Symmetric-Key Cryptography

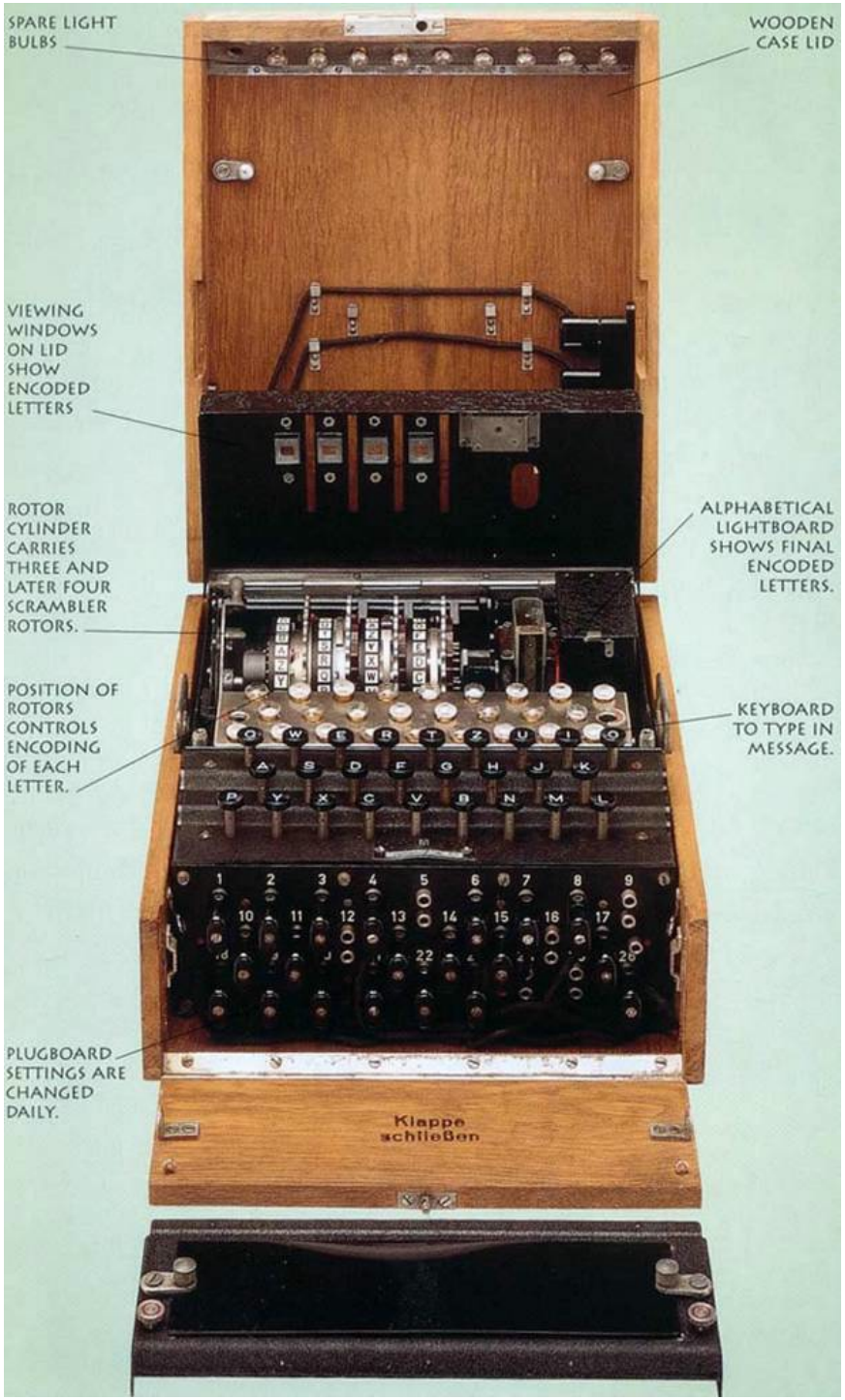
CS 161: Computer Security

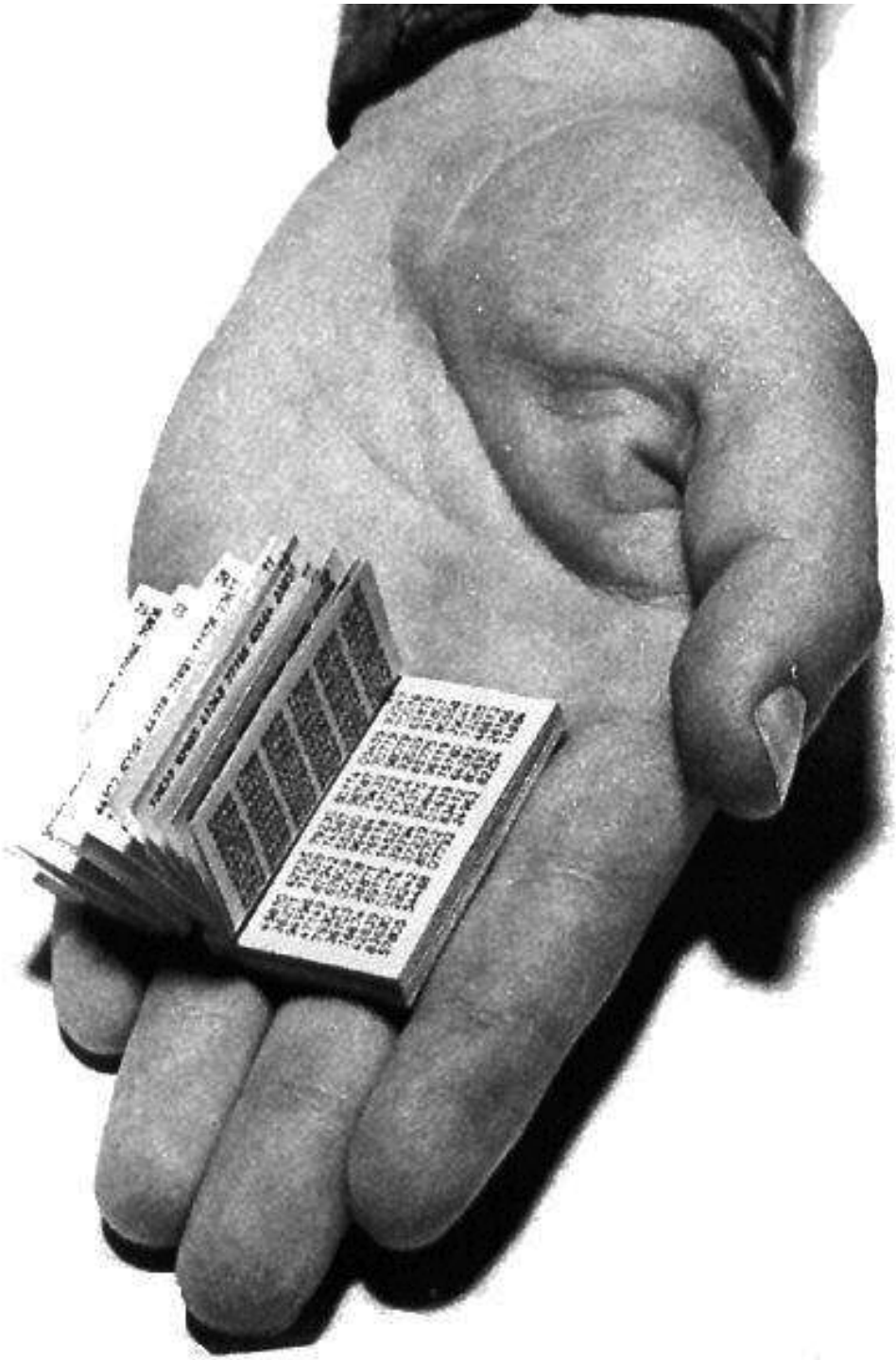
Prof. Vern Paxson

TAs: Devdatta Akhawe, Mobin Javed & Matthias Vallentin

