Symmetric-Key Cryptography

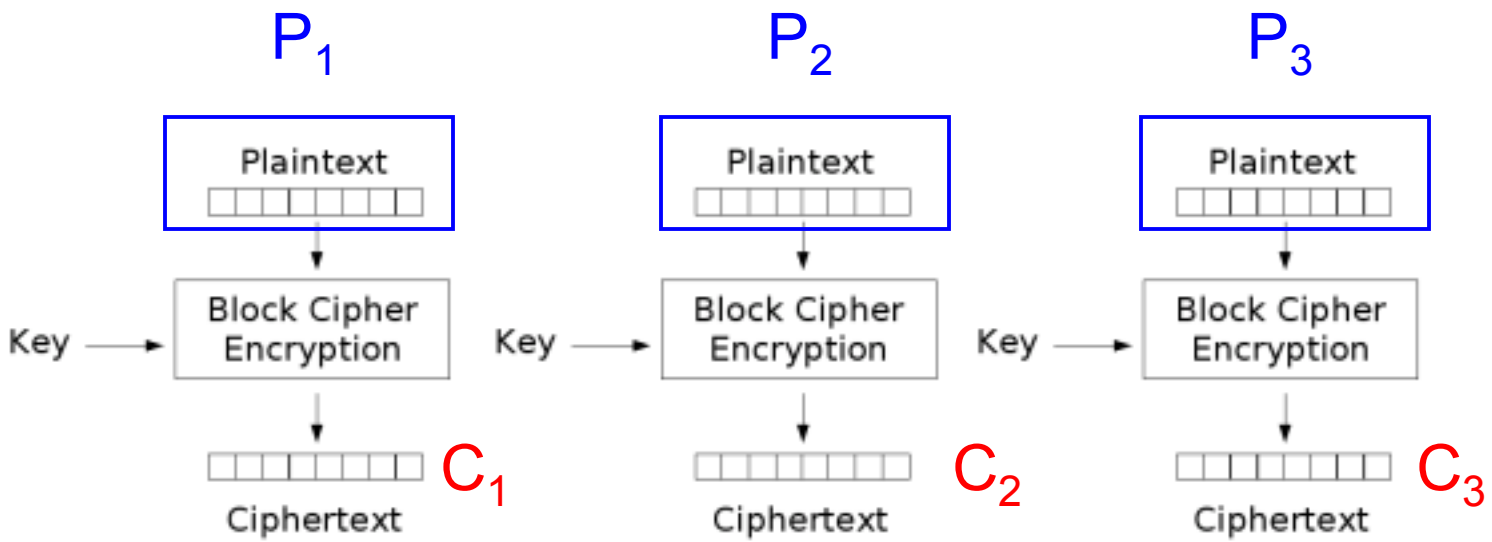
CS 161: Computer Security

Prof. Vern Paxson

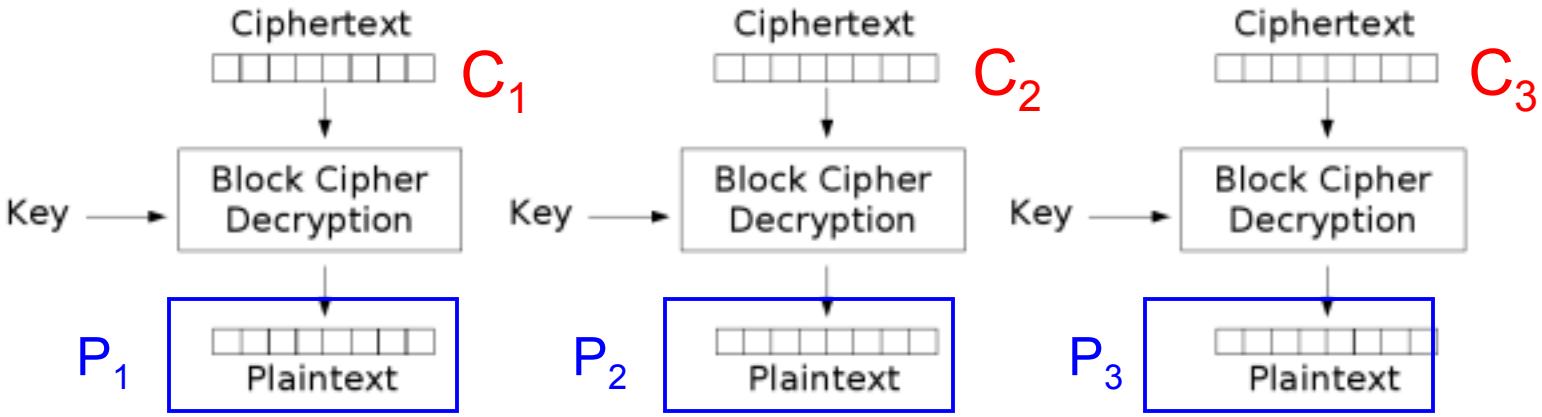
TAs: Jethro Beekman, Mobin Javed,
Antonio Lupher, Paul Pearce
& Matthias Vallentin

