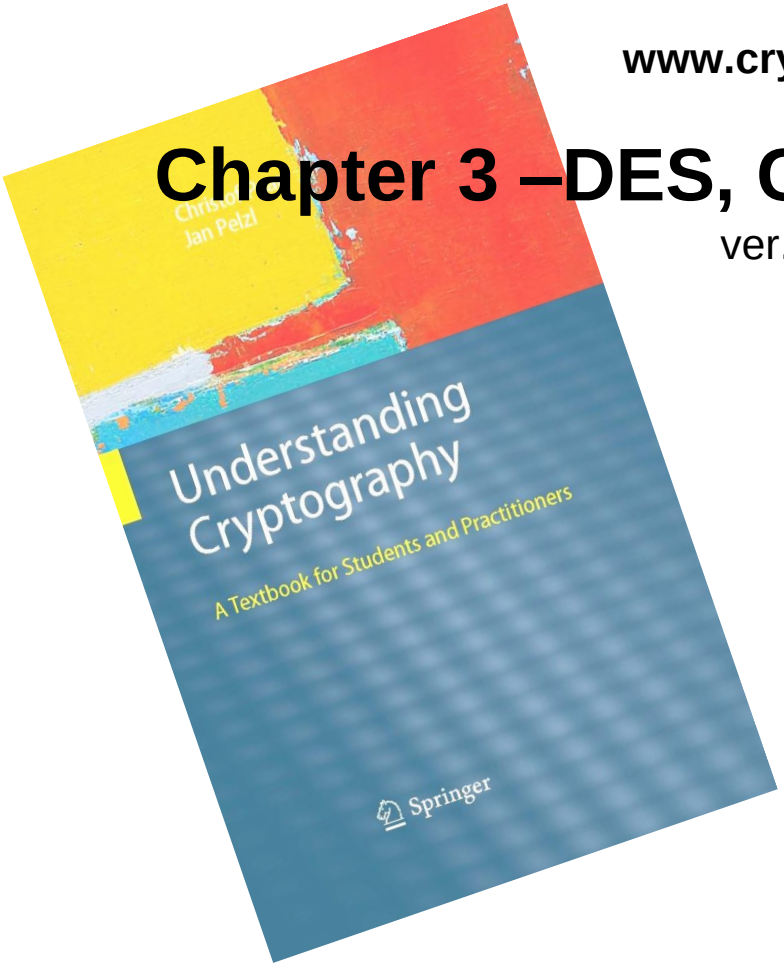
Understanding Cryptography – A Textbook for Students and Practitioners