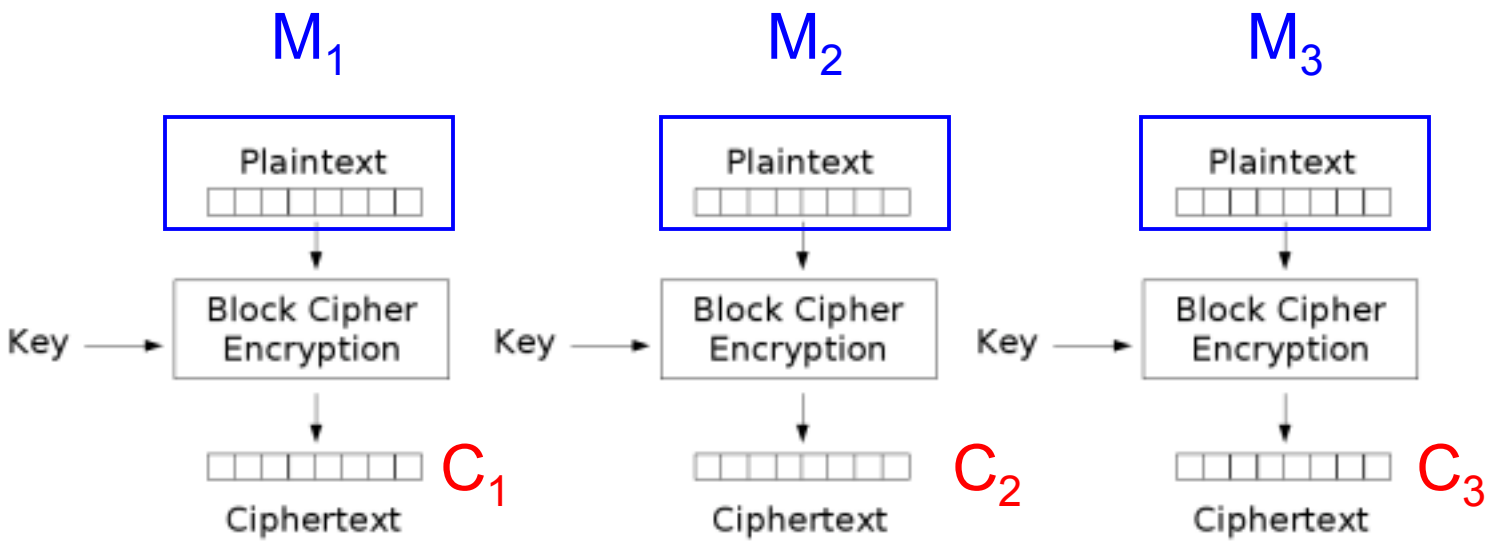
http://inst.eecs.berkeley.edu/~cs161/

March 10, 2011

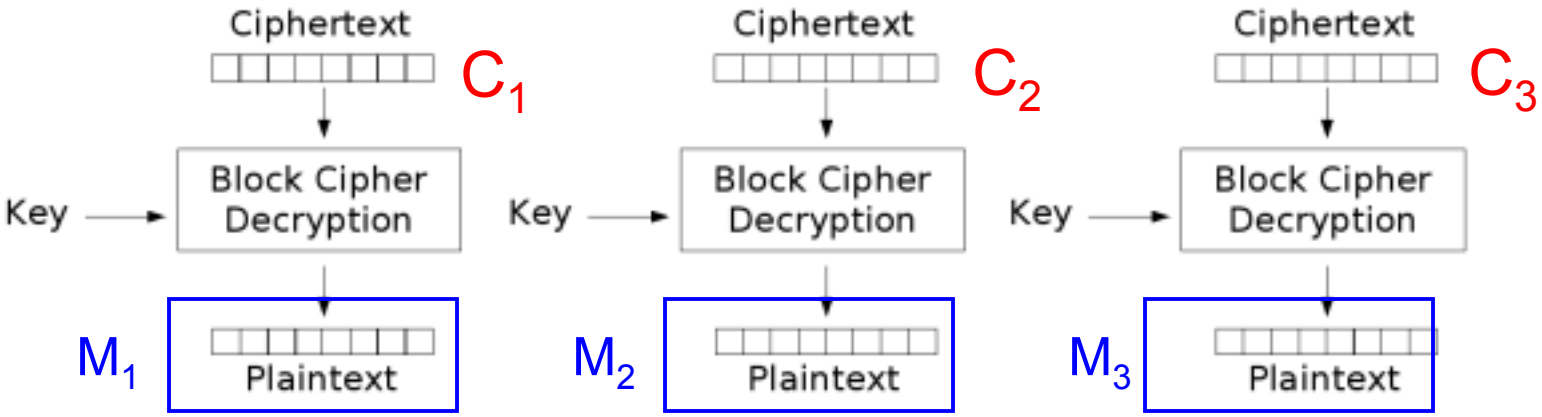

SPARE LIGHT BULBS
WOODEN CASE LID
VIEWING WINDOWS ON LID SHOW ENCODED LETTERS
ROTOR CYLINDER CARRIES THREE AND LATER FOUR SCRAMBLER ROTORS.
ALPHABETICAL LIGHTBOARD SHOWS FINAL ENCODED LETTERS.
POSITION OF ROTORS CONTROLS ENCODING OF EACH LETTER.
KEYBOARD TO TYPE IN MESSAGE.
PLUGBOARD SETTINGS ARE CHANGED DAILY.
Klappe schließen




