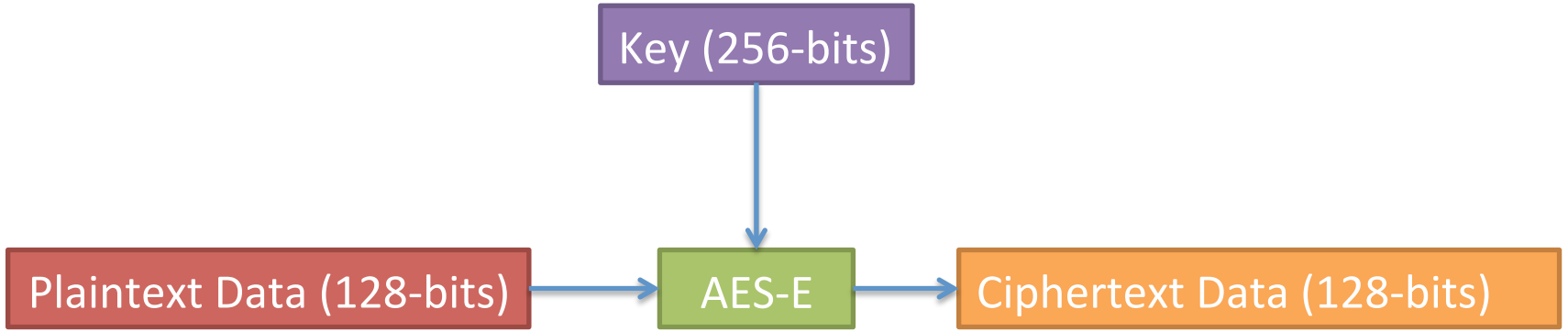
Operating Modes

Introduction to Basic Cryptography

Dr. Ryan Riley

Recall…

- Block ciphers encrypt fixed size data blocks using fixed size keys



Large Messages?

- Given a key, a block cipher can encrypt a block of data
- What if I want to encrypt more than just a block?

- Example:
  - AES: 128-bit (16-bytes) block size
  - Want to encrypt a 30 MB video

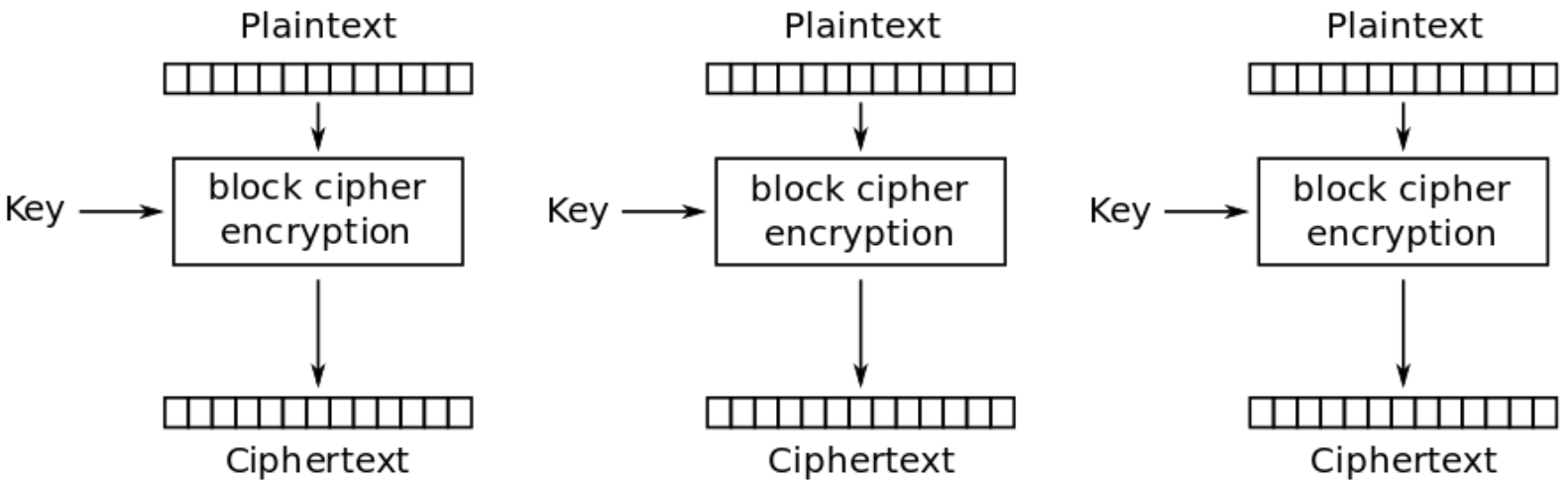
Block Cipher Operating Modes

- We need to break up the data into blocks and then encrypt those
- The way we do this impacts security
- There are 5 traditional ways, called *operating modes*
  - We're going to cover 3
- There are more than even the 5

