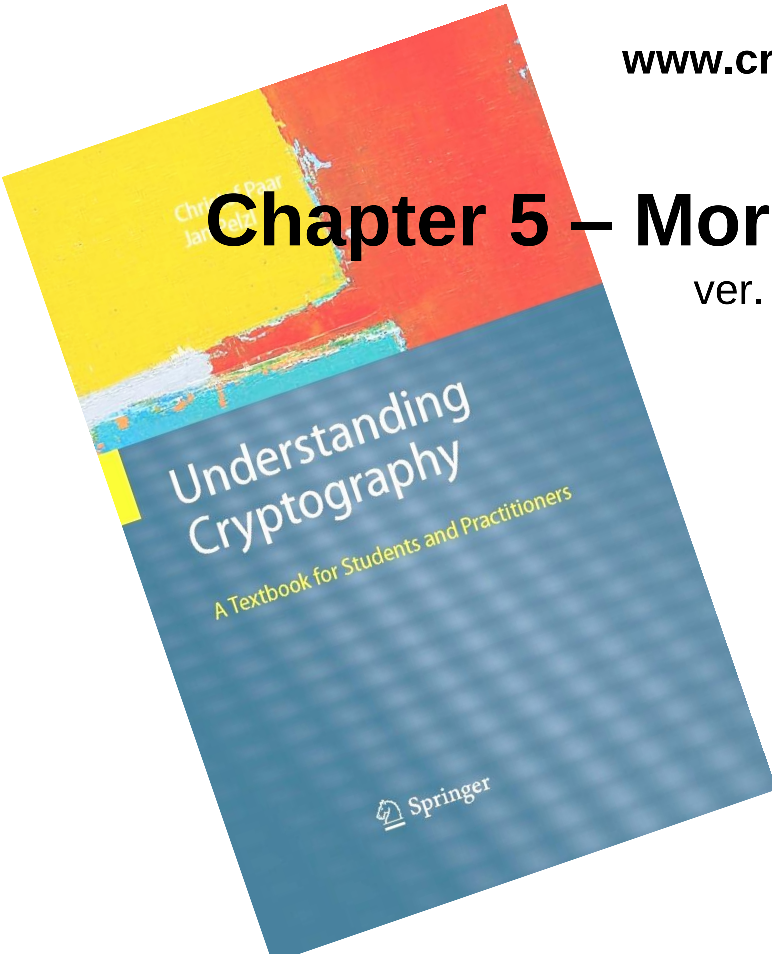
Understanding Cryptography – A Textbook for Students and Practitioners

by Christof Paar and Jan Pelzl

www.crypto-textbook.com



Chapter 5 – More About Block Ciphers

ver. October 5, 2024

These slides were originally prepared by Amir Moradi, Christof Paar and Jan Pelzl. Later, they were modified by Tomas Fabsic for purposes of teaching I-ZKRY at FEI STU.

Homework

- Read Section 5.1 (you can skip subsections 5.1.3, 5.1.4 and 5.1.6).

Some legal stuff (sorry): Terms of Use

- The slides can used free of charge. All copyrights for the slides remain with Christof Paar and Jan Pelzl.
- The title of the accompanying book “Understanding Cryptography” by Springer and the author’s names must remain on each slide.
- If the slides are modified, appropriate credits to the book authors and the book title must remain within the slides.
- It is not permitted to reproduce parts or all of the slides in printed form whatsoever without written consent by the authors.

Content of this Chapter

- Encryption with Block Ciphers for Confidentiality: Modes of Operation
  - Electronic Code Book mode (ECB)
  - Cipher Block Chaining mode (CBC)
  - Counter mode (CTR)

Block Ciphers

- A block cipher is much more than just an encryption algorithm, it can be used ...
  - to build different types of block-based encryption schemes
  - to realize stream ciphers
  - to construct hash functions
  - to make message authentication codes
  - to build key establishment protocols
  - to make a CSPRNG
  - ...

Encryption with Block Ciphers for Confidentiality

- There are several ways of encrypting long plaintexts, e.g., an e-mail or a computer file, with a block cipher ("modes of operation")
  - Electronic Code Book mode (ECB)
  - Cipher Block Chaining mode (CBC)
  - Counter mode (CTR)
- All of the above modes have only one goal – **confidentiality (dôvernosť)**.
- Confidentiality:
  - The content of the message is hidden from illegitimate parties.

