

## Motivation

Differential cryptanalysis is a general tool in the cryptanalysis of block ciphers. Originally devised to cryptanalyse the Data Encryption Standard (DES), it has later been applied to other block ciphers, stream ciphers and hash functions. A differential attack exploits predictable propagation of the difference between a pair of inputs of a cryptographic primitive, to the corresponding outputs.

In this project, we implement the original attack of Biham and Shamir on the DES and round-reduced variants, respectively.

## Goals and Tasks

- ▶ Acquire the necessary background
- ▶ Understand differential cryptanalysis
- ▶ Understand the attack on DES
- ▶ Implement (parts of) the attack

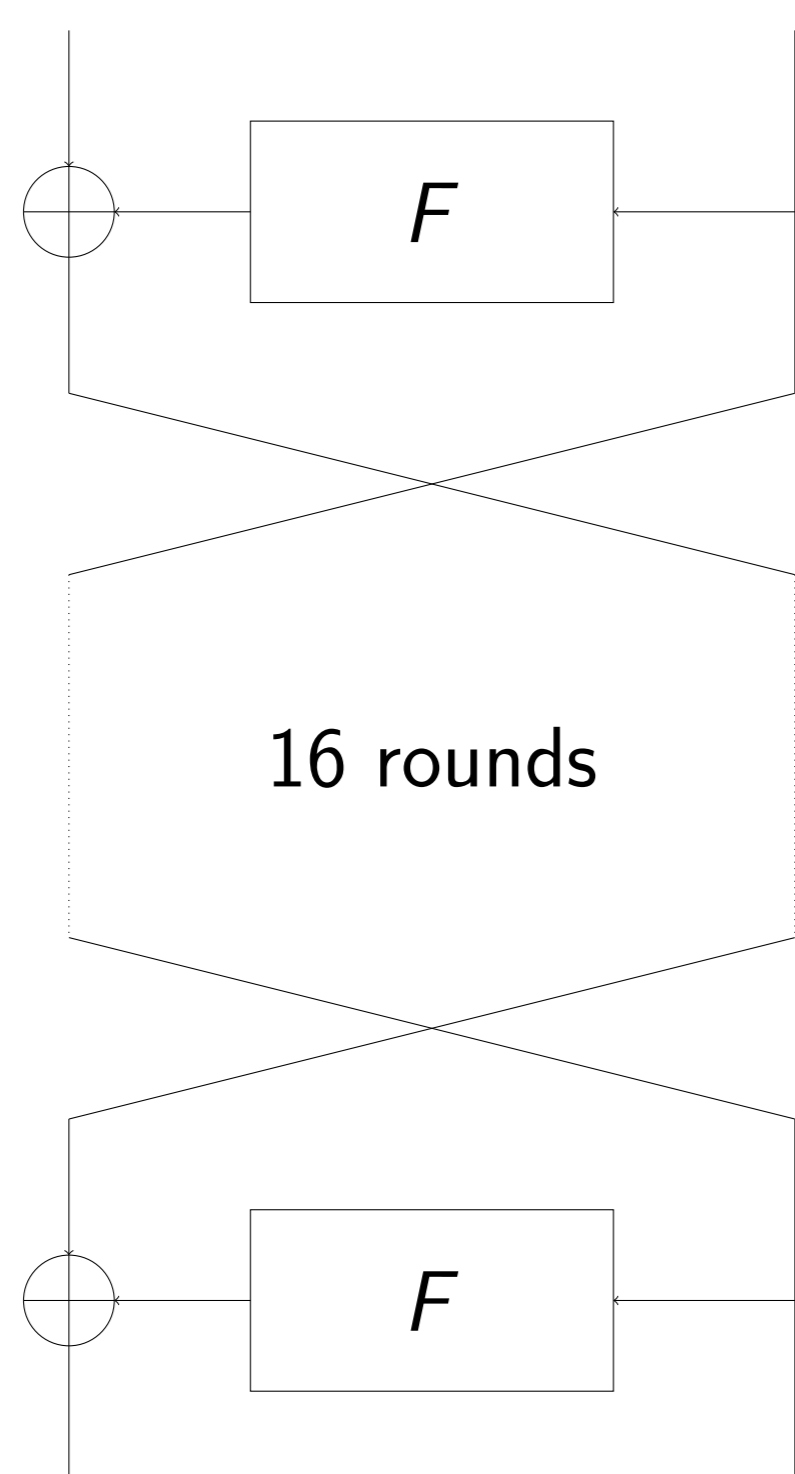


Figure 1: Schematic view of DES.

## Literature

- ▶ E. Biham and A. Shamir. Differential Cryptanalysis of DES-like Cryptosystems. *J. Cryptology*, 4(1):3–72, 1991.
- ▶ E. Biham and A. Shamir. Differential Cryptanalysis of the Full 16-Round DES. In E. F. Brickell, editor, *CRYPTO*, volume 740 of *LNCS*, pages 487–496. Springer, 1992.

## Deliverables

- ▶ Project files (.zip, cleaned)
- ▶ Documentation (inline)
- ▶ Readme (getting started)
- ▶ Presentation (10 .ppt slides)

## Project Schedule

- ▶ Start Immediately
- ▶ Month 1 Reading literature
- ▶ Month 2 Implementing
- ▶ Month 3 Final deliverables

## Studies

- INF
- SW
- TEL
- TM

## Prerequisites

- ▶ C/C++ programming

## Advisor / Contact

[martin.schlaeffer@iaik.tugraz.at](mailto:martin.schlaeffer@iaik.tugraz.at)