Electronic Code Book (ECB)

- Obvious method
- Break data into blocks, encrypt each block independently
- Use the same key for every block

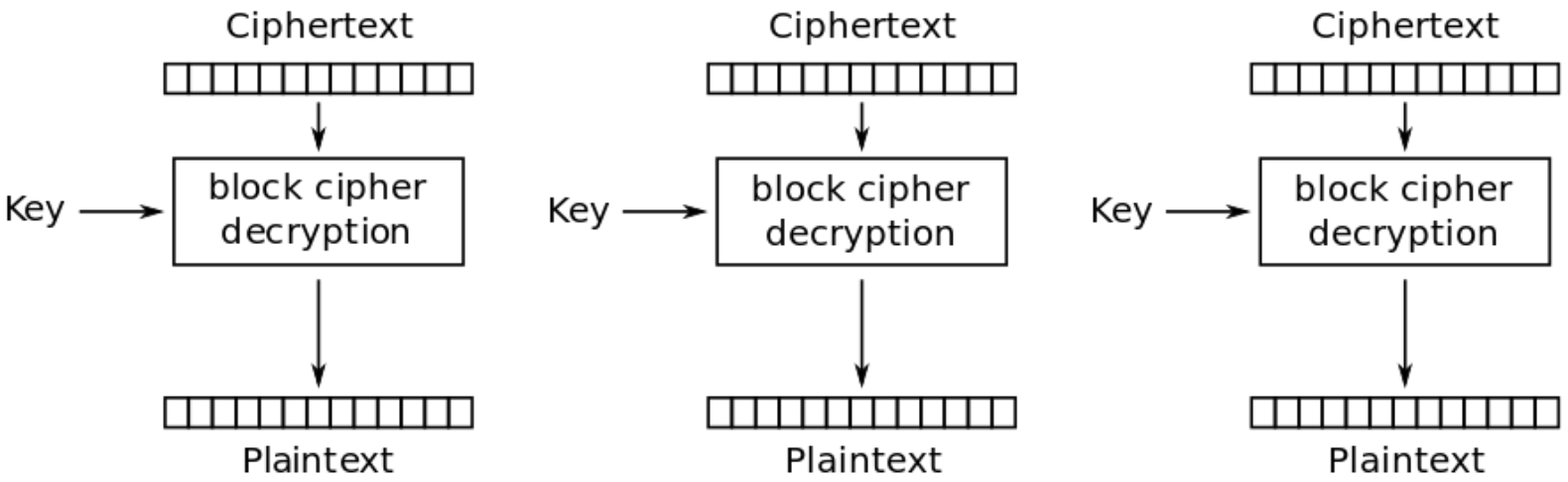
ECB: Encryption



Electronic Codebook (ECB) mode encryption

From: http://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

ECB: Decryption



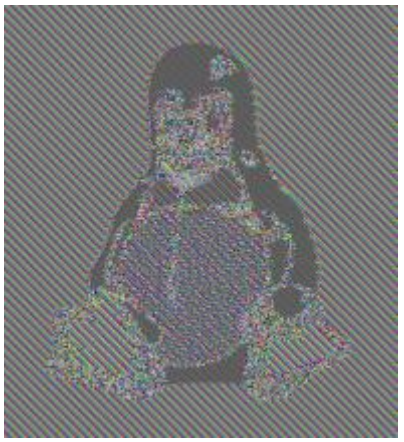
Electronic Codebook (ECB) mode decryption

From: http://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

ECB: Problem

- The same PT blocks produce the same CT blocks
  - Just like a substitution cipher in the simple ciphers
  - Many computer files have duplicate blocks, and we don't want an attacker to be able to tell this

