SUTD 51.505: 𝔽oundations of Cybersecurity (2018)

Exercise Sheet 11
November 23, 2018

- List your names (max 3 members for each group) on the answer sheet, **if you have actually worked on the exercises.**
- Answer questions in the same order as in the exercise sheet.
- Type in 12pt font, with 1.5 line spacing.
- There can be multiple acceptable answers. Justify carefully your reasoning.
- Go to the point, avoid copying verbatim definitions from the slides or the book.
- Submit your classwork and homework solutions (in pdf file) to eDimension by the deadlines below. Each group only needs one submission.
- Grading: total 100 points for each classwork and homework, each exercise has equal points in the same classwork and homework.

Classwork due on Friday November 23, 10:00 PM

Exercise 1
Implement the final version of the key negotiation protocol. (You can use external libraries.)

Exercise 2
Is the symmetric key based mutual authentication protocol (Slide 26) subject to reflection attack? If yes, describe the attack.

Homework due on Friday November 30, 6:59 PM

Exercise 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 following three classes: `KDC, Alice, Bob`, and present the protocol as an interaction between three objects of these classes.

a) Are you aware of any limitations or security problems of your solution (consider replay attacks, confidentiality and authentication, overheads, etc.)?

b) Do you see any ways of improving them?

Exercise 2

Design (or find) a fair non-repudiation protocol to further reduce the TTP's involvement, for example, using an off-line TTP.

- **On-line TTP** is actively involved in every instance of a non-repudiation service (e.g. the protocol in Slide 38).
- **Off-line TTP** supports non-repudiation without being involved in each instance of a service.