12-116
12-112
12-113
© D. Rijmenants 2009

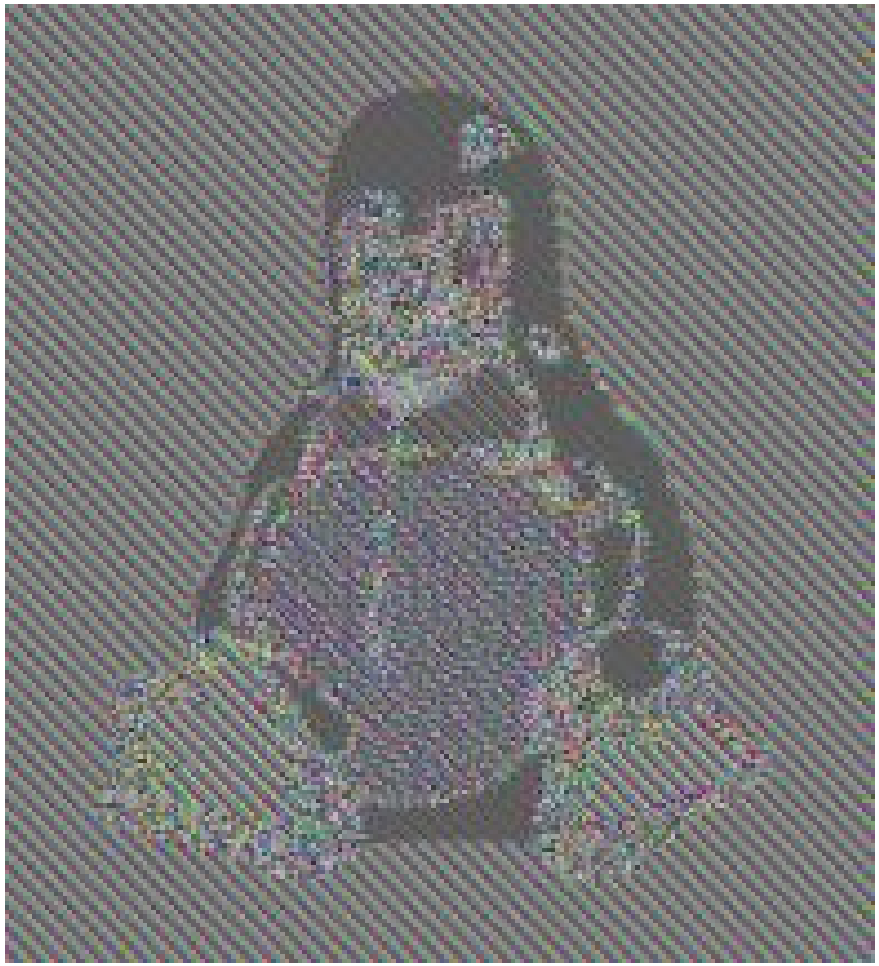


Electronic Codebook (ECB) mode encryption

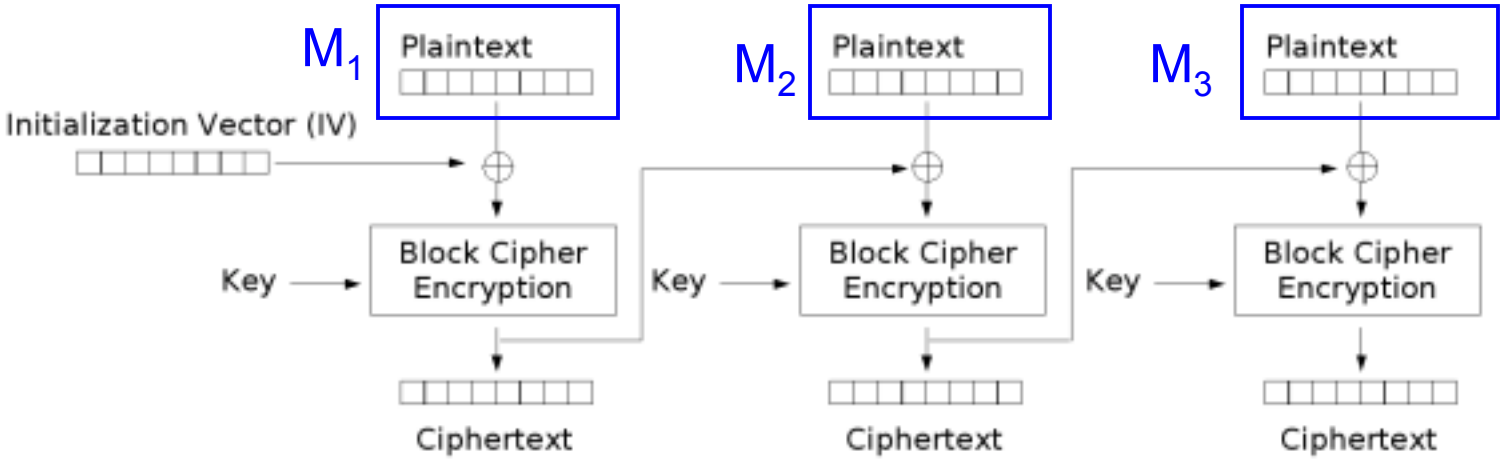


