Cryptography

Block Cipher Modes of Operation

Block Ciphers with Multiple Blocks

Electronic Code Book

Cipher Block Chaining Mode

Cipher Feedback Mode

Output Feedback Mode

Counter Mode

XTS-AES

# Block Cipher Modes of Operation

Cryptography

School of Engineering and Technology
CQUniversity Australia

Prepared by Steven Gordon on 23 Dec 2021,
modes.tex, r1949

# Contents

## Block Ciphers with Multiple Blocks

## Electronic Code Book

## Cipher Block Chaining Mode

## Cipher Feedback Mode

## Output Feedback Mode

## Counter Mode

## XTS-AES

# How Do Block Ciphers Encrypt Arbitrary Length Plaintext?

- Block cipher: operates on fixed length $b$-bit input to produce $b$-bit ciphertext
- What about encrypting plaintext longer than $b$ bits?
- Naive approach: Break plaintext into $b$-bit blocks (padding if necessary) and apply cipher on each block independently
  - ECB
- Security issues arise:
  - Repetitions of input plaintext blocks produces repetitions of output ciphertext blocks
  - Repetitions (patterns) in ciphertext are bad!
- Different *modes of operation* have been developed
- Tradeoffs between security, performance, error handling and additional features (e.g. include authentication)

We will not cover each mode of operation in detail, but rather present them so you are aware of some of the common modes. For more technical details of some of these modes of operation, including discussion of padding, error propagation and the use of initialisation vectors, see NIST Special Publication 800-38A Recommendations for Block Cipher Modes of Operation: Methods and Techniques. Additional (newer) modes of operation are in the NIST SP 800-38 series, such as 800-38C CCM, 800-38D GCM and 800-38E XTS-AES.