http://inst.eecs.berkeley.edu/~cs161/

March 12, 2013

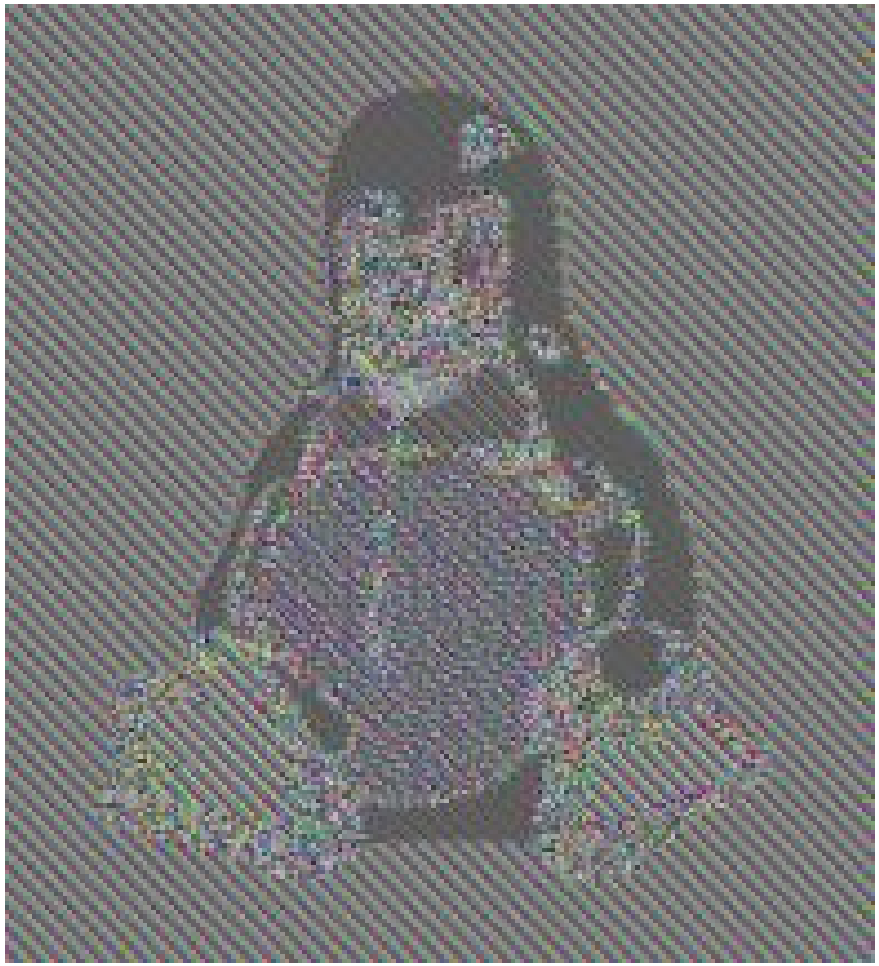


Electronic Codebook (ECB) mode encryption

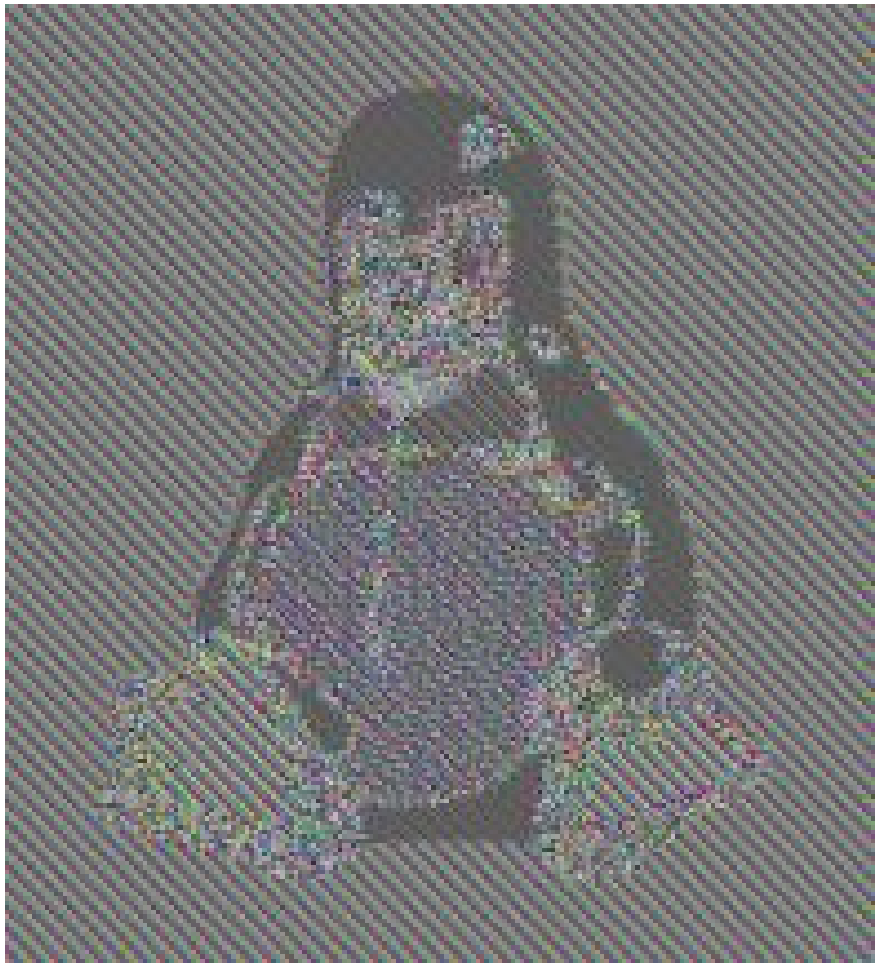


