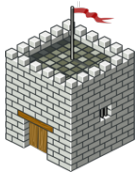
𝔽oundations of Cybersecurity
Exercise Sheet 8
Singapore University of Technology and Design
November 15, 2017



- There can be multiple acceptable answers. Justify carefully your reasoning.
- Go to the point, avoid copying verbatim definitions from the slides or the book.
- Show the solutions of classwork (groups of max 3 persons) to an instructor before the end of the class.
- Submit your homework solutions (groups of max 2) to eDimension by the deadline below.

Classwork due on Wednesday November 15, 10:00 PM

Question 1

Implement the final version of the key negotiation protocol. (You can use external libraries.)

Homework due on Wednesday November 22, 6:59 PM

Question 1

Design and implement a simple key management protocol. The protocol should base on a KDC that shares keys with Alice and Bob. Alice, initiating communication, should establish (through the KDC) a shared key with Bob. Introduce the three following classes: `KDC, Alice, Bob`, and present the protocol as an interaction between three objects of these classes.

Are you aware of any limitations or security problems of your solution (consider replay attacks, confidentiality and authentication, introduced overheads, ...)? Do you see any ways of improving them? Benchmark your protocol. How many key establishments can it handle per second?