# Contents

Block Ciphers with Multiple Blocks

Electronic Code Book

Cipher Block Chaining Mode

Cipher Feedback Mode

Output Feedback Mode

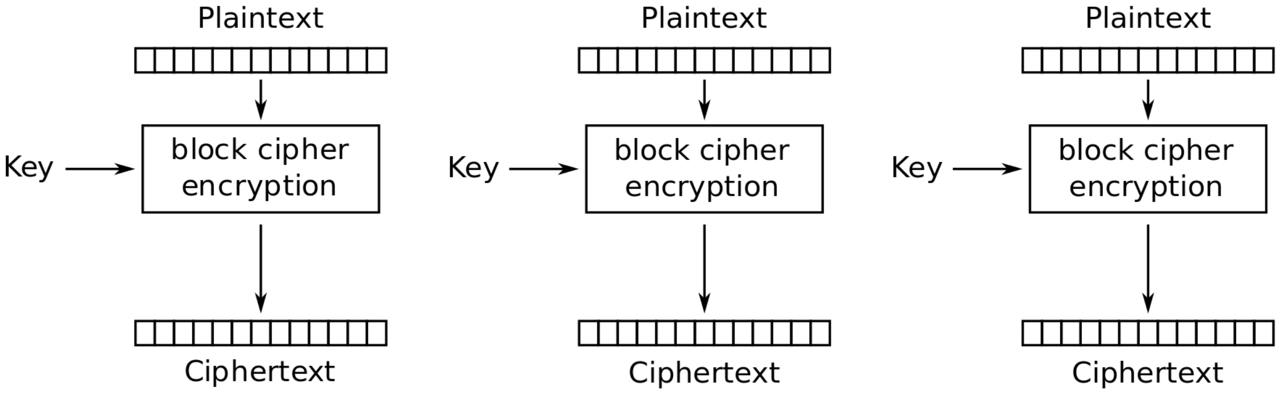
Counter Mode

XTS-AES

# ECB Summary

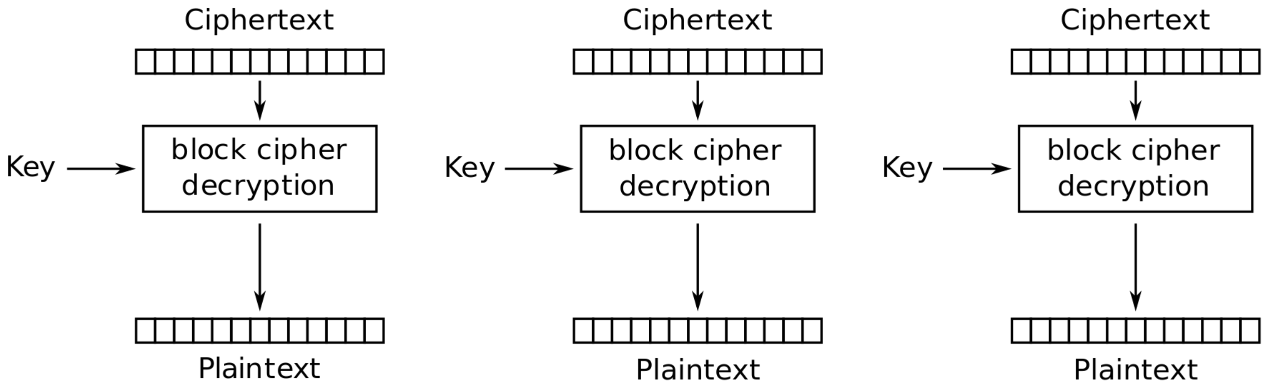
- Each block of 64 plaintext bits is encoded independently using same key
- Typical applications: secure transmission of single values (e.g. encryption key)
- Problem: with long message, repetition in plaintext may cause repetition in ciphertext

# ECB Encryption



Credit: Wikimedia `https://commons.wikimedia.org/wiki/File:ECB_encryption.svg`, public domain

# ECB Decryption



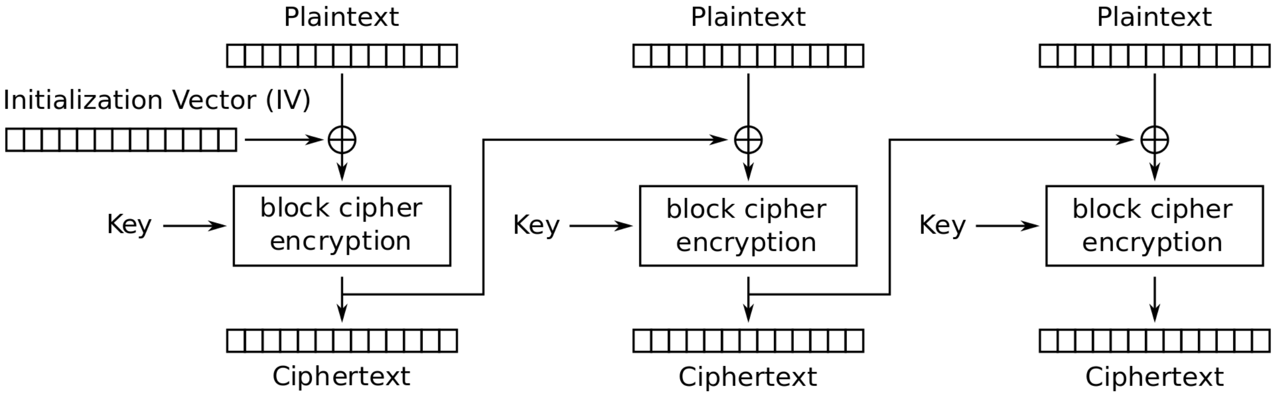
Credit: Wikimedia `https://commons.wikimedia.org/wiki/File:ECB_decryption.svg`, public domain

# Contents

# CBC Summary

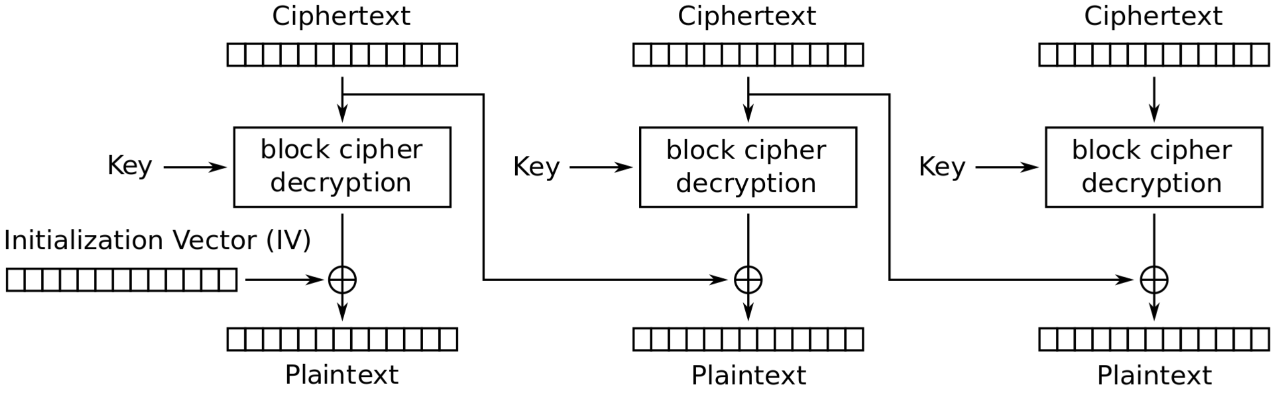
- Input to encryption algorithm is XOR of next 64-bits plaintext and preceding 64-bits ciphertext
- Typical applications: General-purpose block-oriented transmission; authentication
- Initialisation Vector (IV) must be known by sender/receiver, but secret from attacker

