Block Cipher Operation

CSS322: Security and Cryptography

Sirindhorn International Institute of Technology
Thammasat University

Prepared by Steven Gordon on 15 November 2010
CSS322Y10S2L06, Steve/Courses/CSS322/Lectures/modes.tex, r1517

Contents

- Modes of Operation
- Electronic Code Book
- Cipher Block Chaining Mode
- Cipher Feedback Mode
- Output Feedback Mode
- Counter Mode
- Feedback Characteristics of Modes
- XTS-AES

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 of Operation

Electronic Code Book

Cipher Block Chaining Mode

Cipher Feedback Mode

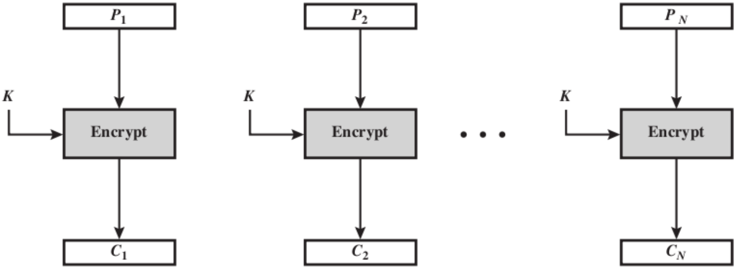
Output Feedback Mode

Counter Mode

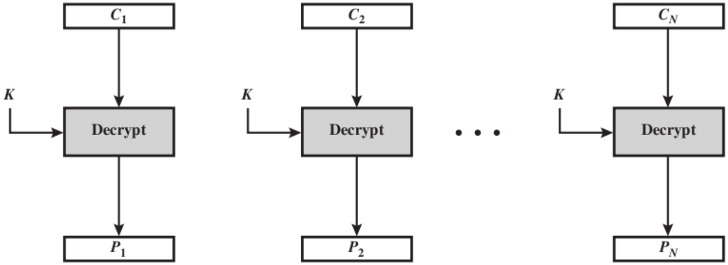
Feedback Characteristics of Modes

XTS-AES

ECB Encryption



ECB Decryption



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

Contents

Modes of Operation

Electronic Code Book

Cipher Block Chaining Mode