Plaintext

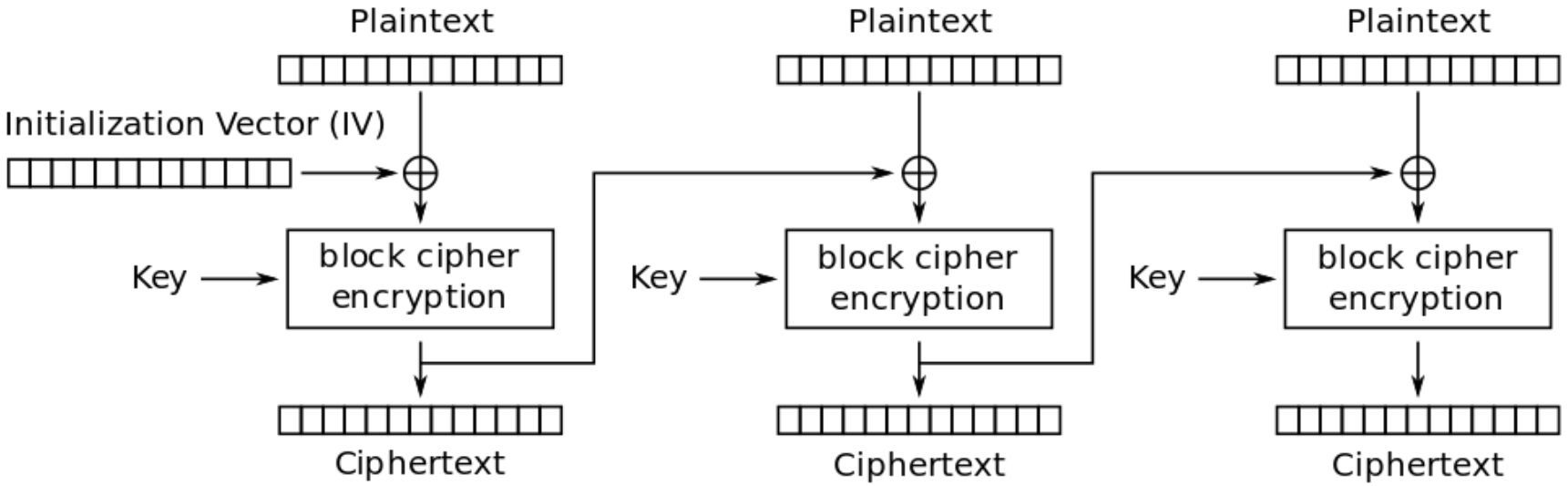


AES-ECB

Cipher Block Chaining (CBC)

- Each block is dependent on the previous one
  - This fixes many of the problems with ECB

CBC: Encryption



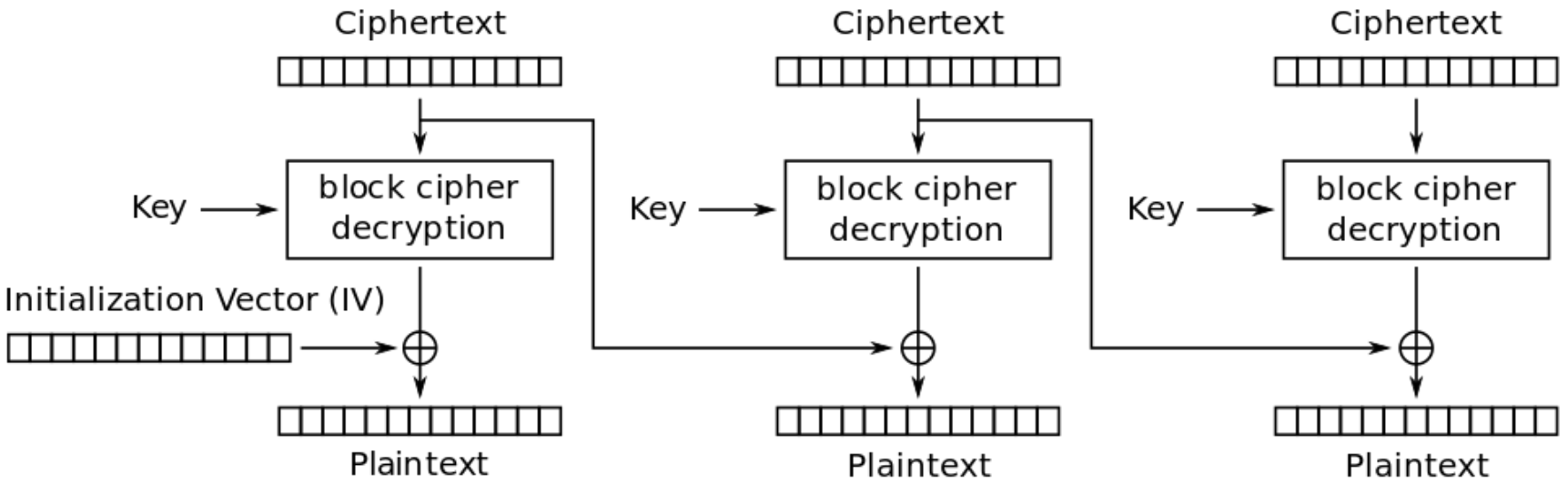
Cipher Block Chaining (CBC) mode encryption