# CBC Encryption



Credit: Wikimedia https://commons.wikimedia.org/wiki/File:CBC_encryption.svg, public domain

# CBC Decryption



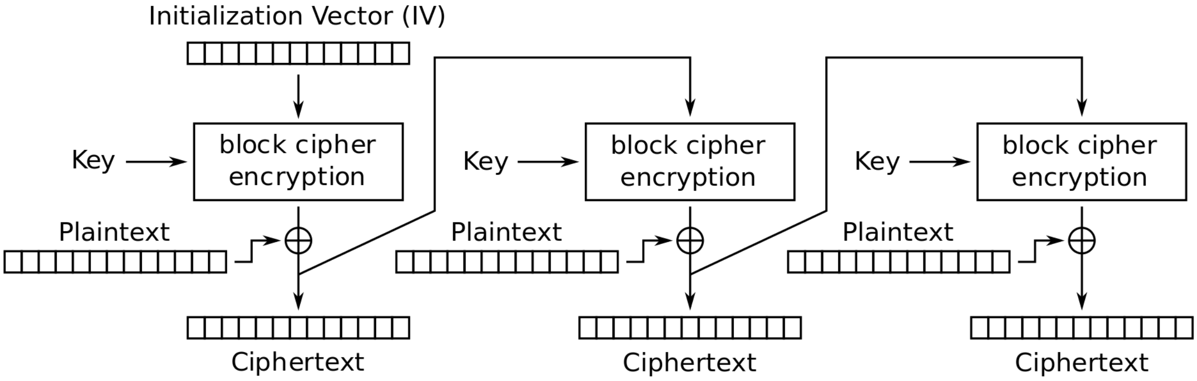
Credit: Wikimedia https://commons.wikimedia.org/wiki/File:CBC_decryption.svg, public domain

# Contents

# CFB Summary

- Converts block cipher into stream cipher
  - No need to pad message to integral number of blocks
  - Operate in real-time: each character encrypted and transmitted immediately
- Input processed *s* bits at a time
- Preceding ciphertext used as input to cipher to produce pseudo-random output
- XOR output with plaintext to produce ciphertext
- Typical applications: General-purpose stream-oriented transmission; authentication

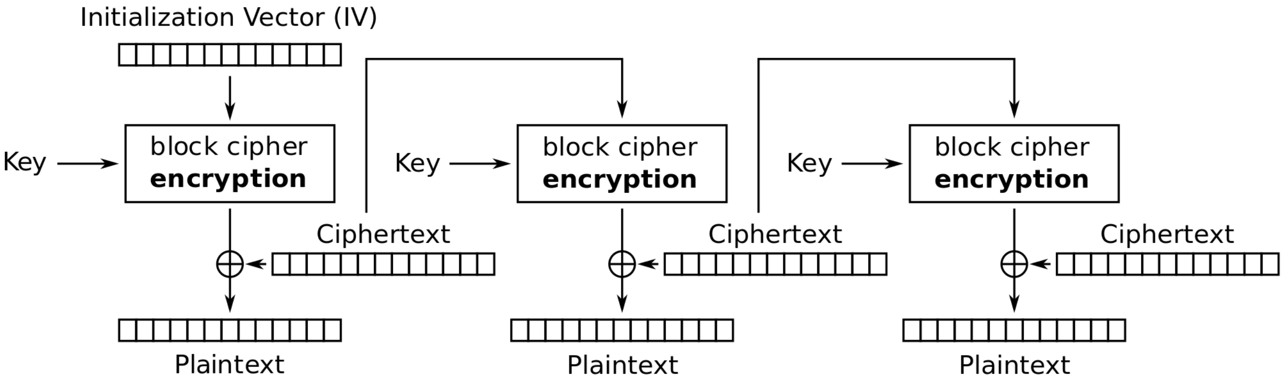
# CFB Encryption



Cipher Feedback (CFB) mode encryption

Credit: Wikimedia https://commons.wikimedia.org/wiki/File:CFB_encryption.svg, public domain

