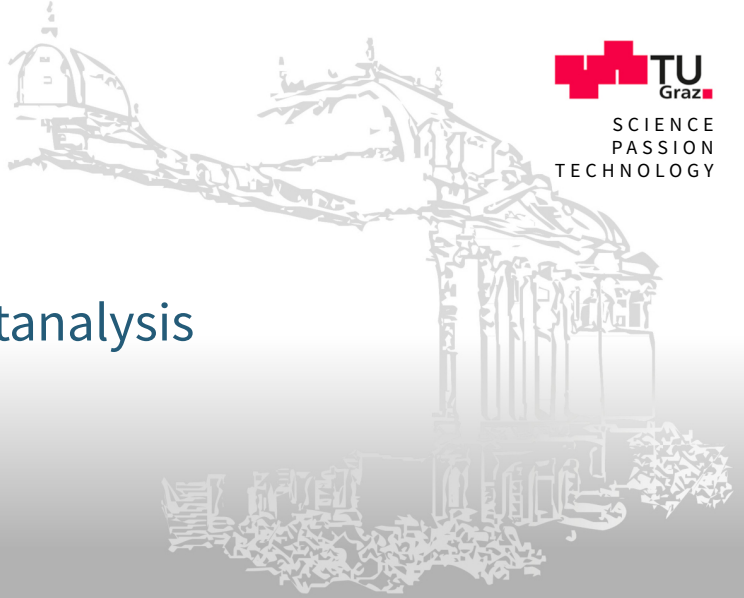

SCIENCE
PASSION
TECHNOLOGY

Differential Cryptanalysis

Maria Eichlseder

Course Name – WS 2020/21

Outline

Introduction

Context and Idea

Dependencies

Minimum dependencies:

- `cryptolecture.cls`
- `beamerthemetugraz2018.sty`

Recommended dependencies:

- `beamerthemetugraz/background_16-9.jpg` or `beamerthemetugraz/background_4-3.jpg`
- `tikzlibrarycipher.code.tex`

Differential Cryptanalysis

- Proposed by Biham and Shamir [BS90] for `DES`
- …

Attack Strategy

Alice and Bob

Alice

Bob

Caesar

Eve

Hatguy

Title

Content

Questions

Bibliography I

[BS90] Eli Biham and Adi Shamir. **Differential Cryptanalysis of DES-like Cryptosystems**. Advances in Cryptology – CRYPTO 1990. Vol. 537. LNCS. Springer, 1990, pp. 2–21. DOI: 10.1007/3-540-38424-3_1.