CSc 466/566

Computer Security

15 : Cryptography — Modes and Padding

Version: 2019/12/11 23:15:00

Department of Computer Science
University of Arizona

collberg@gmail.com

Christian Collberg

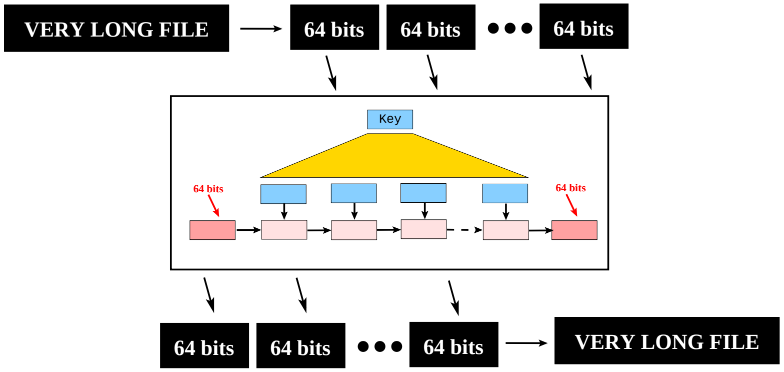
Outline

1. Introduction
2. ECB Mode — Don't Use This!
3. Padding
4. Better Modes of Operations
   - CBC
   - CFB
   - OFB
   - CTR
5. Evaluation
6. Summary

Learning Outcomes

- Algorithm for message padding
- Modes of operations: what are they, how are they used, show how they can fail
- Use of initialization vectors

Encrypting Large Plaintext



- A large message is encrypted piece-by-piece, each piece of size *blocksize*.
- More later about modes of operation, how to assemble/disassemble the sequence of blocks.

Block Cipher: Modes

- Modes of operation deal with how to encrypt a message of arbitrary length using a block cipher.
- To be useful, a mode must be at least as secure and as efficient as the underlying cipher.
- The most common modes for block ciphers are:
  1. Electronic Code Book (ECB)
  2. Cipher Block Chaining (CBC)
  3. Cipher Feedback (CFB)
  4. Output Feedback(OFB)
  5. Counter (CTR)

Outline

1. Introduction
2. ECB Mode — Don't Use This!
3. Padding
4. Better Modes of Operations
   - CBC
   - CFB
   - OFB
   - CTR
5. Evaluation
6. Summary

ECB Mode

- Electronic Codebook
- In ECB mode, each plaintext block is encrypted independently with the block cipher.
- Encryption:

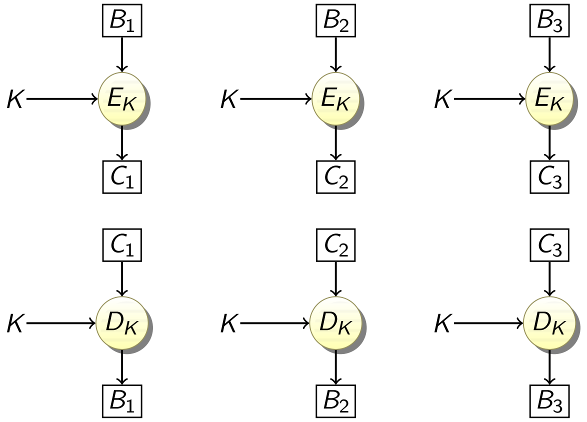
$$C_i \leftarrow E_K(B_i)$$

- Decryption:

$$B_i \leftarrow D_K(C_i)$$

- Notation:
  - B_i is the i:th plaintext block.
  - C_i is the i:th ciphertext block.

ECB Mode. . .



ECB Mode: Analysis

- Pros:
  - Simple.
  - Tolerates blocks lost in transit.
  - Easy to parallelize.
- Cons:
  - Identical plaintext blocks (eg. blocks of sky in a jpg) result in identical ciphertext ⇒ data patterns aren't hidden.

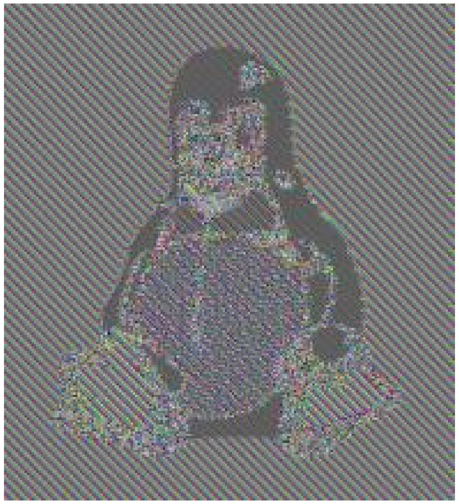
ECB Mode: Don't use it!