# CFB Decryption



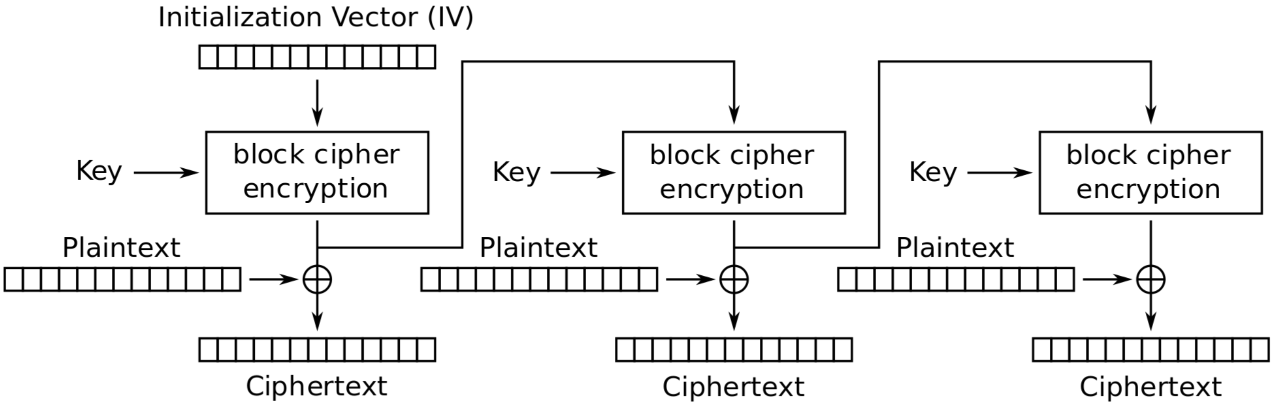
Credit: Wikimedia https://commons.wikimedia.org/wiki/File:CFB_decryption.svg, public domain

# Contents

# OFB Summary

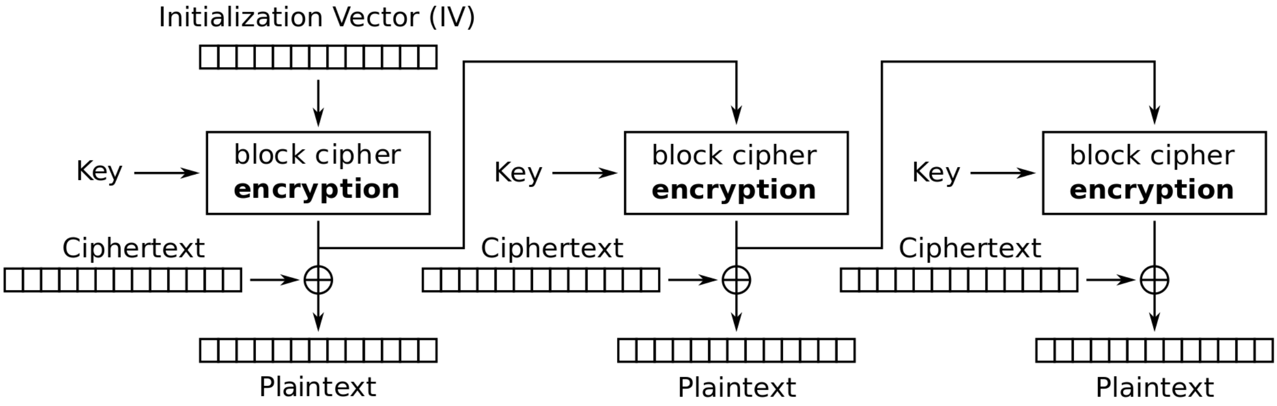
- Converts block cipher into stream cipher
- Similar to CFB, except input to encryption algorithm is preceding encryption output
- Typical applications: stream-oriented transmission over noisy channels (e.g. satellite communications)
- Advantage compared to OFB: bit errors do not propagate
- Disadvantage: more vulnerable to message stream modification attack

# OFB Encryption



Credit: Wikimedia https://commons.wikimedia.org/wiki/File:OFB_encryption.svg, public domain