Electronic Codebook (ECB) mode decryption

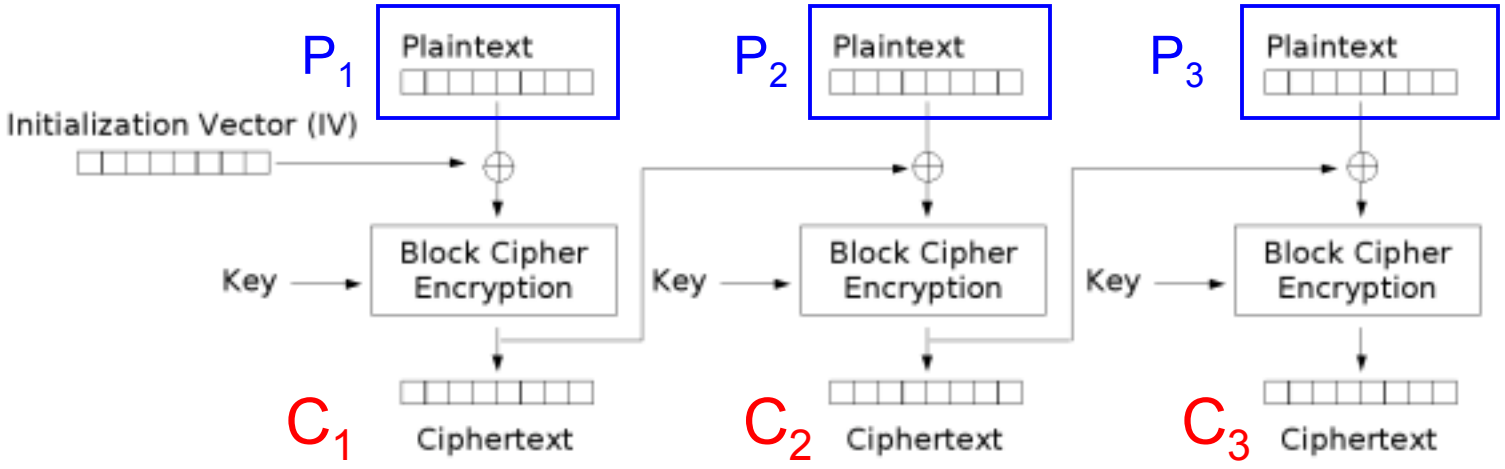
Original image



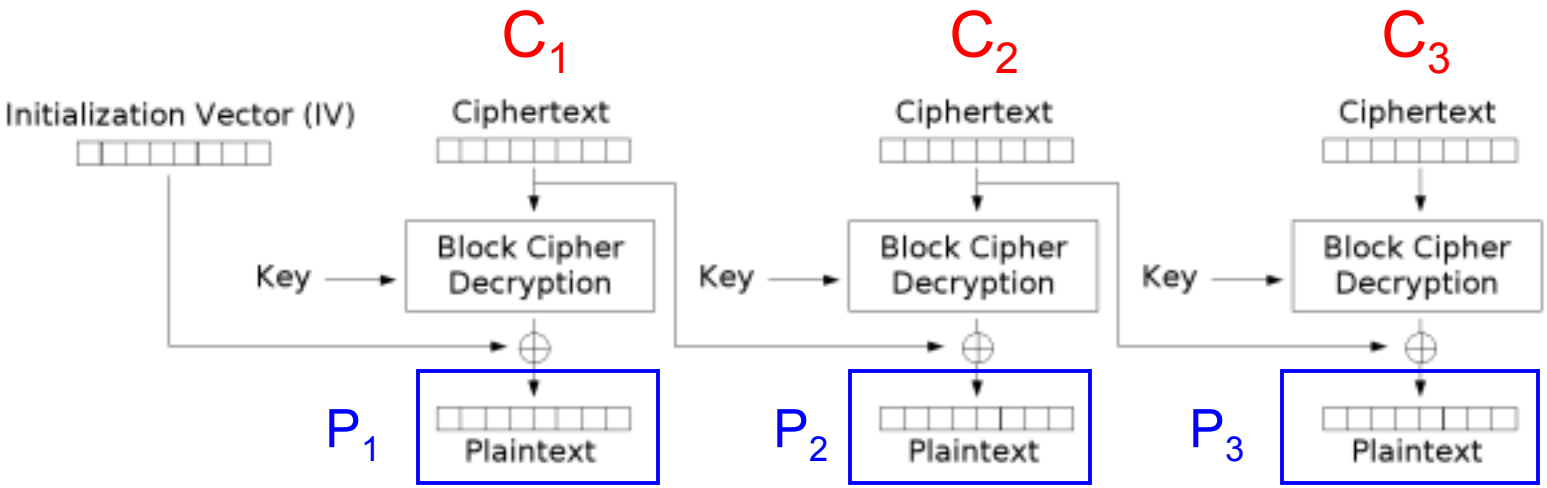
Encrypted with ECB



Later (identical) message again encrypted with ECB

