CSS322

Block Cipher Operation

Modes

ECB

CBO

CFE

OF

CTF

Feedbac

XTS-AES

Block Cipher Operation

CSS322: Security and Cryptography

Sirindhorn International Institute of Technology
Thammasat University

Prepared by Steven Gordon on 29 December 2011 CSS322Y11S2L04, Steve/Courses/2011/S2/CSS322/Lectures/modes.tex, r2070

Contents

Modes

ECI

СВО

CEI

СТІ

г...

YTS AF

Modes of Operation

Electronic Code Book

Cipher Block Chaining Mode

Cipher Feedback Mode

Output Feedback Mode

Counter Mode

Feedback Characteristics of Modes

Modes

ECB

CB(

CF

СТ

Feedbar

YTS AEG

Modes of Operation

- ▶ Block cipher: operates on fixed length *b*-bit input to produce *b*-bit ciphertext
- ▶ What about encrypting plaintext longer than *b* bits?
- Break plaintext into b-bit blocks (padding if necessary) and apply cipher on each block
- Security issues arise: different modes of operation have been developed

Contents

Modes

ECB

СВО

CFI

СТІ

CII

recubac

XTS-AES

Modes of Operation

Electronic Code Book

Cipher Block Chaining Mode

Cipher Feedback Mode

Output Feedback Mode

Counter Mode

Feedback Characteristics of Modes

CRI

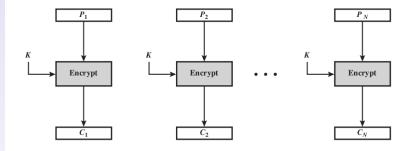
CFF

CIF

Feedbad

XTS-AF

ECB Encryption



IVIOU

ECB

CRI

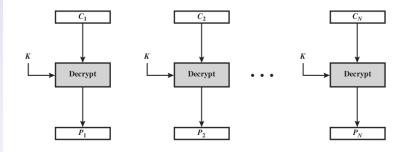
CEF

CIII

Feedbad

XTS-AES

ECB Decryption



CFI

СТ

Feedbac

XTS-AE9

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

CBC

Contents

Cipher Block Chaining Mode

СВС

CEE

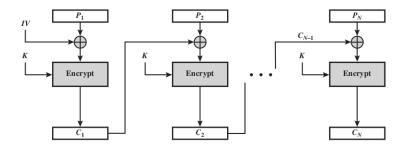
CIL

CTR

Feedbac

XTS-AF9

CBC Encryption



СВС

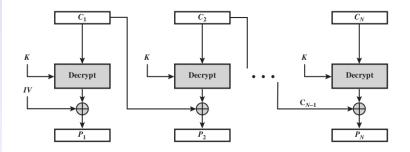
CER

CIF

Feedbac

XTS-AF

CBC Decryption



Mode

ECE

CBC

CF

Ο.

CT

Candles

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

Contents

Mode

ECE

CBO

CFB

UFI

СТІ

reedbac

XTS-AE

Modes of Operation

Electronic Code Book

Cipher Block Chaining Mode

Cipher Feedback Mode

Output Feedback Mode

Counter Mode

Feedback Characteristics of Modes

Modes

LCD

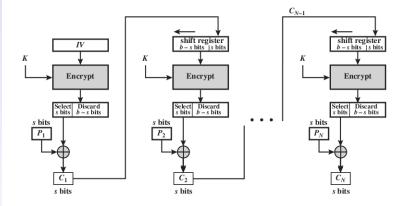
CFB

СТВ

Feedbac

YTS AF





Block Cipher Operation

Modes

ECD

CD.

CFB

CFE

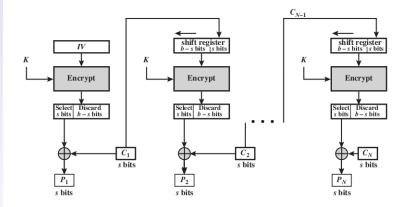
OF

CTE

Feedbac

XTS-AF9

CFB Decryption



ECE

CB(

CFB

OF

CTI

Feedbac

XTS_AF

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 pseudorandom output
- ▶ XOR output with plaintext to produce ciphertext
- ► Typical applications: General-purpose stream-oriented transmission; authentication

Modes

ECF

CBO

CFI

OFB

CTF

Feedbac

XTS-AE

Modes of Operation

Electronic Code Book

Cipher Block Chaining Mode

Cipher Feedback Mode

Output Feedback Mode

Counter Mode

Feedback Characteristics of Modes

Block Cipher Operation

Mode

ECD

CDA

CEL

CFE

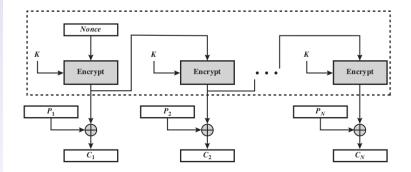
OFB

CTF

Feedbac

XTS-AF

OFB Encryption



Block Cipher Operation

Modes

ECP

CD

CEL

CFE

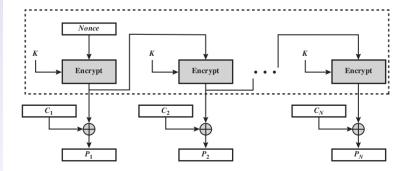
OFB

CTR

Feedbac

XTS-AF

OFB Decryption



Mode

ECD

CBO

CFI

OFB

СТІ

Feedba

XTS-AF

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

Modes of Operation

Electronic Code Book

Cipher Block Chaining Mode

Cipher Feedback Mode

Output Feedback Mode

Counter Mode

Feedback Characteristics of Modes

Block Cipher Operation

Modes

ECD

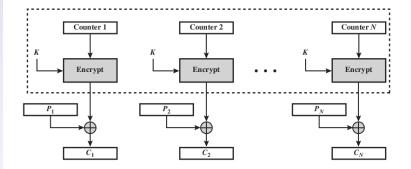
CIL

CTR

Feedbad

XTS-AF

CTR Encryption



ECR

CRO

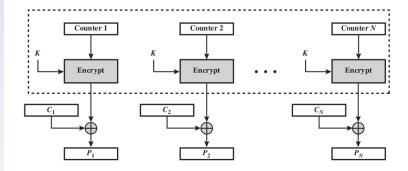
CFF

CTR

геепрас

XTS-AES

CTR Decryption



CBO

CFI

CTR

_ ..

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

Mode

EC

CBO

CEI

CF

- - -

CTF

Feedback

XTS-AES

Contents

Modes of Operation

Electronic Code Book

Cipher Block Chaining Mode

Cipher Feedback Mode

Output Feedback Mode

Counter Mode

Feedback Characteristics of Modes

ECD

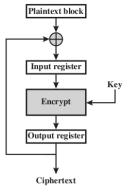
CDO

CEE

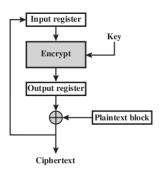
Feedback

XTS-AES

Feedback: CBC and CFB



(a) Cipher block chaining (CBC) mode



(b) Cipher feedback (CFB) mode

ECR

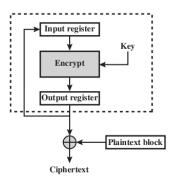
CP

CEE

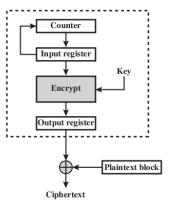
Feedback

XTS-AES

Feedback: OFB and CTR



(c) Output feedback (OFB) mode



(d) Counter (CTR) mode

Contents

XTS-AES

CD

CEE

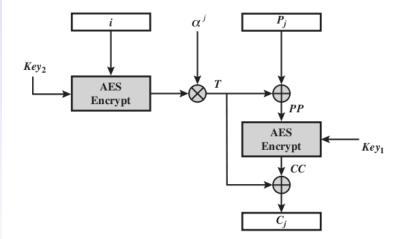
CIL

CIR

Feedbac

XTS-AES

XTS-AES Encryption of Single Block



ECB

CBO

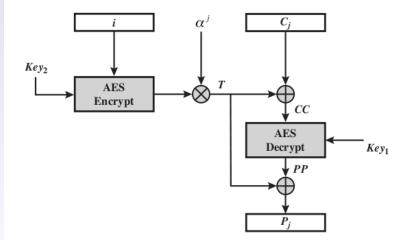
CFE

СТР

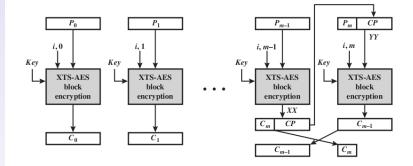
- 0

XTS-AES

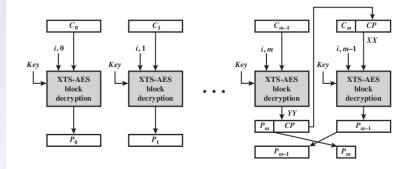
XTS-AES Decryption of Single Block











Mode

ECE

CD

CE

__

СТІ

Ecodbac

XTS-AES

Encryption for Stored Data

- XTS-AES designed for encrypting stored data (as opposed to transmitted data)
- ► See Chapter 6.7 for details and differences to transmitted data encryption