Symmetric-Key Cryptography

CS 161: Computer Security

Prof. Raluca Ada Popa

February 22, 2016

Announcements

- Wednesday, Feb 24
  - 8-9:30pm (in 155 Dwinelle)
  - Covers material up to today
  - Cheat sheet double sided
- Review session on Wed in lecture
  - Sample example questions, review material before
- Homework 2 (due today)

Special guests

- Alice 
- Bob 
- The attacker (Eve - “eavesdropper”, Malice)  
- Sometimes Chris too

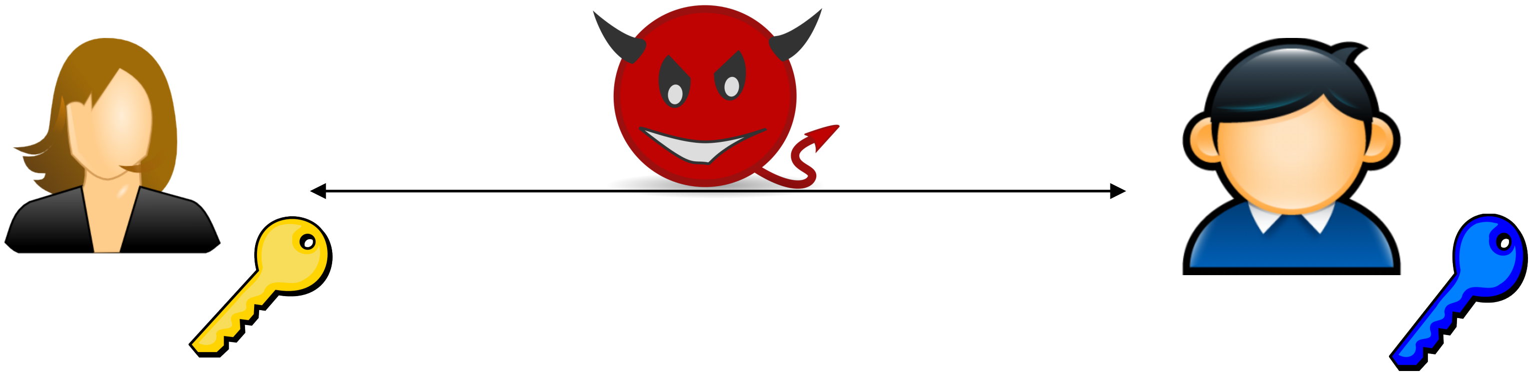
Cryptography

- Narrow definition: secure communication over insecure communication channels
- Broad definition: a way to provide formal guarantees in the presence of an attacker

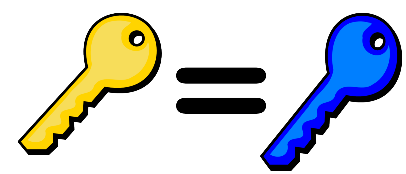
Three main goals

- Confidentiality: preventing adversaries from reading our private data,
- Integrity: preventing attackers from altering some data,
- Authenticity: determining who created a given document

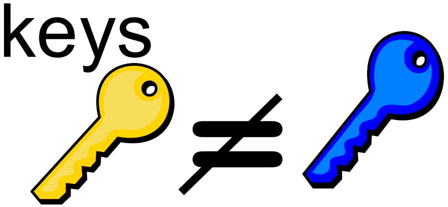
Modern Cryptography



- Symmetric-key cryptography
  - The same secret key is used by both endpoints of a communication