Encryption with Block Ciphers for Authenticity and Integrity

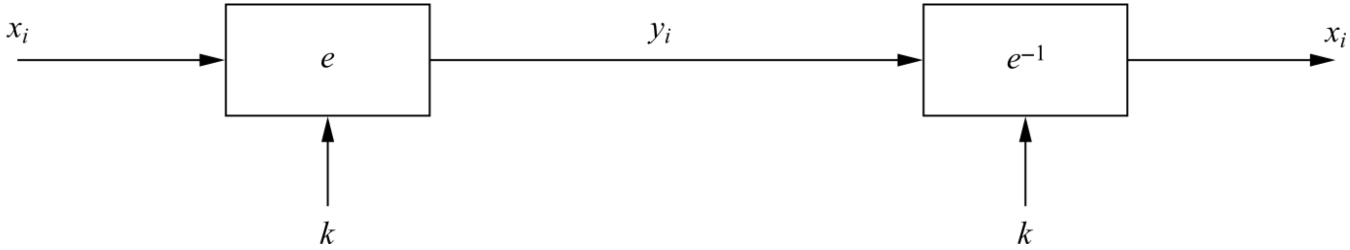
- Other important goals in cryptography:
  - Is the message really coming from the original sender? (**authenticity**)
  - Was the ciphertext altered during transmission? (**integrity)**
- Modes providing authenticity and integrity (Chapter 13):
  - CBC-MAC
  - Cipher-based MAC (CMAC)
- Modes providing both confidentiality and authenticity and integrity (Chapter 13):
  - Cipher Block Chaining-Message Authentication Code (CCM)
  - Galois Counter mode (GCM)
- Today, **CCM and GCM are the most recommended modes** when confidentiality is needed!

Content of this Chapter

- Encryption with Block Ciphers for Confidentiality: Modes of Operation
  - **Electronic Code Book mode (ECB)**
  - Cipher Block Chaining mode (CBC)
  - Counter mode (CTR)

Electronic Code Book mode (ECB)

- $e_k(x_i)$ denote the encryption of a b-bit plaintext block x_i with key k
- $e_k^{-1}(y_i)$ denote the decryption of b-bit ciphertext block y_i with key k
- Messages which exceed b bits are partitioned into b-bit blocks
- **Each Block is encrypted separately**



Encryption: $y_i = e_k(x_i),\ \ i \geq 1$

Decryption: $x_i = e_k^{-1}(y_i) = e_k^{-1}(e_k(x_i)),\ \ i \geq 1$

ECB: advantages/disadvantages

- Advantages
  - no block synchronization between sender and receiver is required
  - bit errors caused by noisy channels only affect the corresponding block but not succeeding blocks
  - Block cipher operating can be parallelized
    - advantage for high-speed implementations

- **Disadvantages**
  - **ECB encrypts highly deterministically!**
    - identical plaintexts result in identical ciphertexts
      - an attacker recognizes if the same message has been sent twice
    - plaintext blocks are encrypted independently of previous blocks
      - an attacker may reorder ciphertext blocks which results in valid plaintext

Substitution Attack on ECB

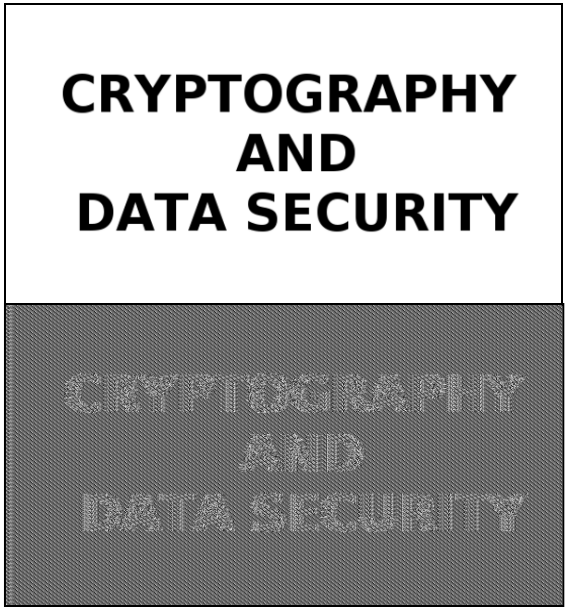
- Once a particular plaintext to ciphertext block mapping $x_i \rightarrow y_i$ is known, a sequence of ciphertext blocks can easily be manipulated
- Suppose an *electronic bank transfer*

Block #	1	2	3	4	5
	Sending Bank A	Sending Account #	Receiving Bank B	Receiving Account #	Amount $

  - the encryption key between the two banks does not change too frequently
  - The attacker sends $1.00 transfers from his account at bank A to his account at bank B repeatedly
    - He can check for ciphertext blocks that repeat, and he stores blocks 1,3 and 4 of these transfers
  - He now simply replaces block 4 of other transfers with the block 4 that he stored before
    - *all transfers* from some account of bank A to some account of bank B are redirected to go into the attacker's B account!

Example of encrypting bitmaps in ECB mode

- Identical plaintexts are mapped to identical ciphertexts



- Statistical properties in the plaintext are preserved in the ciphertext

Content of this Chapter

- Encryption with Block Ciphers for Confidentiality: Modes of Operation
  - Electronic Code Book mode (ECB)
  - **Cipher Block Chaining mode (CBC)**
  - Counter mode (CTR)

Cipher Block Chaining mode (CBC)

- There are two main ideas behind the CBC mode:
  - The encryption of all blocks are “chained together”
    - ciphertext y_i depends not only on block x_i but on all previous plaintext blocks as well
  - The encryption is randomized by using an initialization vector (IV)