- Don't Do It!

> *the* Phantasy Star Online: Blue Burst *online video game uses Blowfish in ECB mode. Before the key exchange system was cracked leading to even easier methods, cheaters repeated encrypted* **monster killed** *message packets, each an encrypted Blowfish block, to illegitimately gain experience points quickly.[citation needed]*

en.wikipedia.org/wiki/Block_cipher_modes_of_operation

ECB Mode: Analysis. . .



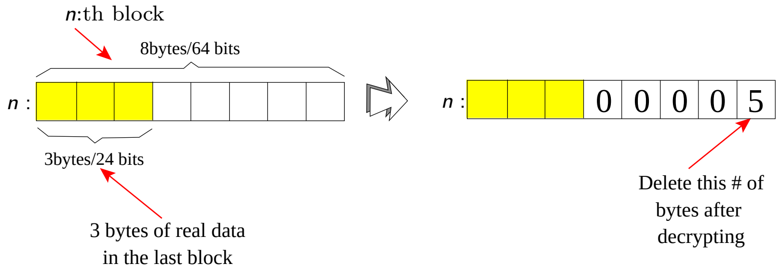
Source: https://en.wikipedia.org/wiki/Initialization_vector

Outline

1. Introduction
2. ECB Mode — Don't Use This!
3. Padding
4. Better Modes of Operations
   - CBC
   - CFB
   - OFB
   - CTR
5. Evaluation
6. Summary

Message Padding

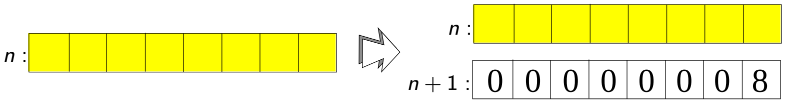
- What happens if the last plaintext block is not completely full?
- The message must be padded to a multiple of the cipher block size.
- One way to do this is to pad with 0:s and make the last byte be the number of bytes to remove from the last block:



n:th block
8bytes/64 bits
n :
3bytes/24 bits
3 bytes of real data in the last block
n :
0 0 0 0 5
Delete this # of bytes after decrypting

Message Padding. . .

- With this method you *have to* pad every message, even if it ends on a block boundary:



- Another method called ciphertext stealing doesn't add any extra blocks.

Outline

1. Introduction
2. ECB Mode — Don't Use This!
3. Padding
4. Better Modes of Operations
   - CBC
   - CFB
   - OFB
   - CTR
5. Evaluation
6. Summary

CBC Mode

- Cipher-Block Chaining
- In CBC mode, each plaintext block is XORed with the previous ciphertext block and then encrypted. An initialization vector IV is used as a seed for encrypting the first block.
- Initialization:

$$C_0 \leftarrow \mathrm{IV}$$

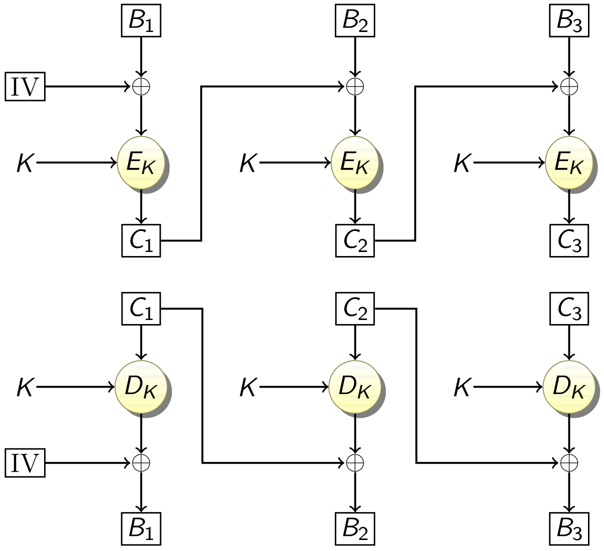
- Encryption:

$$C_i \leftarrow E_K(B_i \oplus C_{i-1})$$

- Decryption:

$$B_i \leftarrow D_K(C_i) \oplus C_{i-1}$$

CBC Mode. . .



