Matura paper contents

Introduction / preparation

- Thanks / dedications
- Introduction
    - Why I chose this project
    - (“The code book” by Simon Singh)
    - Make sure the introduction is clearly separate from the main body!
- Vocabulary (should come before the major chapters, so that the readers can refer to this chapter while reading the explanations of how the two systems work) → will be updated as I continue to work on the project

Major chapters

1. OTP

- A one-time pad is a key (important to clarify: “one time pad” refers both to the method used as well as the key which is employed)
- Method used (step by step in subchapters)
    - Generation of the random key (the actual one-time pad)
    - Modular addition of the key and plaintext (modulo 26, practical example) → possibly mention similarity to the Caesar cipher
    - Decoding of the Ciphertext using the key
- Perfect secrecy (information-theoretical security)
    - Definition
    - (Mathematical proof Shannon, Claude E. (October 1949). "Communication Theory of Secrecy Systems")?
    - Why can only OTP achieve perfect secrecy
- Problems
    - True randomness in generating the key
    - How to securely distribute the OTPs themselves
    - One-time pad → how can the key be disposed of with adequate security

2. AES

- Standard state
  - 4x4 column-major order matrix (Rechnen mit Matrizen SPF Unterlagen holen)
  - Finite field
- Substitution-permutation network
  - Substitution (S-box)
  - Permutation (P-box)
  - Graphical representation
- Method used (step by step in subchapters) → each round consists of these four steps
  - Subbytes
    - What is a subbyte
    - Usage of Rijndael S-boxes (what is a Rijndael S-box / comparison with a general S-box)
  - Shiftrows
  - Mixcolumns
  - Addroundkey
- Fulfilment of Shannon's confusion and diffusion properties
  - Diffusion
    - Definition
    - Fulfilment through AES
  - Confusion (short chapter, the reason for confusion is very similar to the one for diffusion)
- Practical example (to be kept as simple as possible)
- Problems
  - Overreliance on / Overconfidence in AES
  - Private-key cryptography → keeping of a shared secret

3. Comparison / code

- Possibly some code snippets / the whole program (python OTP) → should this be included in chapter 1 instead?
- Possibly interesting / often used Latex structures
- Key similarities between OTP and AES
- Key differences between OTP and AES
    - Illustration through practical examples → How do these differences affect the employment, safety and results of the algorithms
- Comparison through questions → usage of the similarities and differences to explain the answers to these questions
    - Why is AES regarded as far safer, despite the mathematical proof for OTP's perfect secrecy?
    - Historical transition: OTP as the first cryptographic system to utilize a (mechanical) computer (teleprinter cipher proposed by Gilbert Vernam) to today's AES, which is currently the system regarded as appropriate for top secret messages
- Conclusion
    - Restatement of the topic
    - Restate asked question(s)
    - Summarization of main points
    - Combination of the main points → concluding sentence

Appendix

- Closing statement
    - Personal journey throughout writing the paper
        - Learning Git
        - Learning LaTeX
- Reference to journal (GitHub)

Bibliography

- Source management with LaTex