Block Cipher Modes of Operation

Electronic Code Book

Cipher Block
Chaining Mode

Mode Feedback

Output Feedback Mode

Counter Mode

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

ck Mode

ack Mode

r Mode

XTS-AES

Cipher Block Chaining Mo

Mode
Output Feedback

Mode Counter Mode



- ▶ 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)



Contents

Block Ciphers with Multiple Blocks

Electronic Code Book

Cipher Block Chaining Mode

ack Mode

eedback Mode

er Mode

XTS-AES

Electronic Code Book

Cipher Block Chaining Mod

Mode

Output Feedback Mode

Counter Mode
XTS-AES



Cipher Feedbac Mode Output Feedba Mode

Counter N

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

Block Cipher Modes of Operation

Electronic Code

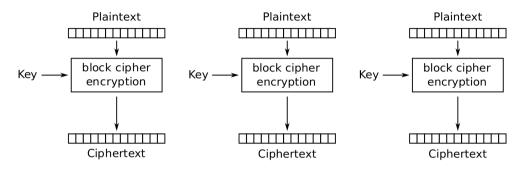
Cipher Feedback Mode Output Feedback

Mode

Counter Mode

XTS-AES

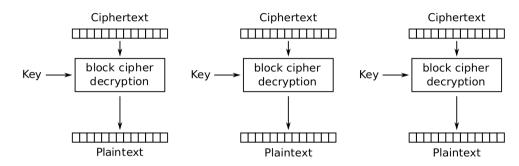
ECB Encryption



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

Electronic Code Book

ECB Decryption



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

ck Ciphers with Multiple Blocks

Electronic Code Book

Cipher Block Chaining Mode

Cipher Feedback Mode

edback Mode

er Mode

S-AES

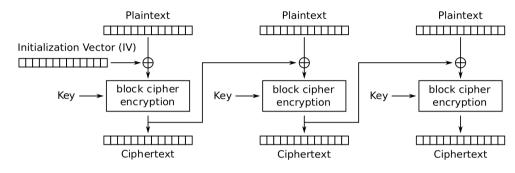
CBC Summary

- ▶ 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

Block Cipher Modes of Operation

Cipher Block Chaining Mode

CBC Encryption

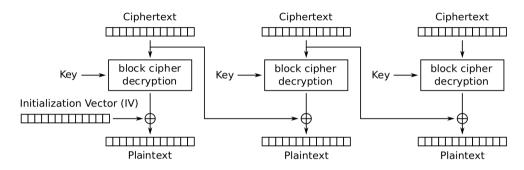


Credit: Wikimedia https://commons.wikimedia.org/wiki/File:CBC_encryption.svg, public domain

Block Cipher Modes of Operation

Cipher Block Chaining Mode

CBC Decryption



 $Credit: \ Wikimedia \ https://commons.wikimedia.org/wiki/File: CBC_decryption.svg, \ public \ domain \ properties of the properties of t$

Cipher Feedback Mode

Contents

Block Cinhers with Multiple Blocks

Cipiler Block Chairing Mode

Cipher Feedback Mode

Feedback Mode

er Mode

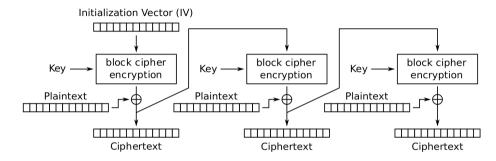
CFB Summary

- 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

Block Cipher Modes of Operation

Cipher Feedback Mode

CFB Encryption



Cipher Feedback (CFB) mode encryption

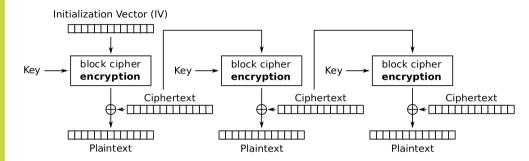
Credit: Wikimedia https://commons.wikimedia.org/wiki/File:CFB_encryption.svg, public domain

Block Cipher Modes of Operation

Cipher Feedback

Mode

CFB Decryption



Credit: Wikimedia https://commons.wikimedia.org/wiki/File:CFB decryption.svg.public domain

Contents

Plack Ciphors with Multiple Placks

Ciphers vole Blocks

Block Cipners with Multiple Blocks

Electronic Coc Book Electronic Code Book

Cipher Block Chaining Mo

Cipher Block Chaining Mode

Cipher Feedback Mode Output Feedback

Cipher Feedback Mode

Counter Mode

Mode

Output Feedback Mode

er Mod

Operation

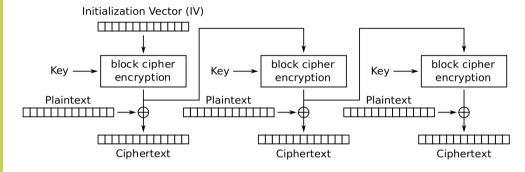
OFB Summary

- 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

Block Cipher Modes of Operation

Output Feedback Mode

OFB Encryption

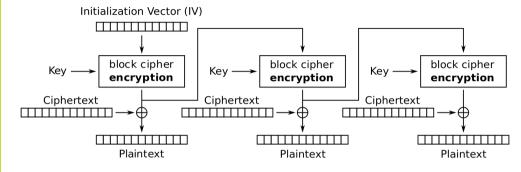


Credit: Wikimedia https://commons.wikimedia.org/wiki/File:OFB_encryption.svg, public domain

Block Cipher Modes of Operation

Output Feedback Mode

OFB Decryption



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

Contents

Block Ciphers with Multiple Blocks

Electronic code Boot

Cipner Block Chaining Wode

Cipher Feedback Mode

out Feedback Mode

Counter Mode

TS-AES

Counter Mode
XTS-AES

CTR Summary

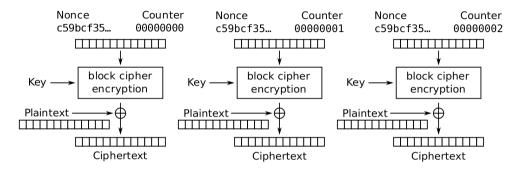
- ► Converts block cipher into stream cipher
- ► Each block of plaintext XORed with encrypted counter
- ► Typical applications: General-purpose block-oriented transmission; useful for high speed requirements
- Efficient hardware and software implementations
- Simple and secure

Counter Mode

Block Cipher Modes of Operation

Counter Mode

CTR Encryption

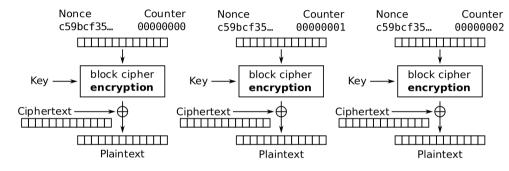


Credit: Wikimedia https://commons.wikimedia.org/wiki/File:CTR_encryption_2.svg, public domain

Block Cipher Modes of Operation

Counter Mode

CTR Decryption



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

Cryptography Block Cipher Modes of Operation

XTS-AES

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