Electronic Codebook (ECB) mode decryption

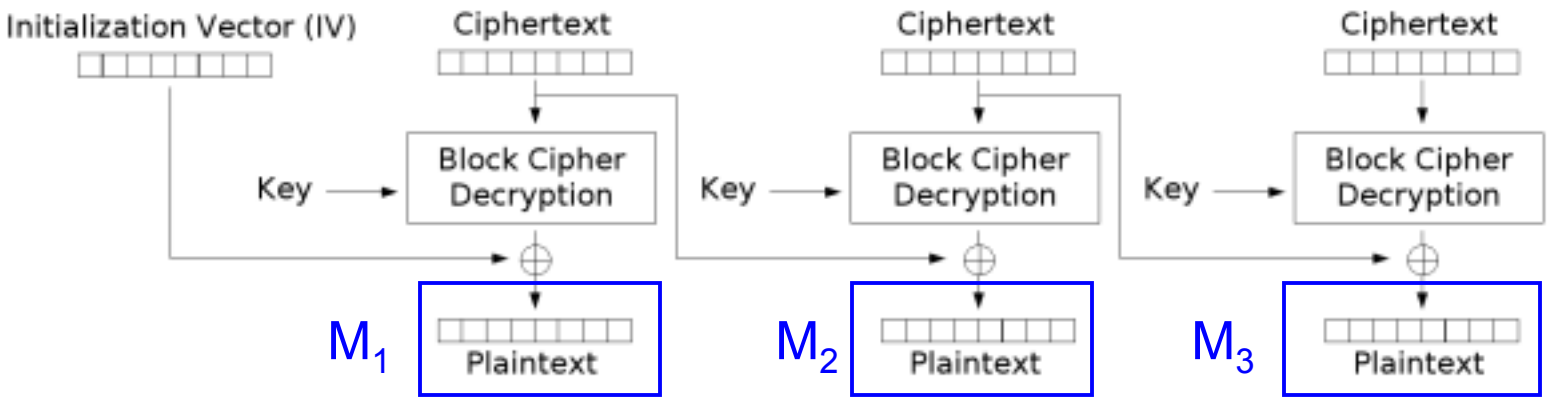
Original image



Encrypted with ECB

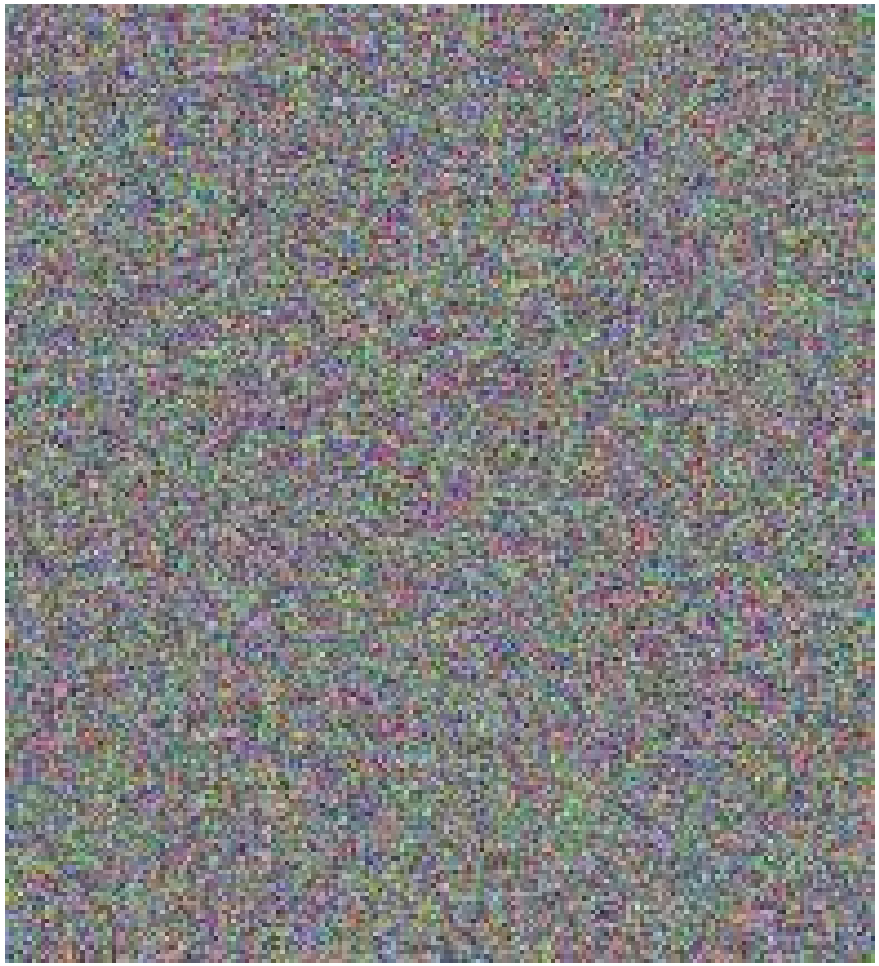