Cipher Feedback Mode

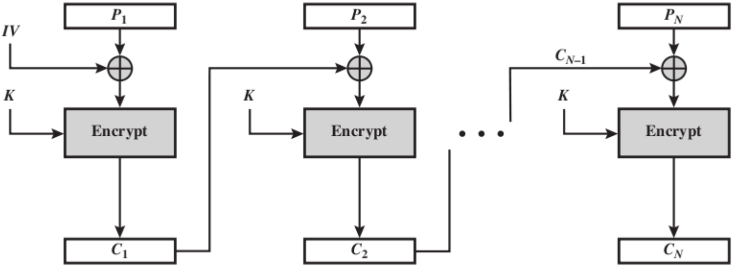
Output Feedback Mode

Counter Mode

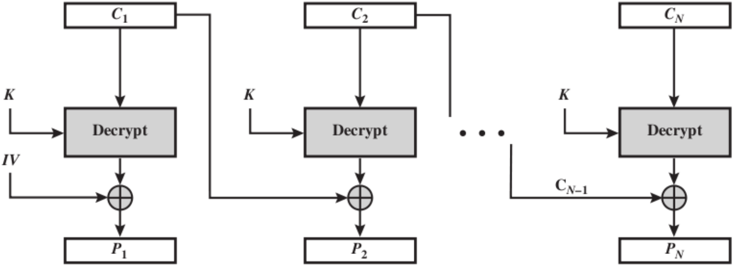
Feedback Characteristics of Modes

XTS-AES

CBC Encryption



CBC Decryption



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

Modes of Operation

Electronic Code Book

Cipher Block Chaining Mode

Cipher Feedback Mode

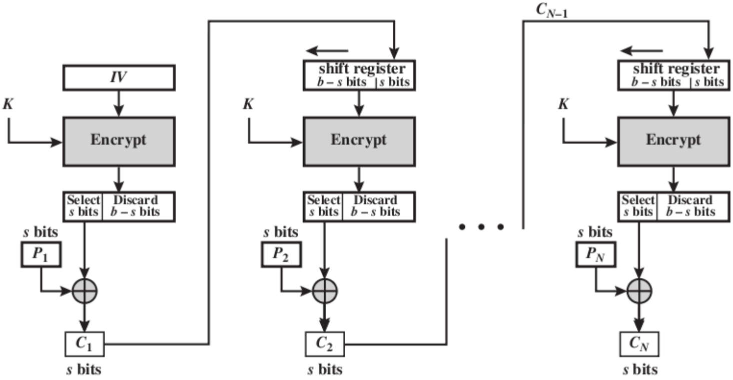
Output Feedback Mode

Counter Mode

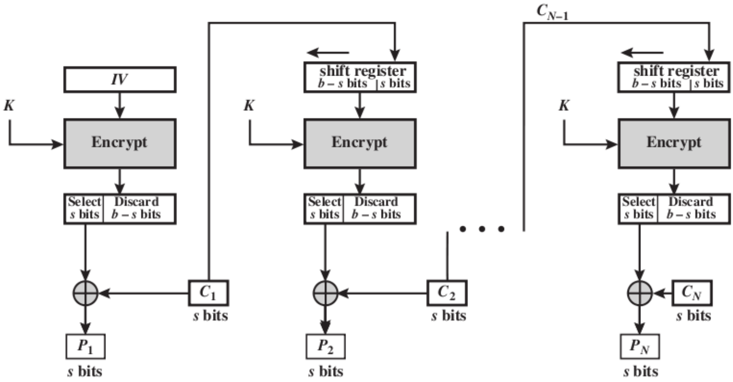
Feedback Characteristics of Modes

XTS-AES

CFB Encryption



CFB Decryption



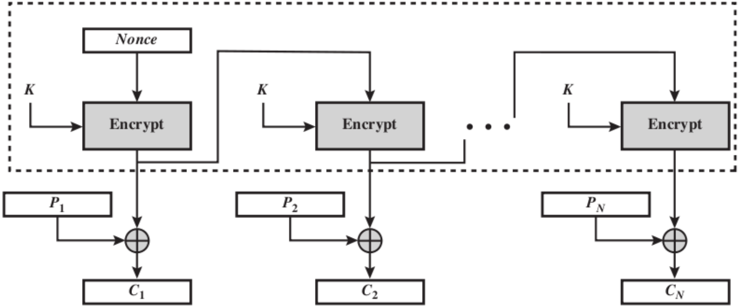
CFB Summary

- 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

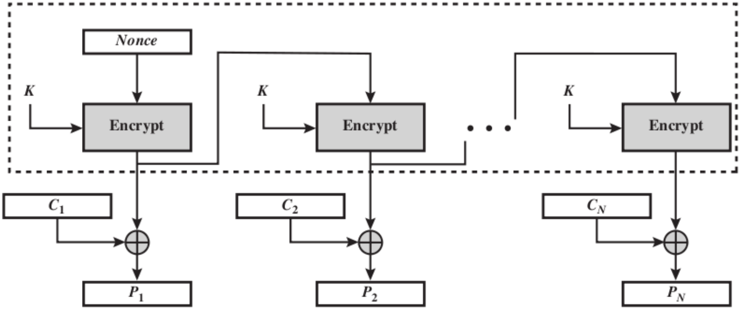
Contents

- Modes of Operation
- Electronic Code Book
- Cipher Block Chaining Mode
- Cipher Feedback Mode
- Output Feedback Mode
- Counter Mode
- Feedback Characteristics of Modes
- XTS-AES

