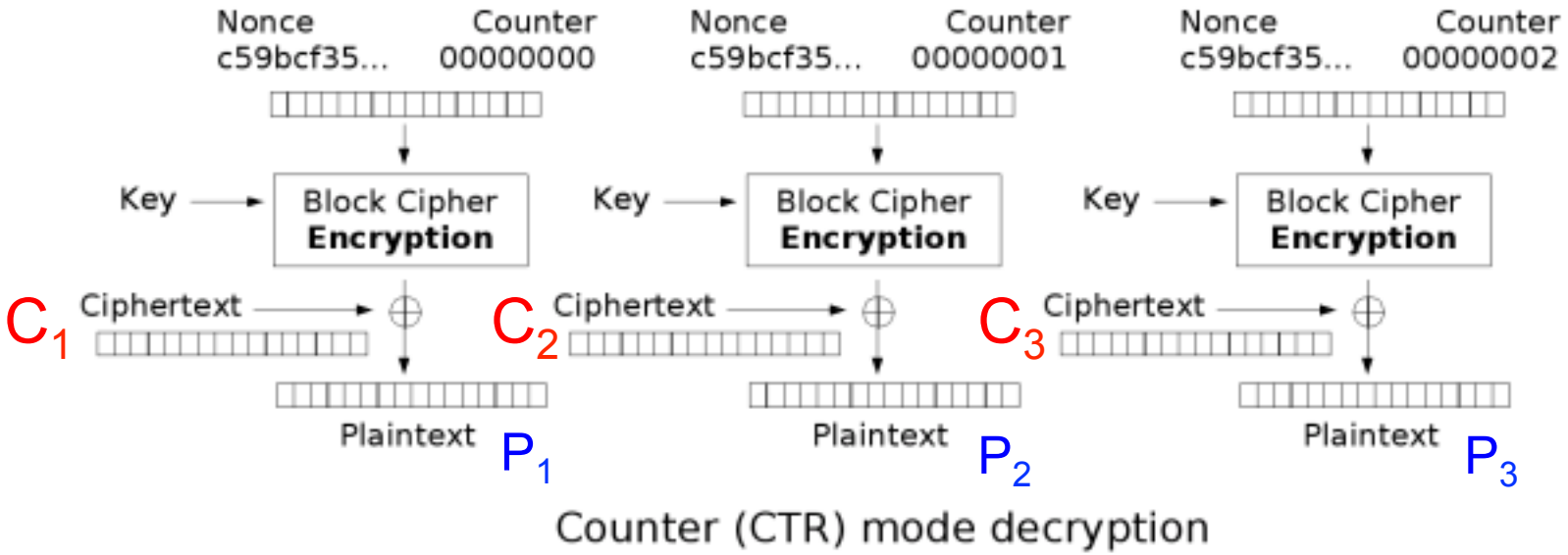


Encrypted with CBC



Counter (CTR) mode encryption

(Nonce = Same as IV)



Counter (CTR) mode decryption

(Note, CTR decryption uses block cipher's *encryption* functionality, not decryption)