- Public-key cryptography
  - Sender and receiver use different keys



Today: Symmetric-key Cryptography

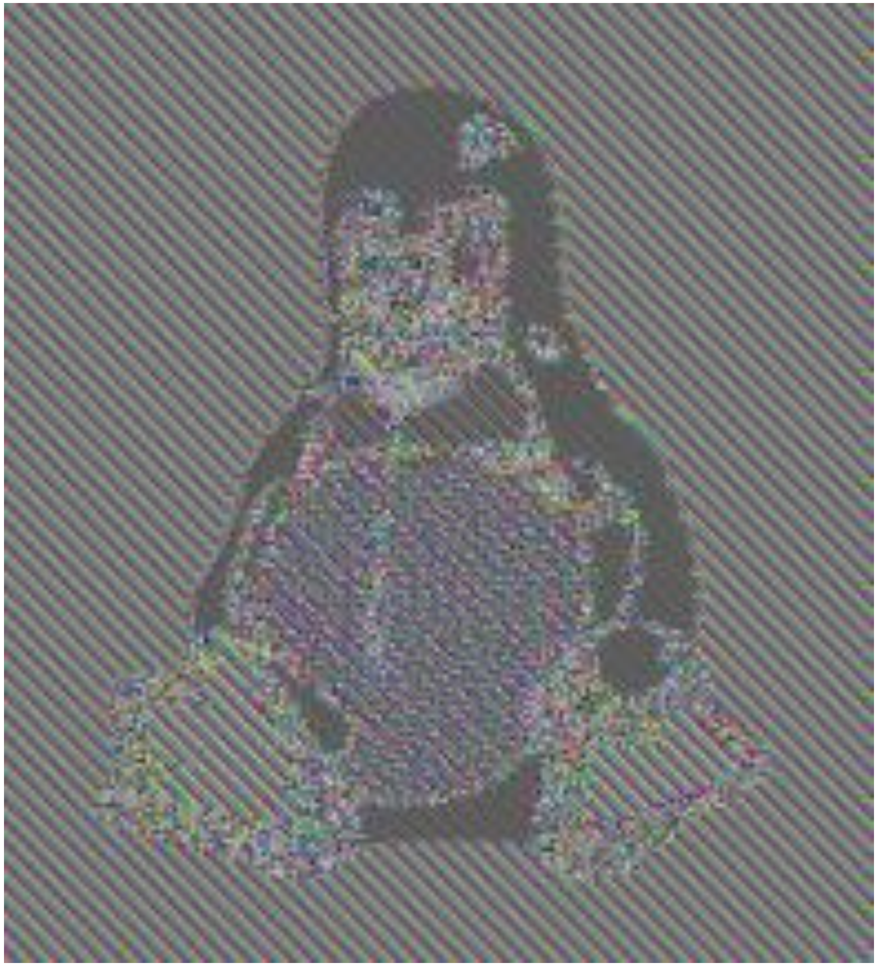
Whiteboard & notes:

- Symmetric encryption definition
- Security definition
- One time pad (OTP)
- Block cipher

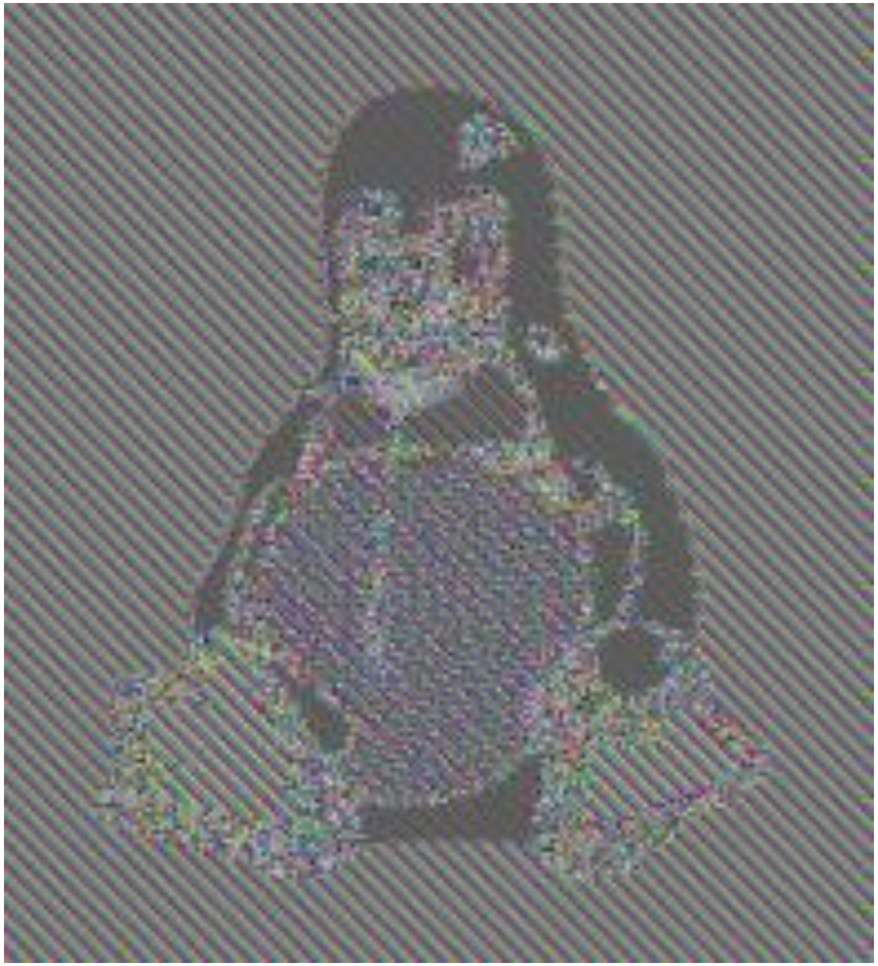
Why block ciphers not enough for encryption by themselves?