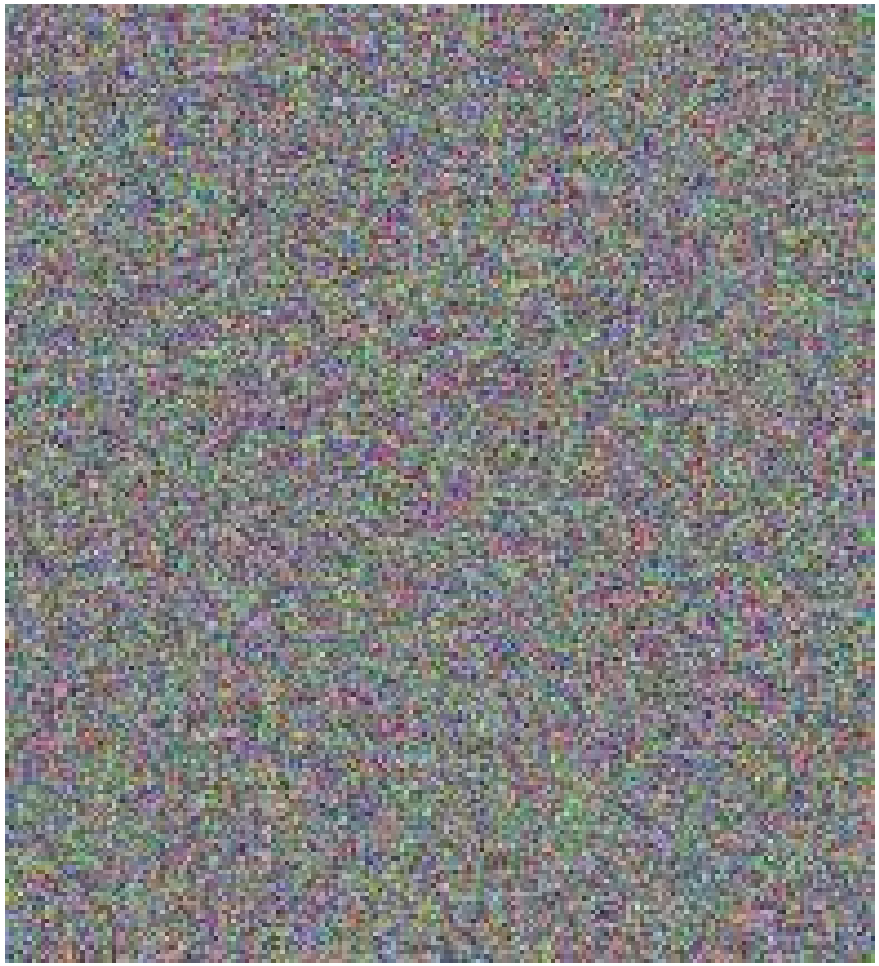


Cipher Block Chaining (CBC) mode encryption



Cipher Block Chaining (CBC) mode decryption

Original image



Encrypted with CBC