CBC Mode: Analysis

- Pros:
  - Identical plaintext blocks will yield different ciphertext blocks.
  - Decryption can be parallelized if all ciphertext blocks are available.
  - If block C_i is lost, C_{i+1} can't be decrypted, but C_{i+2} can.
- Cons:
  - Encryption can't be parallelized.
- Most commonly used mode of operation.
- A one-bit change in a plaintext or IV affects all following ciphertext blocks.

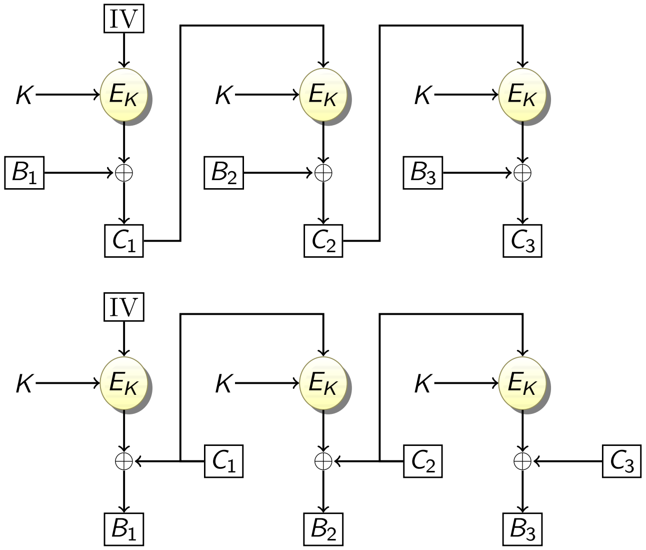
Initialization Vectors

- Several modes use IVs (Initialization Vectors).
- IVs have to be random and unpredictable.
- IVs don't have to be secret. They can be sent in cleartext.
- IVs ensure that two encryptions of the same plaintext result in different ciphertexts.

CFB Mode

- Cipher-FeedBack
- In CFB mode, the previous ciphertext block is encrypted and the output produced is combined with the plaintext block using XOR to produce the current ciphertext block.
- An initialization vector IV is used as a seed for the first block.
- Initialization: $C_0 \leftarrow \mathrm{IV}$
- Encryption: $C_i \leftarrow E_K(C_{i-1}) \oplus B_i$
- Decryption: $B_i \leftarrow E_K(C_{i-1}) \oplus C_i$

CFB Mode...



Exercise: CFB Mode Analysis

- Can decryption be parallelized?
- Can encryption be parallelized?
- Is the code smaller or larger than CBC mode?
- Assume 1 bit of C_i is corrupted in transit. What happens to the decrypted B_i?

OFB Mode

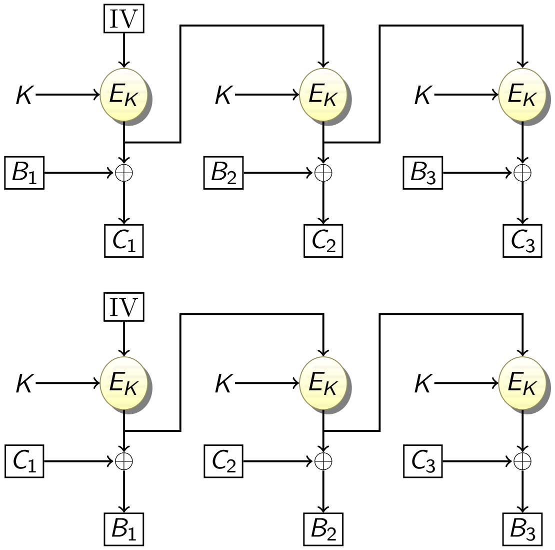
- Output-FeedBack Mode
- OFB mode is similar to CFB mode except that the quantity XORed with each plaintext block are vectors generated independently of both the plaintext and ciphertext.
- Stream cipher
- Initialization: $V_0 \leftarrow \mathrm{IV}$
- Create vectors: $V_i \leftarrow E_K(V_{i-1})$;
- Encryption:

$$C_i \leftarrow V_i \oplus B_i;$$

- Decryption:

$$B_i \leftarrow V_i \oplus C_i;$$

OFB Mode...