- Can only encrypt messages of a certain size
- If message is encrypted twice, attacker knows it is the same message

Original image



Eack block encrypted with a block cipher



Later (identical) message again encrypted

Symmetric key encryption scheme

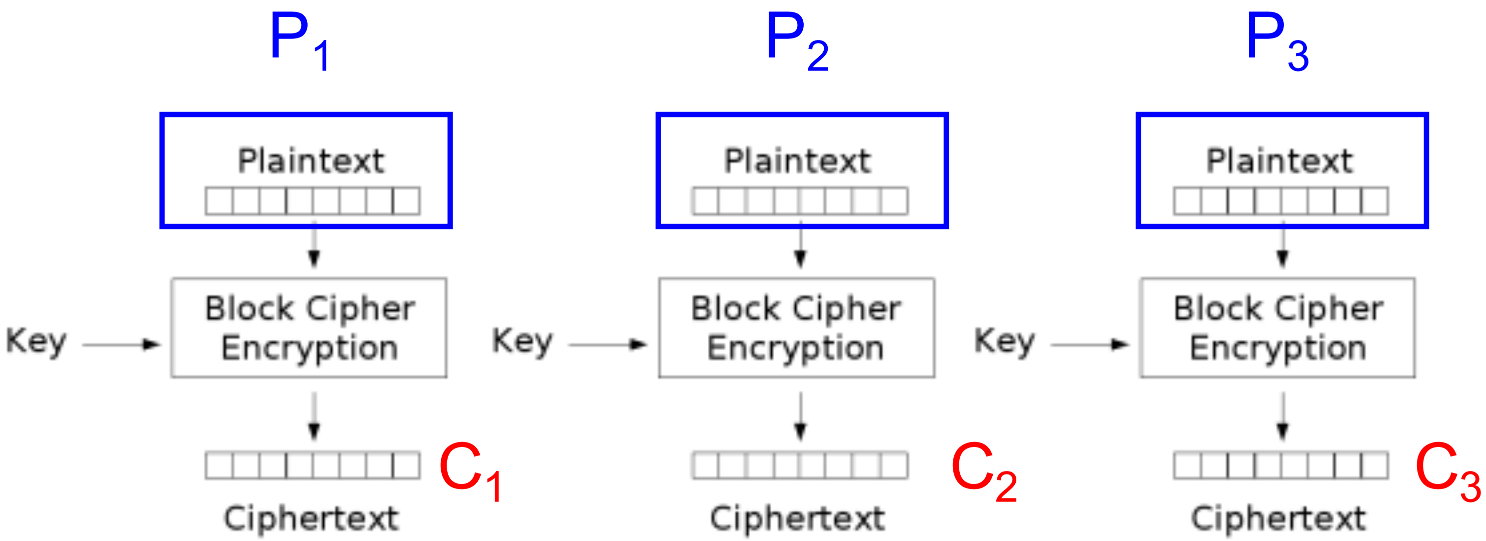
- Can be reused (unlike OTP)
- Builds on block ciphers:
  - Can be used to encrypt long messages
  - Wants to hide that same block is encrypted twice
- Uses block ciphers in certain modes of operation

Electronic Code Book (ECB)

- Split message in blocks P_1, P_2, …
- Each block is a value which is substituted, like a codebook
- Each block is encoded independently of the other blocks

