

Attacks on Block Cipher Modes of Operation

RPISEC

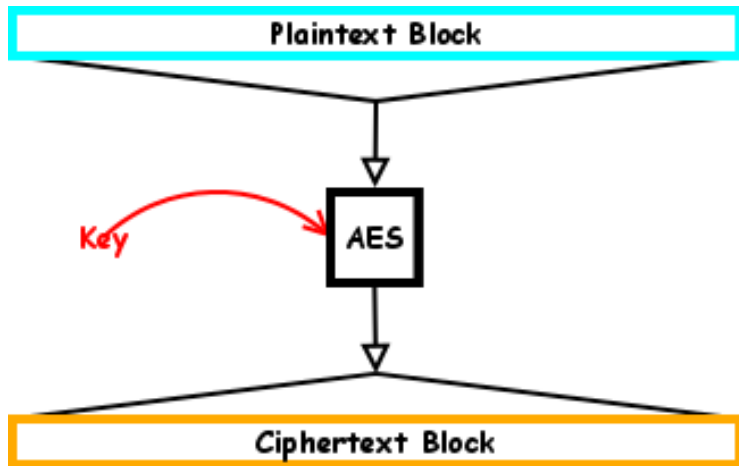
Avi Weinstock (aweinstock), Adam Freeman (triazio)

November 11, 2016

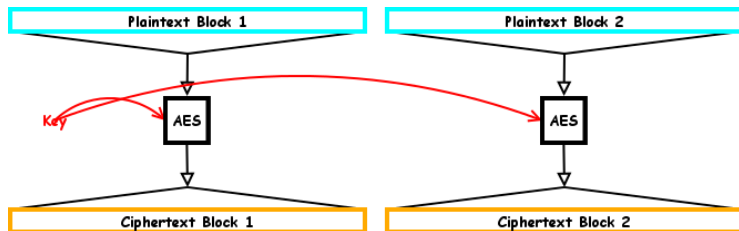
Setup

- ▶ Python libraries: `sudo pip install pycrypto pwntools`
- ▶ pycrypto is practically required, pwntools is merely recommended.
- ▶ triazo is currently hosting the challenges at <http://blackbox.rpi.rip/>
- ▶ You can get an offline copy of the challenges from <https://github.com/pbiernat/BlackBox>

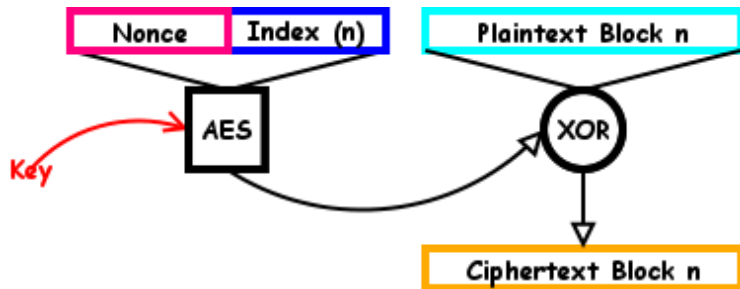
What is a Block Cipher?



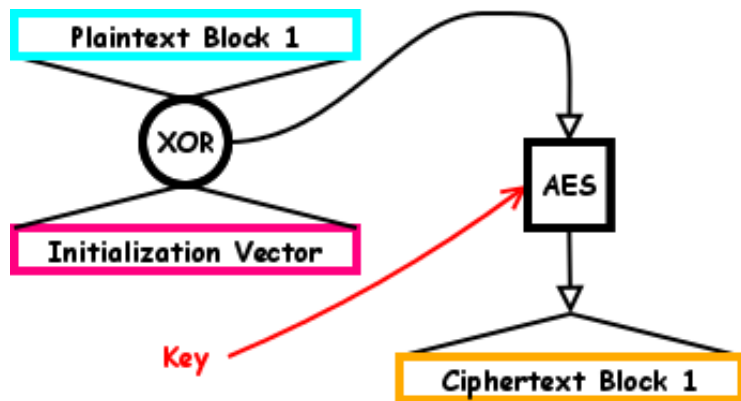
Electronic Code Book (ECB)



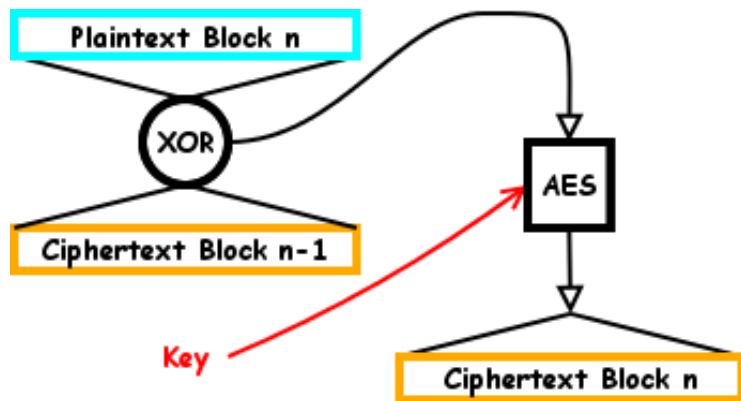
Counter (CTR)



Cipher Block Chaining (CBC)



Cipher Block Chaining (CBC)



Resources

- ▶ https://en.wikipedia.org/wiki/Block_cipher
- ▶ https://en.wikipedia.org/wiki/Block_cipher_modes_of_operation
- ▶ <https://cryptopals.com/>