Cipher Block Chaining (CBC) mode encryption

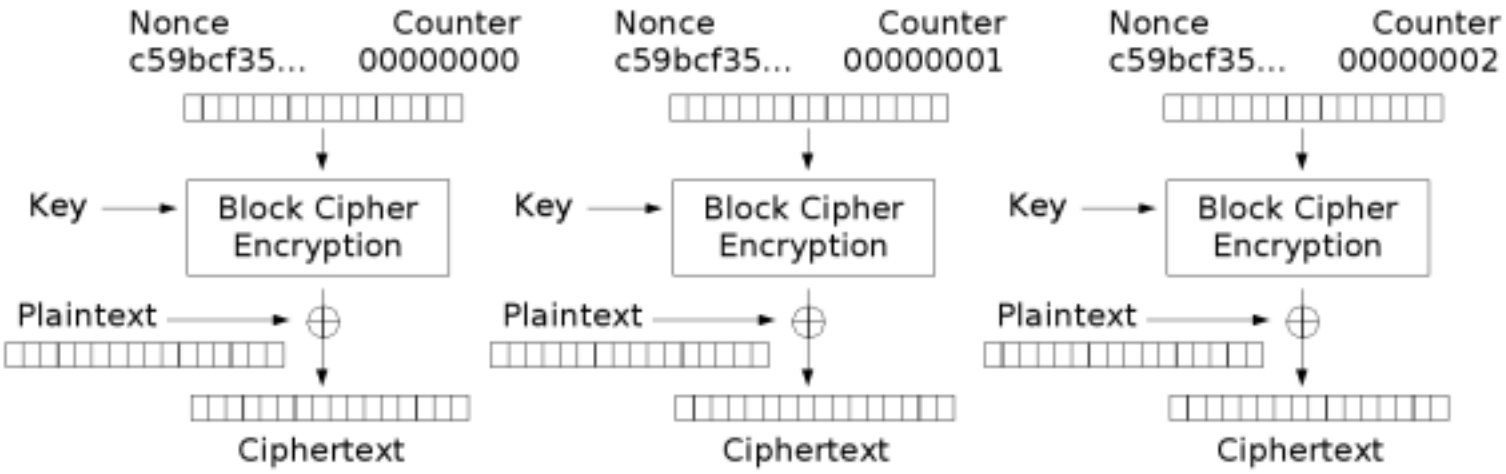


Cipher Block Chaining (CBC) mode decryption

Original image

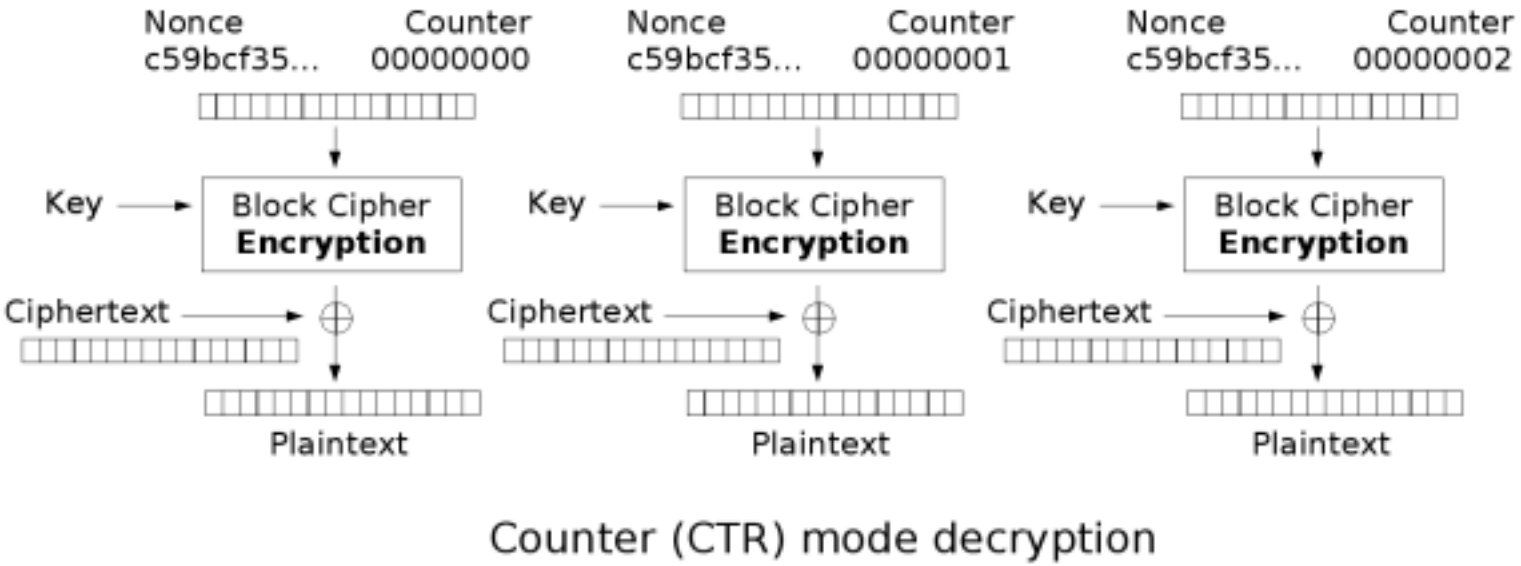


Encrypted with CBC



Counter (CTR) mode encryption

(Nonce = Same as IV)



Counter (CTR) mode decryption

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