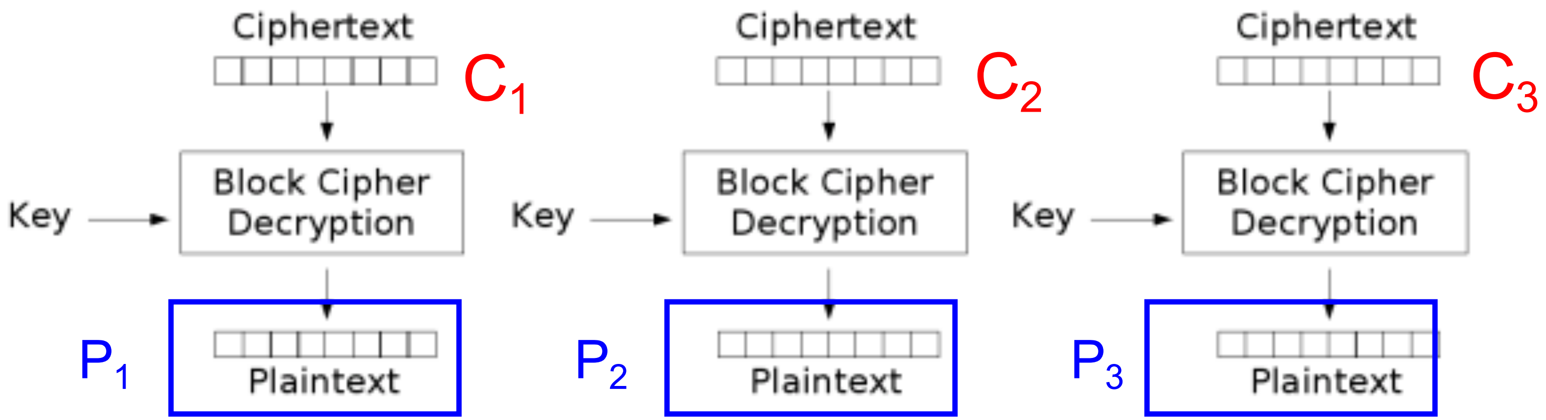
$$C_i = E_K(Pi)$$

Encryption



Electronic Codebook (ECB) mode encryption

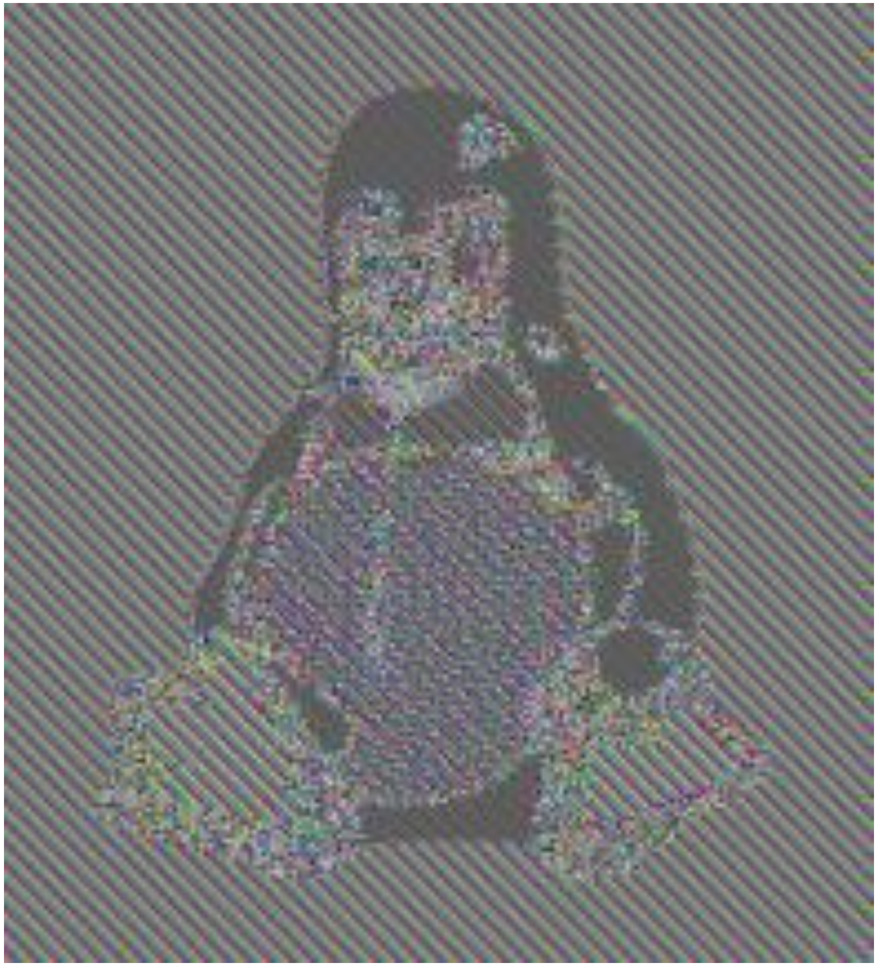