Encryption (first block): $y_1 = e_k(x_1 \oplus \text{IV})$

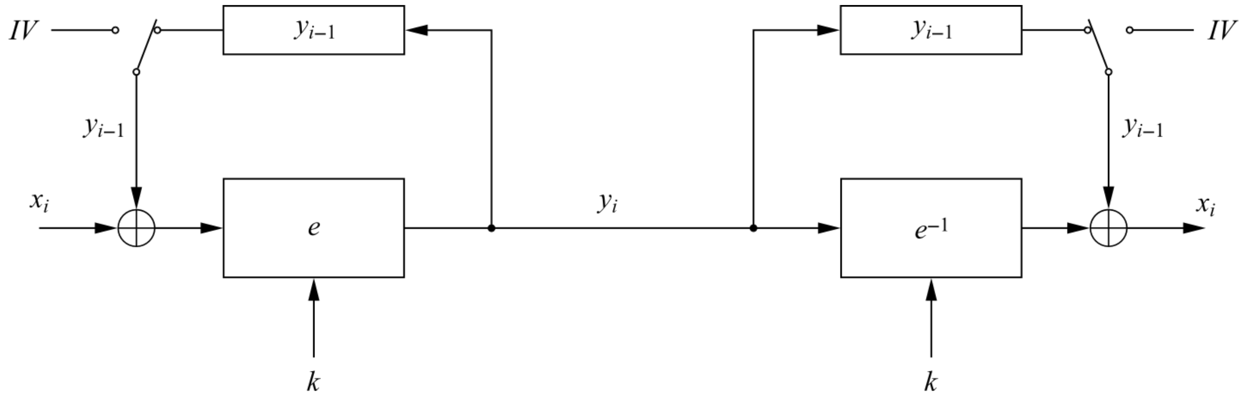
Encryption (general block): $y_i = e_k(x_i \oplus y_{i-1}), \; i \geq 2$

Decryption (first block): $x_1 = e_k^{-1}(y_1) \oplus \text{IV}$

Decryption (general block) : $x_i = e_k^{-1}(y_i) \oplus y_{i-1}, \; i \geq 2$

Cipher Block Chaining mode (CBC)

- For the first plaintext block x_1 there is no previous ciphertext
  - an IV is added to the first plaintext to make each CBC encryption nondeterministic
  - the first ciphertext y_1 depends on plaintext x_1 and the IV
- The second ciphertext y_2 depends on the IV, x_1 *and* x_2
- The third ciphertext y_3 depends on the IV and x_1, x_2 *and* x_3, and so on



Substitution Attack on CBC

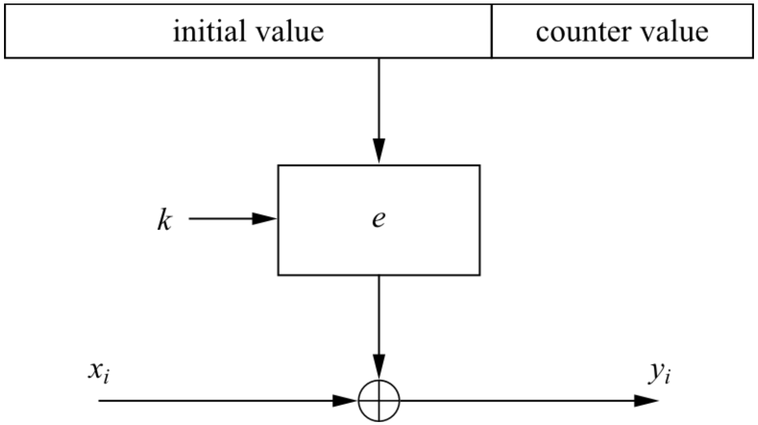
- Suppose the last example (*electronic bank transfer*)
- If the IV is properly chosen for every wire transfer, the attack will not work at all
- If the IV is kept the same for several transfers, the attacker would recognize the transfers from his account at bank A to back B
- If we choose a new IV every time we encrypt, the CBC mode becomes a probabilistic encryption scheme, i.e., two encryptions of the same plaintext look entirely different
- It is not needed to keep the IV *secret*!
- Typically, the IV should be a non-secret nonce (value used only once)

Content of this Chapter

- Encryption with Block Ciphers for Confidentiality: Modes of Operation
  - Electronic Code Book mode (ECB)
  - Cipher Block Chaining mode (CBC)
  - **Counter mode (CTR)**

Counter mode (CTR)

- It uses a block cipher as a **stream cipher**
- The key stream is computed in a blockwise fashion
- The input to the block cipher is a counter which assumes a different value every time the block cipher computes a new key stream block



- can be parallelized since the 2^{nd} encryption can begin before the 1^{st} one has finished
- IV and counter value do not have to be secret

Encryption: $y_i = e_k(\text{IV} \,||\, \text{CTR}_i) \oplus x_i, \quad i \geq 1$

Decryption: $x_i = e_k(\text{IV} \,||\, \text{CTR}_i) \oplus y_i, \quad i \geq 1$

Lessons Learned

- There are many different ways to encrypt with a block cipher.
- Some modes of operation turn a block cipher into a stream cipher.
- The straightforward ECB mode has security weaknesses, independent of the underlying block cipher.
- The counter mode allows parallelization of encryption and is thus suited for highspeed implementations.