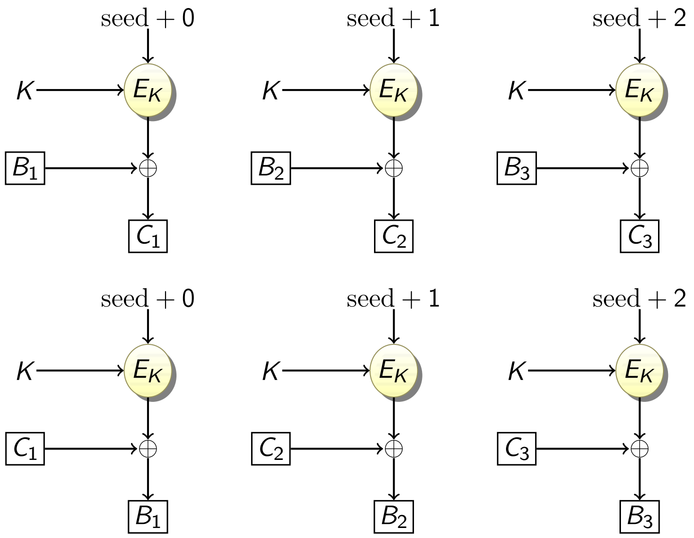
Exercise: OFB Mode Analysis

- Can decryption be parallelized?
- Can encryption be parallelized?
- Is the code smaller or larger than CBC mode?
- Assume 1 bit of C_i is corrupted in transit. What happens to the decrypted B_i?

CTR Mode

- Counter Mode
- CTR mode is similar to OFB: encryption is performed by XORing with a pad.
- Vectors are generated by encrypting $\mathrm{seed}+0, \mathrm{seed}+1, \mathrm{seed}+1, \ldots$ given a random seed.
- Create vectors: $V_i \leftarrow E_K(\mathrm{seed}+i-1)$;
- Encryption: $C_i \leftarrow V_i \oplus B_i$;
- Decryption: $B_i \leftarrow V_i \oplus C_i$;

CTR Mode. . .



Exercise: CTR Mode Analysis

- Can decryption and encryption be parallelized?
- What happens to the next block if one block is dropped in transit?

Outline

1. Introduction
2. ECB Mode — Don't Use This!
3. Padding
4. Better Modes of Operations
   - CBC
   - CFB
   - OFB
   - CTR
5. Evaluation
6. Summary

Misuses of Cryptosystem

- Cryptographic systems are sensitive to the environment.
- The strength of a cryptosystem depends on how it is used.
- Just because a cryptosystem is mathematically strong doesn't mean it's secure – it can be vulnerable to various attacks when used incorrectly.
- Attacks can be carried out in many ways besides guessing the key.

Misuses: Precomputing the Possible Message

If the plaintexts is drawn from a small set, attacker can just encipher all the plaintexts using the public key and search the intercepted ciphertext in database to find the corresponding plaintext (dictionary attack).

Misuses: Misordered Blocks

If different parts of ciphertext are not bound together, the attacker can delete, replay and reorder the ciphertext without being detected.

Misuses: Statistical Regularities

If each part of a message is enciphered separately the ciphertext can give away information about the structure of the message, even if the message itself is unintelligible.

Block Cipher: Performance Criteria

- Key size: decides the upper bound of security using exhaustive search.
- Block size: a larger block is harder to crack but more costly to implement.
- Complexity of cryptographic mapping: affect the implementation cost and real-time performance.
- Data expansion: it is desirable not to increase the size of the data.

Outline

1. Introduction
2. ECB Mode — Don't Use This!
3. Padding
4. Better Modes of Operations
   - CBC
   - CFB
   - OFB
   - CTR
5. Evaluation
6. Summary

Readings and References

- Chapter 8.1.6 in *Introduction to Computer Security*, by Goodrich and Tamassia.
- The Enigma Secret: http://www.youtube.com/watch?v=IJToxIZMbZQ&feature=related
- J. Orlin Grabbe, The DES Algorithm Illustrated, http://orlingrabbe.com/des.htm.

Acknowledgments

Additional material and exercises have also been collected from these sources:

1. Igor Crk and Scott Baker, *620—Fall 2003—Basic Cryptography*.
2. J. Orlin Grabbe, The DES Algorithm Illustrated, http://orlingrabbe.com/des.htm.
3. Andrea Sanchez, *DES Algorithm*, https://www.youtube.com/watch?v=dRH585Ctp3E.
4. Dan Boneh, *The Data Encryption Standard -Cryptography*, https://www.youtube.com/watch?v=UgFoqxKY7cY.