Decryption



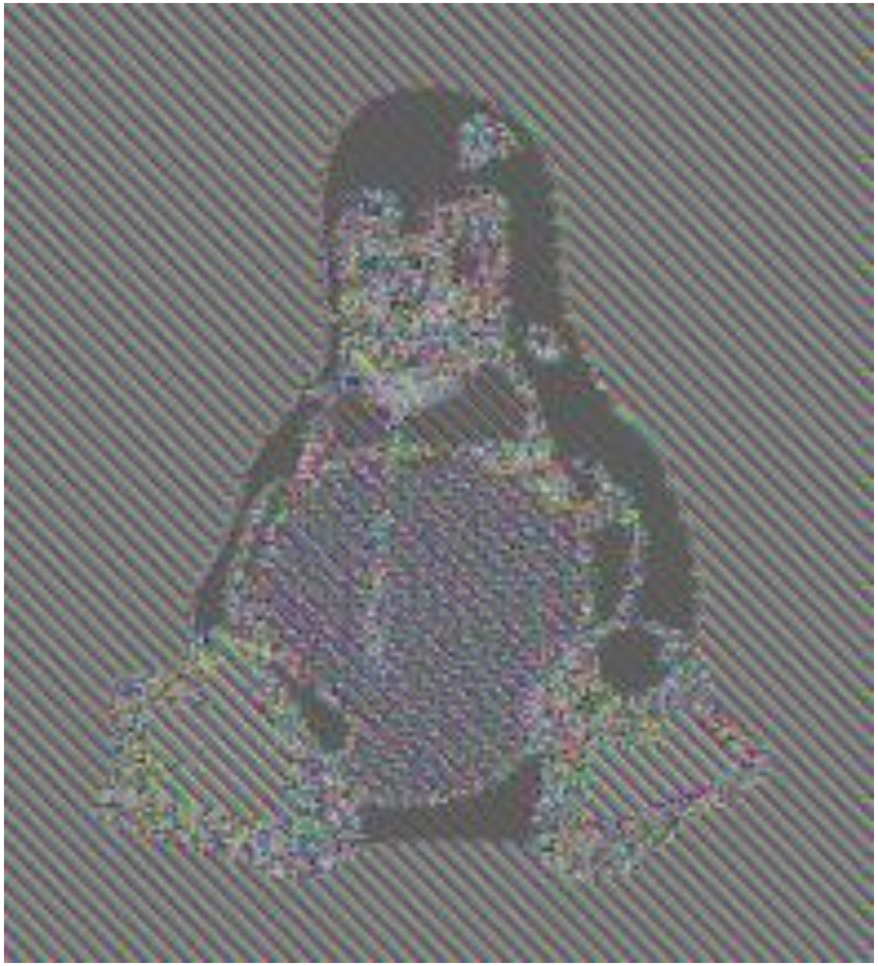
Electronic Codebook (ECB) mode decryption

What is the problem with ECB?