From: http://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

CBC: Initialization Vector (IV)

- The CT of each block is dependent on the previous block
- The first block has no previous block
- We pick a random value, called the *initialization vector* (IV)

CBC: Decryption



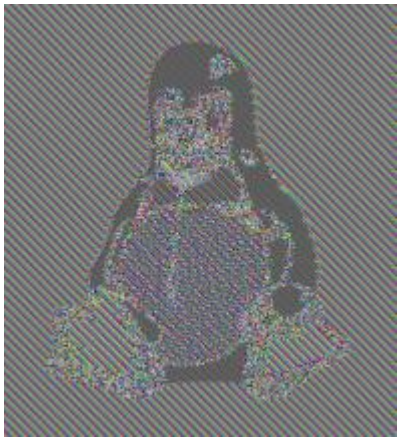
Cipher Block Chaining (CBC) mode decryption

From: http://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

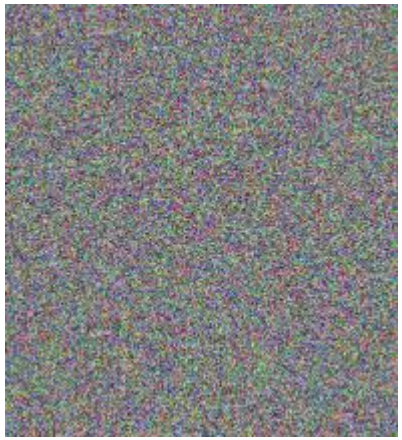
CBC: Better than ECB?

- Remember the ECB problem of one-to-one PT, CT mappings?

Plaintext



AES-ECB



AES-CBC

CBC: Problem

- If I want to change the PT of one block, I must re-encrypt every following block
  - It's a chain, remember?

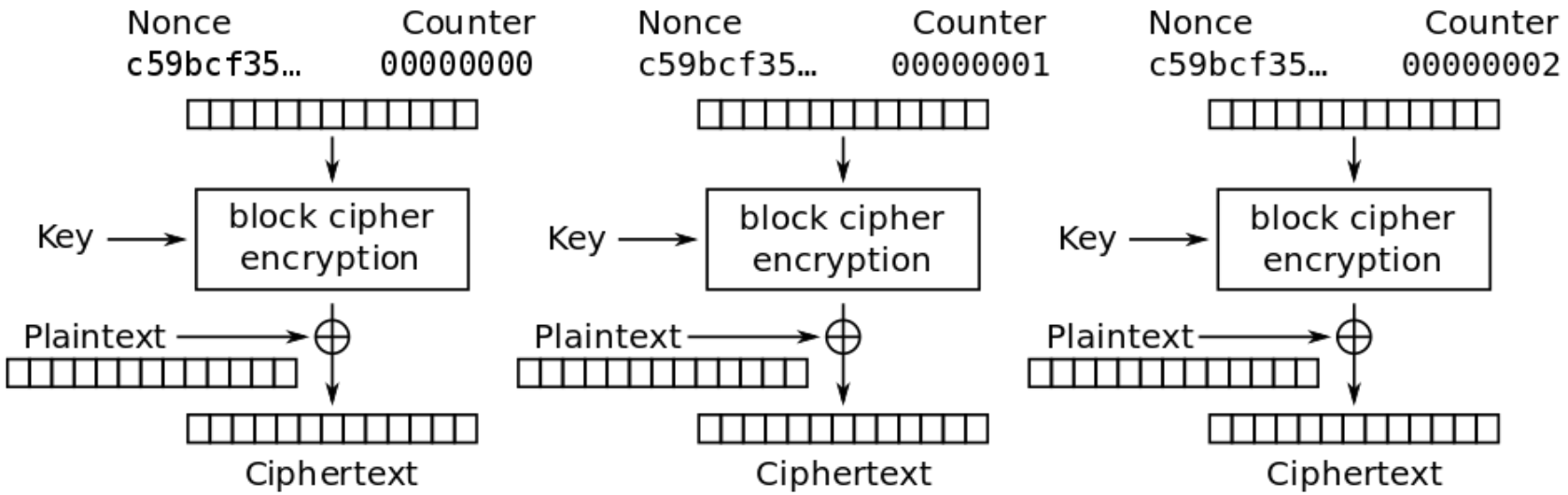
- For some cases, this is bad
  - Encrypted file systems, for example