# OFB Decryption



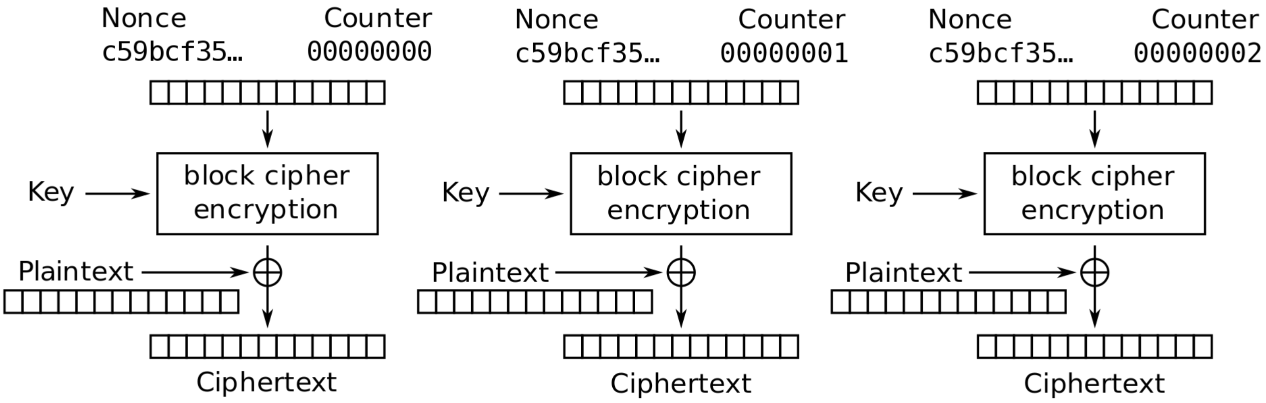
Credit: Wikimedia `https://commons.wikimedia.org/wiki/File:OFB_decryption.svg`, public domain

# Contents

# CTR Summary

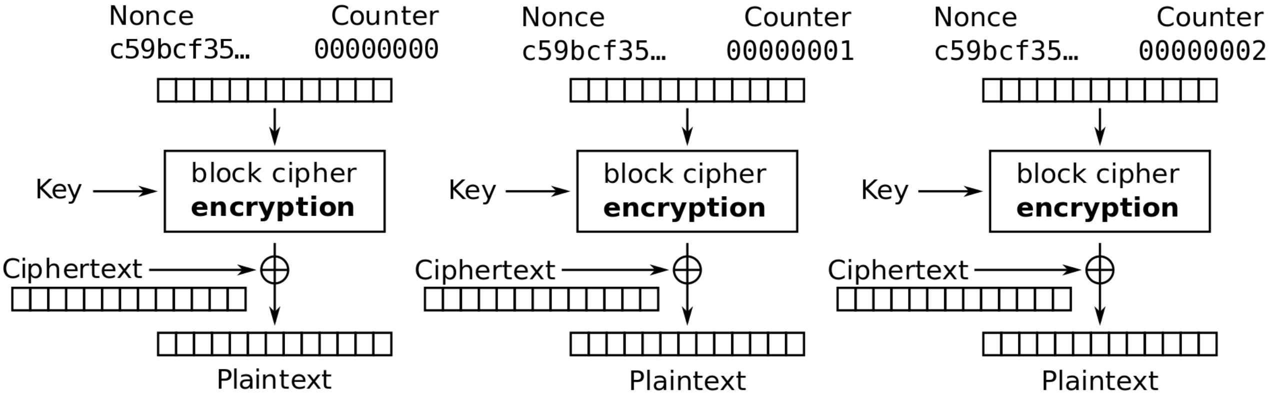
- Converts block cipher into stream cipher
- Each block of plaintext XORed with encrypted counter
- Typical applications: General-purpose block-oriented transmission; useful for high speed requirements
- Efficient hardware and software implementations
- Simple and secure

# CTR Encryption



Credit: Wikimedia https://commons.wikimedia.org/wiki/File:CTR_encryption_2.svg, public domain

# CTR Decryption



Credit: Wikimedia https://commons.wikimedia.org/wiki/File:CTR_decryption_2.svg, public domain

# Contents

# Encryption for Stored Data with XTS-AES

- XTS-AES designed for encrypting stored data (as opposed to transmitted data)
- Overcomes potential attack on CBC whereby one block of the ciphertext is changed by the attacker, and that change does not affect all other blocks
- See Stallings Chapter 6.7 for details and differences to transmitted data encryption