Original image

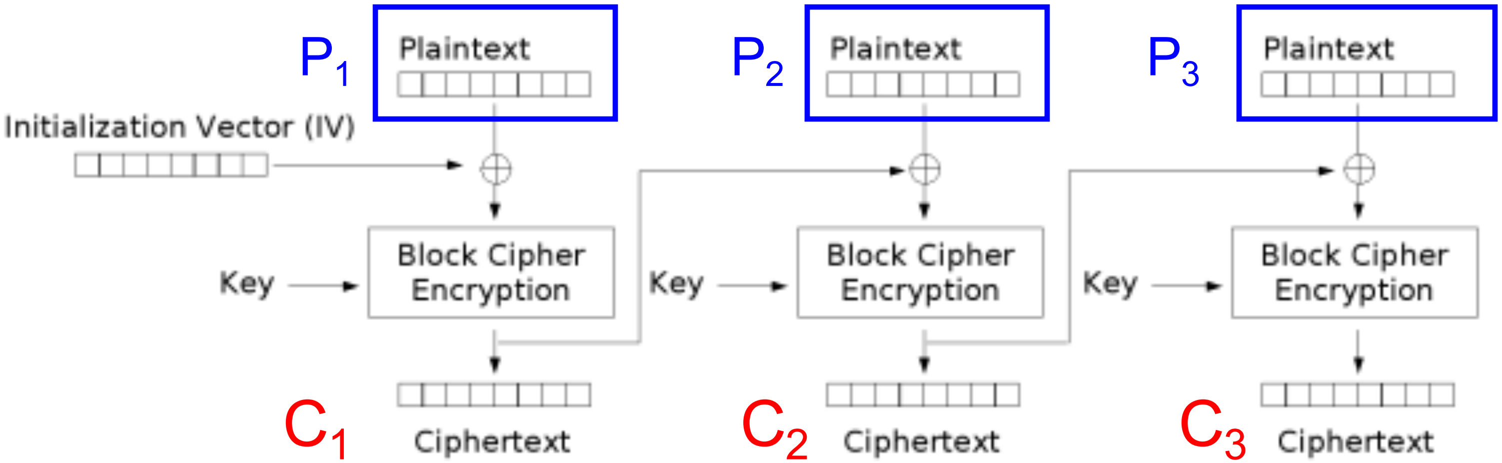


Encrypted with ECB



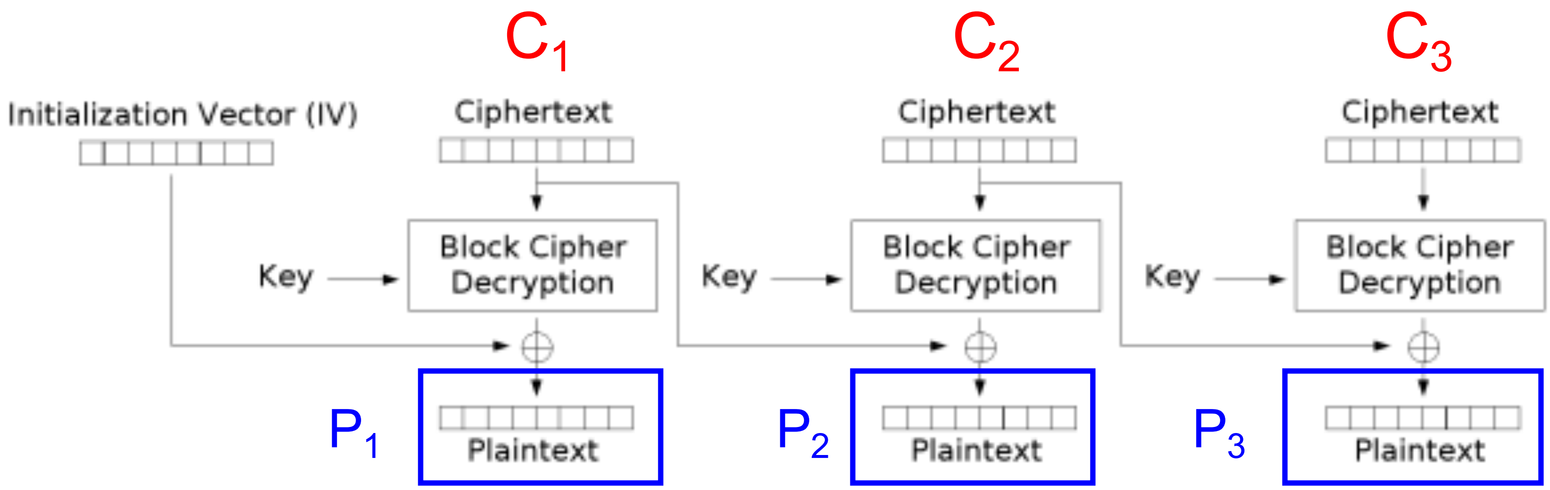
Later (identical) message again encrypted with ECB

CBC: Encryption



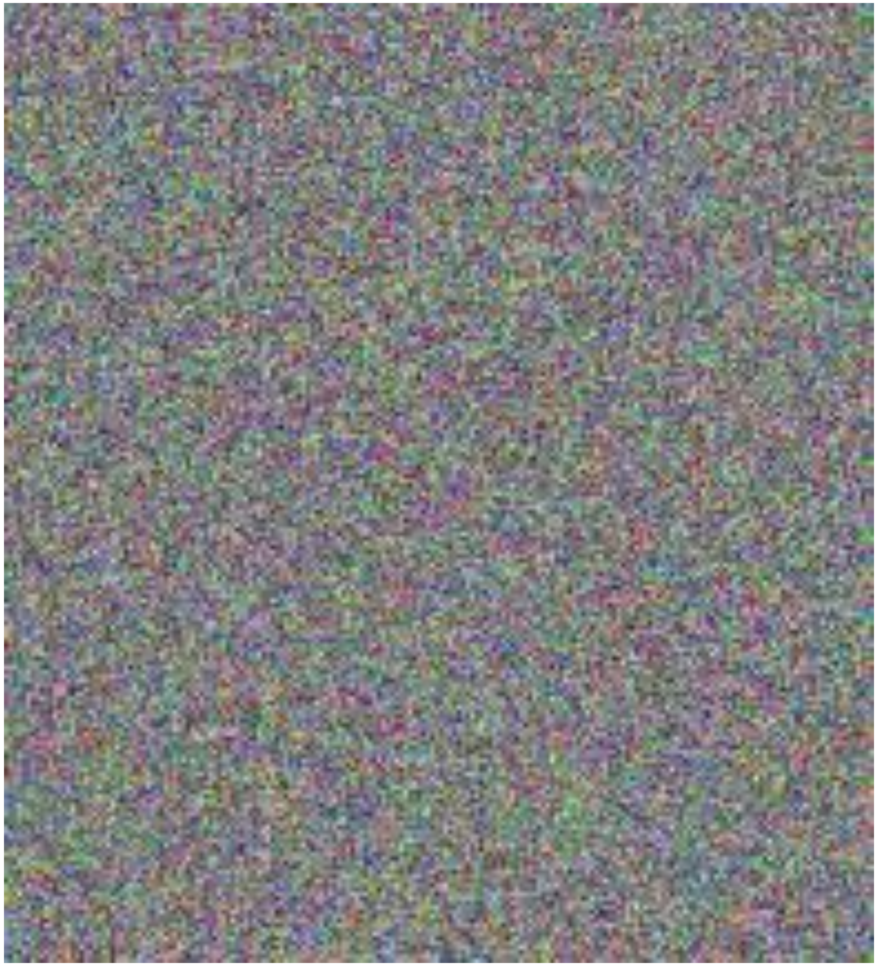
Cipher Block Chaining (CBC) mode encryption

CBC: Decryption



Cipher Block Chaining (CBC) mode decryption

Original image



Encrypted with CBC

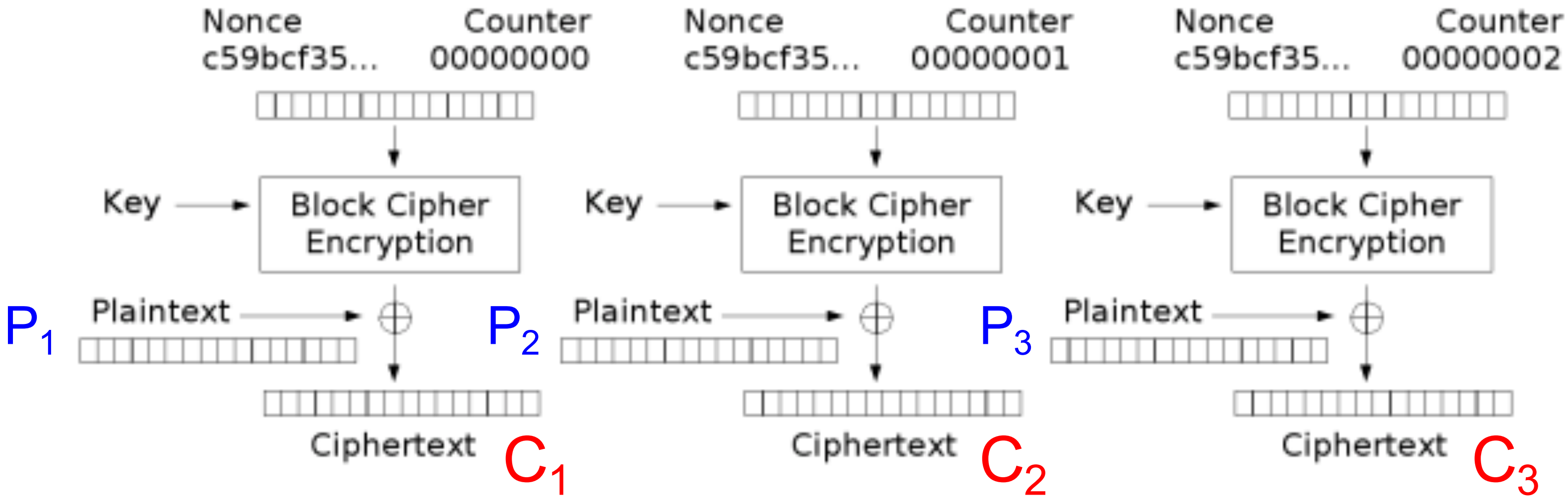
CBC

Popular, still widely used

Caveat: sequential encryption, hard to parallelize

CTR mode gaining popularity

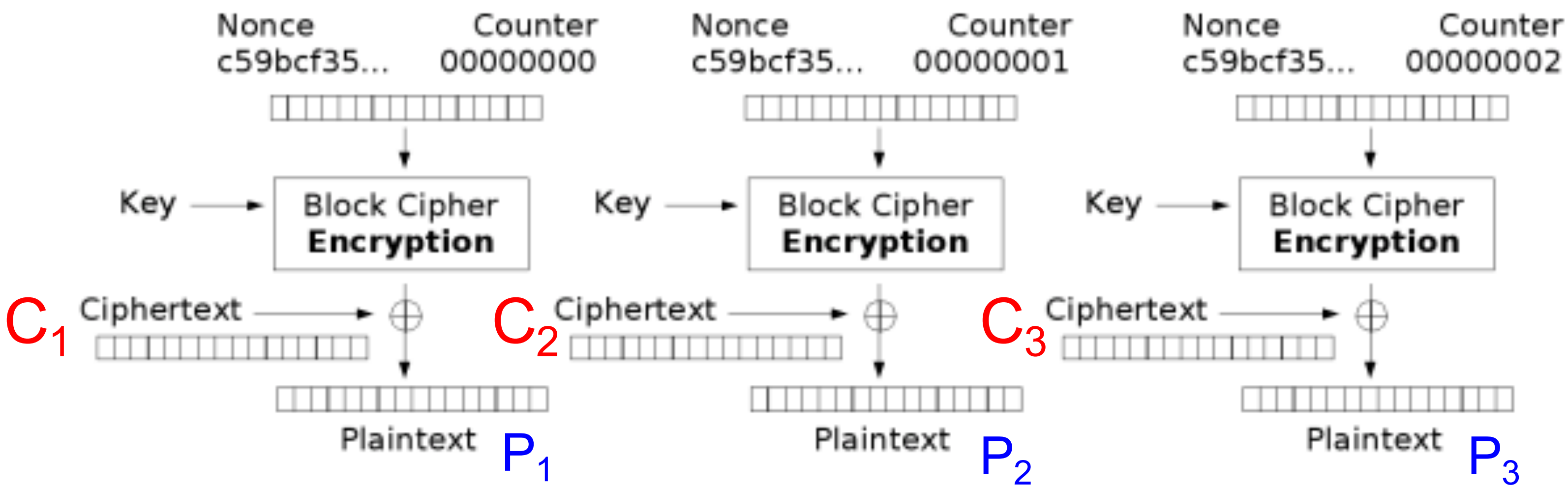
CTR: Encryption



Counter (CTR) mode encryption

(Nonce = Same as IV)

CTR: Decryption



Counter (CTR) mode decryption

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

CBC vs CTR

Security: If you ever reuse the same nonce, CBC might leak some information about the initial plaintext block. CTR will leak information about the entire message.

Speed: Both modes require the same amount of computation, but CTR is parallelizable

Summary

- Split message in blocks P_1, P_2, …
- Each block is a value which is substituted, like a codebook
- Each block is encoded independently of the other blocks

$$C_i = E_K(Pi)$$