by Christof Paar and Jan Pelzl

www.crypto-textbook.com



Chapter 3 –DES, Confusion and Diffusion

ver. Sep 27, 2024

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

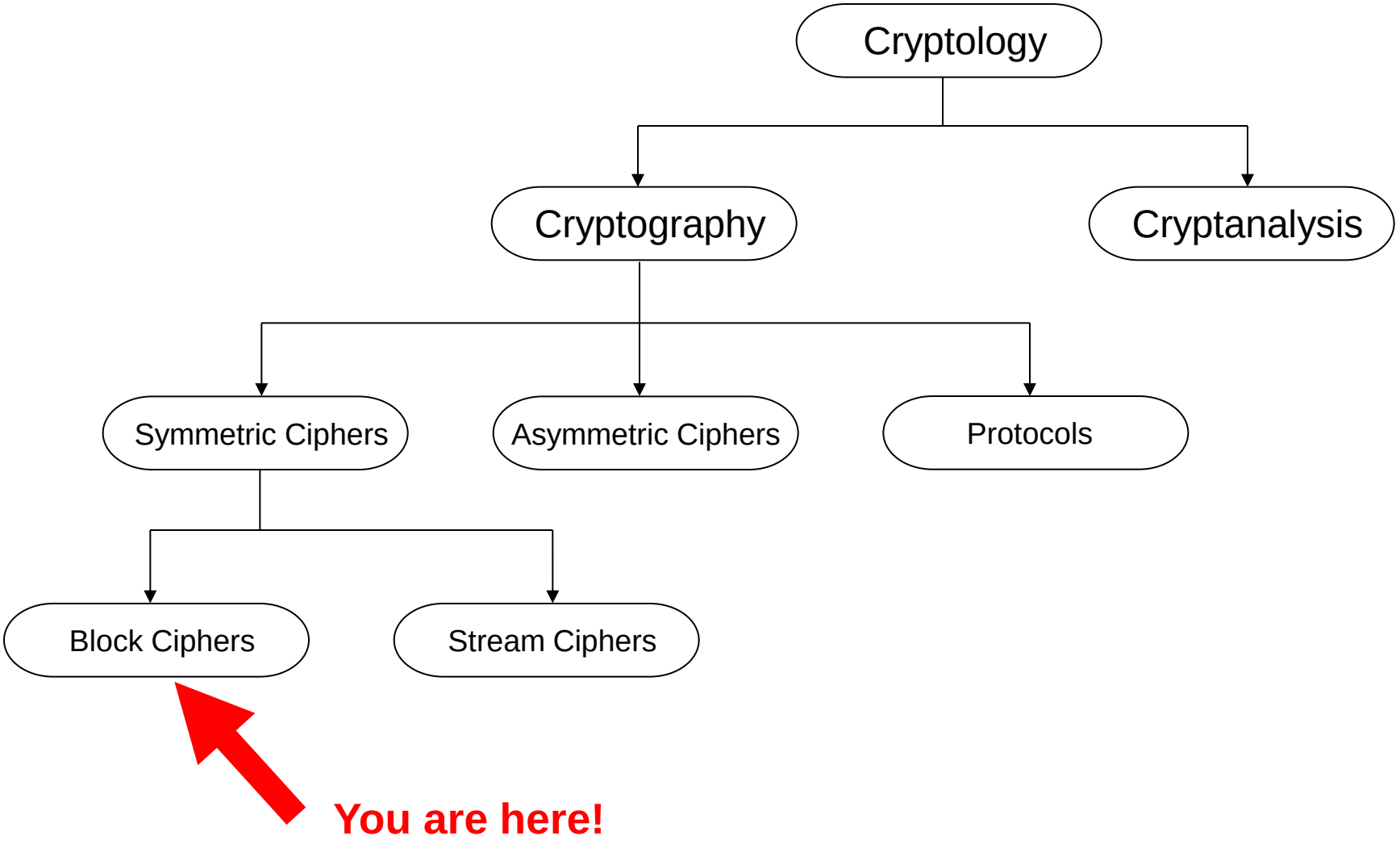
Homework

- Read Section 3.1 (pages 74 - 76).

Some legal stuff (sorry): Terms of Use

- The slides can used free of charge. All copyrights for the slides remain with the authors.
- 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.

Classification of DES in the Field of Cryptology



DES Facts

- Data Encryption Standard (DES) encrypts **blocks of size 64 bit**.
- Developed by **IBM** based on the cipher *Lucifer* under influence of the *National Security Agency* (NSA), the design criteria for DES have not been published.
- Encryption and decryption algorithms have a structure of a ***Feistel network (feistelovská sieť)***.
- **Standardized 1977** by the **National Bureau of Standards** (NBS) today called *National Institute of Standards and Technology* (NIST).
- Nowadays considered **insecure** due to the small **key length of 56 bit.**
- Replaced by the *Advanced Encryption Standard* (**AES**) in 2001.

- For a more detailed history see Chapter 3.1 in *Understanding Cryptography.*

Block Cipher Primitives: Confusion and Diffusion

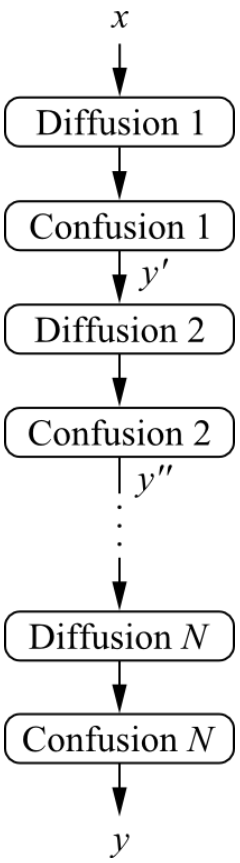
- Claude Shannon: There are two primitive operations with which strong encryption algorithms can be built:

  1. **Confusion (konfúzia):** An encryption operation where the **relationship between the key and ciphertext is complex (non-linear)**.
     Today, a common element for achieving confusion is **substitution**.

  2. **Diffusion (difúzia) :** An encryption operation where the **influence of one plaintext symbol is spread over many ciphertext symbols** with the goal of hiding statistical properties of the plaintext.

- Both operations by themselves cannot provide security. The idea is to concatenate confusion and diffusion elements to build so called ***product ciphers (súčinové šifry)*.**

Product Ciphers *(súčinové šifry)*



- Most of today's block ciphers are ***product ciphers*** as they consist of rounds which are applied repeatedly to the data.
- Can reach excellent diffusion: **changing of one bit of plaintext results** *on average* in the **change of half the output bits**.

Example: