“Introduction to Block Ciphers“

Seminar
“Block Cipher Cryptanalysis“
Summer 2011

Tim Syben

18.04.2011
Agenda

• Block Cipher

• Stream Cipher

• Modes of Operation
  • Electronic Code Book (ECB)
  • Cipher Block Chaining (CBC)
  • Output Feedback Mode (OFB)
  • Cipher Feedback Mode (CFB)
  • Counter Mode (CTR)

• Summery

• Conclusion
Block Cipher

• Symmetric key cipher

![Diagram of Block Cipher]

• Operates on fixed-length groups of bits (block)

• Typical block size: 64 bit or 128 bit

Symmetric encryption [can06]
Anatomy of a Block Cipher

General approach of most block cipher designs:

• Round function
  • Repeated several times (rounds)
    • First round takes n-bit plaintext as input
    • Last round outputs n-bit cipher text
  • Each round depends on a roundkey
    • Derived from k-bit secret key (key schedule)
    • Has to be bijective

Two Examples

1. Feistel ciphers
2. SP Networks
Feistel Cipher vs. SP Network

Feistel Cipher

SP Network

Feistel cipher and SP network [can06]
Feistel Cipher

Examples of Block Ciphers using a Feistel structure:

• DES
  • Published 1977
  • Designed by IBM

• Blowfish
  • Published 1992
  • Designed by Bruce Schneier

• RC5
  • Published 1994
  • Designed by Ron Rivest
Introduction to Block Ciphers

Examples of Block Ciphers using a SP Network structure:

- AES (Rijndael)
  - Published 1998
  - Designed by Vincent Rijmen and Joan Daemen

- CAST-128
  - Published 1996
  - Designed by Carlisle Adams and Stafford Tavares

- IDEA
  - Published 1991
  - Designed by Xuejia Lai and James Massey
Overview

• Block Cipher ✓

• Stream Cipher ←

• Modes of Operation
  • Electronic Code Book (ECB)
  • Cipher Block Chaining (CBC)
  • Output Feedback Mode (OFB)
  • Cipher Feedback Mode (CFB)
  • Counter Mode (CTR)

• Summery
• Conclusion
Stream Cipher

- Symmetric key cipher
- Input is a continuous stream of plaintext
- Single bit will be encrypted one by one

Stream encryption [can06]
Stream Cipher

Examples:

- One Time Pad
  - 1917

- A5/1
  - Developed 1987
  - Used in the GSM standard

Stream encryption [can06]
Block Cipher vs. Stream Cipher

Block encryption (ECB) [can06]

Stream encryption  [can06]
Overview

• Block Cipher ✓

• Stream Cipher ✓

• Modes of Operation ←
  • Electronic Code Book (ECB)
  • Cipher Block Chaining (CBC)
  • Output Feedback Mode (OFB)
  • Cipher Feedback Mode (CFB)
  • Counter Mode (CTR)

• Summery

• Conclusion
Modes of Operation

• Defines a way how to encrypt arbitrary-length messages using a block cipher
  • Devide message into blocks – encrypt each of them independently

• Last block has to be extended to match block size
  • Padding

• Some modes need an additional input value
  • Initialisation vector
Padding

• Various padding schemes
  
  • Zero Padding
    
    ... | 1100 0110 1001 0101 1011 0101 0000 0000 |
    
    ... | 1A 45 AE 56 9B DD 5D FF | 26 14 FC FC 00 00 00 00 |
  
  • Ansi X.923
    
    ... | 1A 45 AE 56 9B DD 5D FF | 26 14 FC FC 00 00 00 04 |
  
  • ISO 11026
    
    ... | 1A 45 AE 56 9B DD 5D FF | 26 14 FC FC 81 A6 23 04 |
Padding

• Good padding scheme
  • Generate random bits/bytes
  • End of message is clear

• Choice of padding scheme affects the security
Initialization Vector

• Fixed-size input value
• Requires to be random or pseudorandom
• A good initialization vector should be
  • Unique
  • Unpredictable
Overview

- Block Cipher ✓
- Stream Cipher ✓

- Modes of Operation
  - Electronic Code Book (ECB)
  - Cipher Block Chaining (CBC)
  - Output Feedback Mode (OFB)
  - Cipher Feedback Mode (CFB)
  - Counter Mode (CTR)

- Summery
- Conclusion
Electronic Code Book (ECB)
Electronic Code Book (ECB)

- **Advantages**
  - En-/decryption of each block could be parallelized

- **Disadvantages**
  - Two blocks with identical plaintext produces identical ciphertext
  - Bit error in one block affect the whole block
  - Plaintext patterns are still visible after encryption
Electronic Code Book (ECB)
Electronic Code Book (ECB)

Summary

• Most naive mode of operation
• En-/decryption of a block does not depend on the successor or predecessor
• Not suitable for encryption of messages bigger than one block
Overview

• Block Cipher ✓

• Stream Cipher ✓

• Modes of Operation
  • Electronic Code Book (ECB) ✓
  • Cipher Block Chaining (CBC) ←
  • Output Feedback Mode (OFB)
  • Cipher Feedback Mode (CFB)
  • Counter Mode (CTR)

• Summery

• Conclusion
Cipher Block Chaining (CBC)
Cipher Block Chaining (CBC)

- Advantages
  - Decryption could be parallelized
  - Different initialization vectors
    - Different ciphertext
  - Plaintext patterns are blurred

- Disadvantages
  - Encryption has to be done sequential
  - Bit error in one block affects two blocks
Cipher Block Chaining (CBC)

Summary

• CBC-Mode was invented to eliminate the disadvantages of the ECB-Mode
  • Equal messages produce different cipher text by using different initialization vectors
• Encryption of a plaintext block depends on this block and its predecessor
Overview

• Block Cipher ✓

• Stream Cipher ✓

• Modes of Operation
  • Electronic Code Book (ECB) ✓
  • Cipher Block Chaining (CBC) ✓
  • Output Feedback Mode (OFB) ←
  • Cipher Feedback Mode (CFB)
  • Counter Mode (CTR)

• Summery

• Conclusion
Output Feedback Mode (OFB)
Output Feedback Mode (OFB)

• Advantages
  • Keystream can be pre-computed
  • No padding
  • Bit error only affect one bit

• Disadvantages
  • Keystream computation cannot be parallelized
  • Reusing of key an initialization vector is dangerous
  • Bit-flipping attacks are easy
Output Feedback Mode (OFB)

Summary

• Combines a block cipher with a stream cipher

• Needs an initialization vector

• Uses same function for encryption and decryption
  • Makes it possible to choose the faster function
  • Makes it possible to use one-way-functions

• Pre-calculation possible
Overview

• Block Cipher ✓

• Stream Cipher ✓

• Modes of Operation
  • Electronic Code Book (ECB) ✓
  • Cipher Block Chaining (CBC) ✓
  • Output Feedback Mode (OFB) ✓
  • Cipher Feedback Mode (CFB) ←
  • Counter Mode (CTR)

• Summery

• Conclusion
Cipher Feedback Mode (CFB)
Cipher Feedback Mode (CFB)

- **Advantages**
  - No padding
  - Bit error only affects one bit
  - Decryption can be parallelized

- **Disadvantages**
  - Bit-flipping attacks are easy
  - Encryption cannot be parallelized
  - No pre-computation of the keystream
Cipher Feedback Mode (CFB)

Summary

• Similar to OFB-Mode

• Combines a block cipher with a stream cipher

• Needs an initialization vector

• Uses same function for encryption and decryption
  • Makes it possible to choose the faster function
  • Makes it possible to use one-way-functions

• Encryption of a plaintext block depends on its predecessors
Overview

• Block Cipher ✓

• Stream Cipher ✓

• Modes of Operation
  • Electronic Code Book (ECB) ✓
  • Cipher Block Chaining (CBC) ✓
  • Output Feedback Mode (OFB) ✓
  • Cipher Feedback Mode (CFB) ✓
  • Counter Mode (CTR) ←

• Summery

• Conclusion
Counter Mode (CTR)

Counter (CTR) mode encryption

Counter (CTR) mode decryption

Pictures from Wikimedia Commons
Counter Mode (CTR)

- **Advantages**
  - En-/decryption of each block could be parallelized
  - No padding
  - Keystream can be pre-computed
    - Can be done in parallel

- **Disadvantages**
  - Bit-flipping attacks are easy
  - Reusing of key and nonce/counter is dangerous
Counter Mode (CTR)

Summary

• Combines a block cipher with a stream cipher

• Just as in the ECB mode en-/decryption of a block does not depend on the successor or predecessor
Overview

• Block Cipher ✓
• Stream Cipher ✓
• Modes of Operation ✓
  • Electronic Code Book (ECB) ✓
  • Cipher Block Chaining (CBC) ✓
  • Output Feedback Mode (OFB) ✓
  • Cipher Feedback Mode (CFB) ✓
  • Counter Mode (CTR) ✓
• Summery ←
• Conclusion
Summary

Now, we should all be able to give a short answer to these questions:

• What is a block cipher?
• What are the differences between a block cipher and a stream cipher?
• For what do we need Modes of operation?
Summary

And we all know 5 modes of operation:

- Electronic Code Book (ECB)
- Cipher Block Chaining (CBC)
- Output Feedback Mode (OFB)
- Cipher Feedback Mode (CFB)
- Counter Mode (CTR)
Overview

• Block Cipher ✓
• Stream Cipher ✓
• Modes of Operation ✓
  • Electronic Code Book (ECB) ✓
  • Cipher Block Chaining (CBC) ✓
  • Output Feedback Mode (OFB) ✓
  • Cipher Feedback Mode (CFB) ✓
  • Counter Mode (CTR) ✓
• Summery ✓
• Conclusion ←
Conclusion

Security of a block cipher always depends on:

• Choice of the cipher itself
• Choice of mode of operation
• Choice of padding scheme
• Choice of initialization vector
References


• [wob01] Reinhard Wobst – Abenteuer Kryptologie, Addison-Wesley, 2001

• [can06] Christophe de Canniere, Alex Biryukov and Bart Preneel – „An Introduction of Block Cipher Cryptanalysis“, Proceedings of the IEEE, 02.2006
Thank you!

Questions?