Counter (CTR)

- Simulates a stream cipher
- Each block is encrypted independently, but it involves an incrementing *nonce*

- A nonce is a number chosen randomly, but is not a secret
  - Identical to an IV, but a different name just because of how it is used

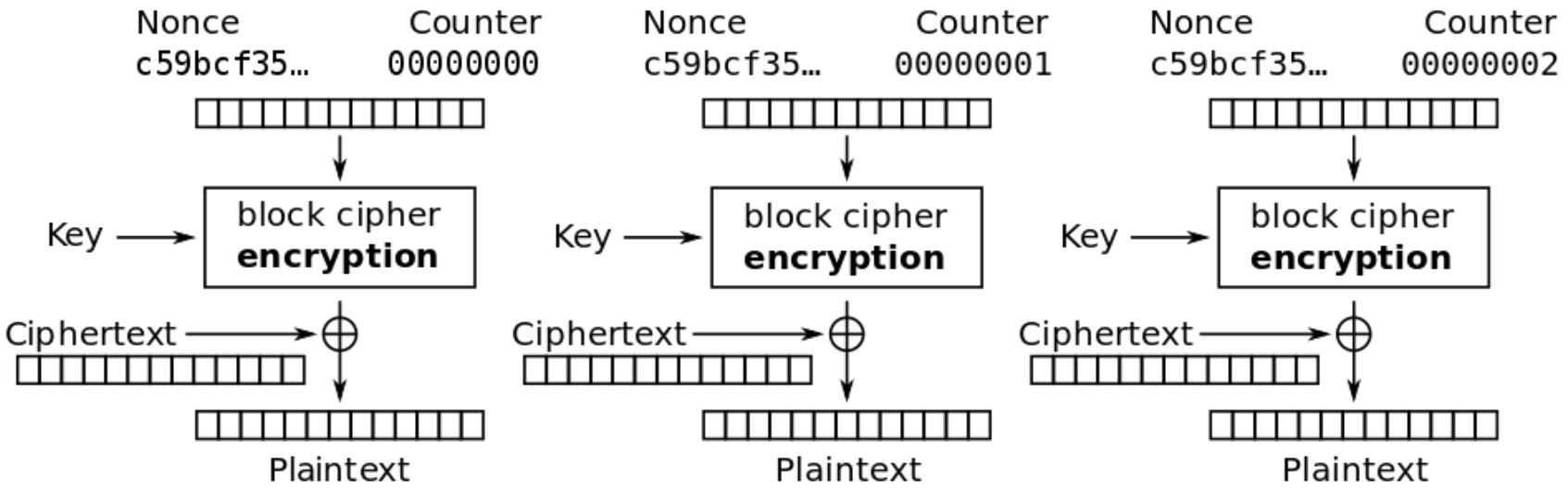
CTR: Encryption



Counter (CTR) mode encryption

From: http://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

CTR: Decryption



Counter (CTR) mode decryption

From: http://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

Operating Modes

- You need to spend some more time reading and thinking about these in order to get them
- They are hard at first, but easy later
- Read the Wikipedia entry on "Block Cipher Mode of Operation"
  - It is very good
  - Learn the strengths and weaknesses
- For many use cases, CBC is what you want to use

Summing Up

- When using block ciphers to encrypt data larger than one block, you need to pick an operating mode
- Your choice impacts security, performance, etc.