

# Quantification and Visualization of Cryptographic Notions\*

Hiwi

Attack trees and graphs from the literature are used to analyze single systems in which edges always have the same meaning: Single attacks in the case of attack graphs, sub-attacks in the case of attack trees. For our use case (see Figure 1), the system can be thought of as a “cryptosphere”, but edges can have different meanings. A more precise classification is in progress and part of the Hiwi-Job.

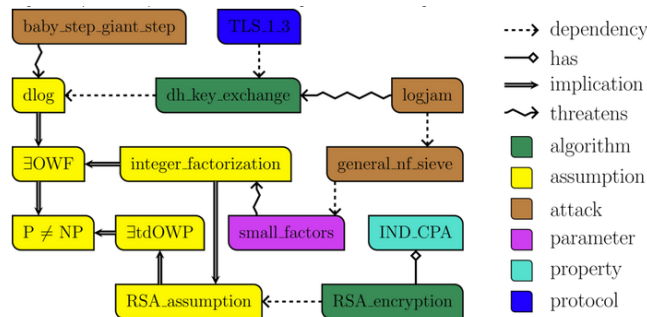


Figure 1: Cryposphere attack tree.

## Scope of the work

The student is expected to

- Extend and document the existing Frontend, Backend
- Design and develop a graph model for security notions

Formal:

- Number of hours: 20-40 per month
- Earliest start date: 23rd February, 2023

## Requirements

Following knowledge is required

### Frontend

- UI: Vuitify, Axios
- Visualization: Vis.js, D3.js

### Backend

- Python3
- Flask, SQLite

### Cryptography

- Overview of security notions
- Basic knowledge on relations of the above

## Contact/Kontakt

In case of interest or for further information, please contact/ Bei Interesse oder Fragen zur Aufgabenstellung freue ich mich über eine kurze E-Mail an Marcel Tiepelt, [marcel \(dot\) tiepelt \(at\) kit \(dot\) edu](mailto:marcel(dot)tiepelt(at)kit(dot)edu).

\* The project description is only for inclusive reasons in English and the project can also be done in German.