OFB Encryption



OFB Decryption

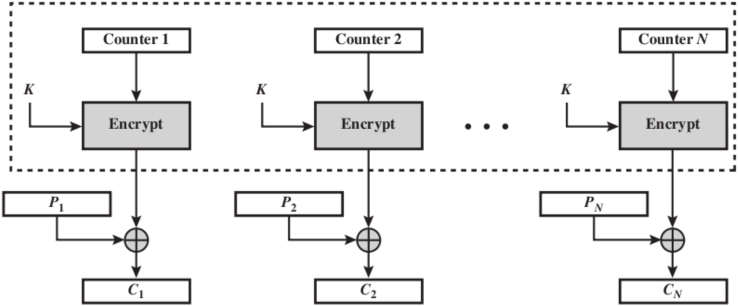


OFB Summary

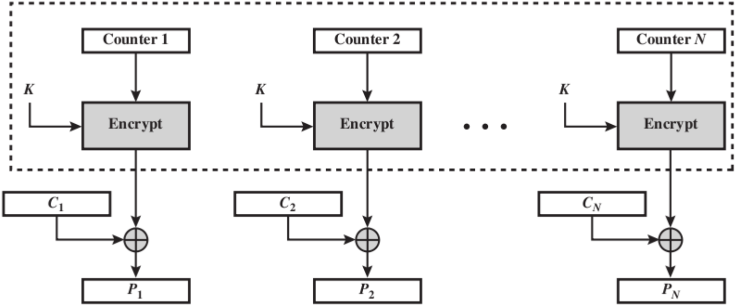
- Converts block cipher into stream cipher
- Similar to CFB, except input to encryption algorithm is preceding encryption output
- Typical applications: stream-oriented transmission over noisy channels (e.g. satellite communications)
- Advantage compared to OFB: bit errors do not propagate
- Disadvantage: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

Contents

CTR Encryption



CTR Decryption



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

Contents

Modes of Operation

Electronic Code Book

Cipher Block Chaining Mode

Cipher Feedback Mode

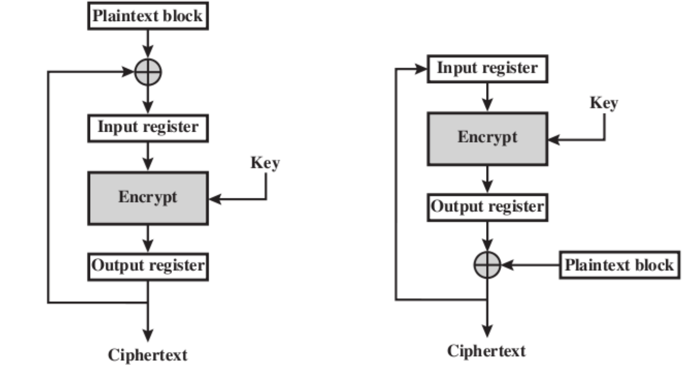
Output Feedback Mode

Counter Mode

Feedback Characteristics of Modes

XTS-AES

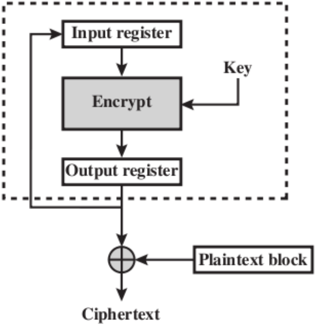
Feedback: CBC and CFB



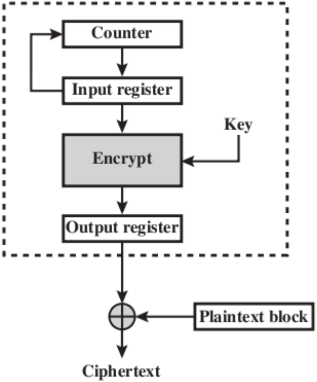
(a) Cipher block chaining (CBC) mode

(b) Cipher feedback (CFB) mode

Feedback: OFB and CTR



(c) Output feedback (OFB) mode



(d) Counter (CTR) mode

Contents

Modes of Operation

Electronic Code Book

Cipher Block Chaining Mode

Cipher Feedback Mode

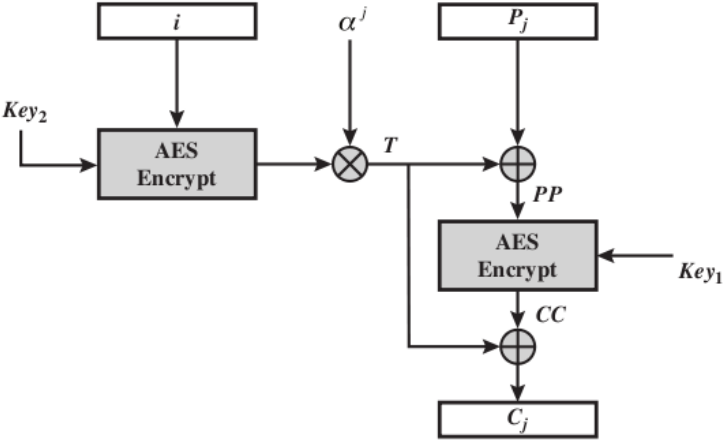
Output Feedback Mode

Counter Mode

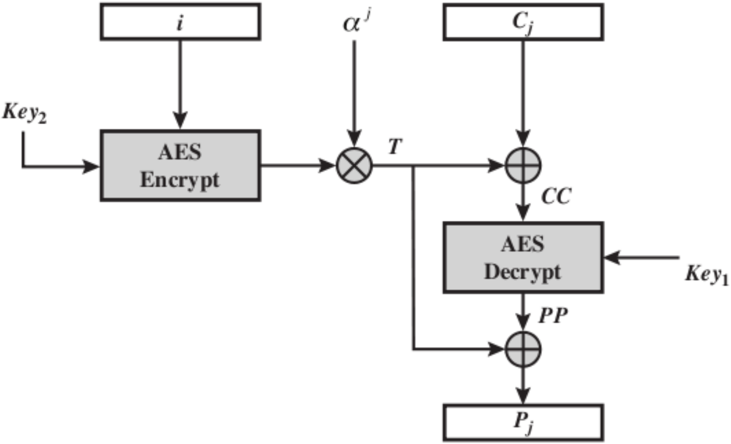
Feedback Characteristics of Modes

XTS-AES

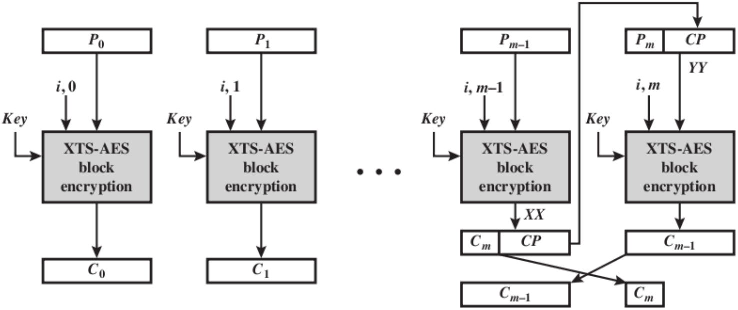
XTS-AES Encryption of Single Block



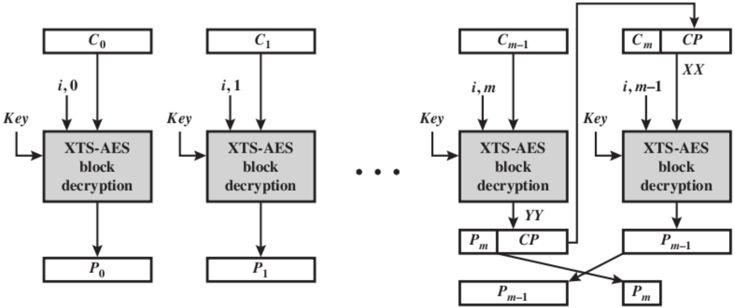
XTS-AES Decryption of Single Block



XTS-AES Encryption



XTS-AES Decryption



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