SUTD 51.505: 𝔽oundations of Cybersecurity (2018)

Exercise Sheet 12
November 30, 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 30, 10:00 PM

Exercise 1

Design and implement a simple digital certificate framework. Your framework should allow to create a certificate chain and validate it.

Homework due on Friday December 7, 6:59 PM

Exercise 1

Incorporate your digital certificate framework (this week's classwork) to your key negotiation protocol (Week 11 classwork). Then incorporate both to your secure channel implementation (Week 9 homework). More specifically, in the final system:

a) Alice and Bob trust a CA (i.e., Alice and Bob have the CA's certificate).

b) This CA issues certificates for Alice and Bob respectively.

c) Alice initiates a connection with Bob, starting an authenticated key negotiation. (She needs to send her certificate which is then validated by Bob.)

d) Bob authenticates the negotiation. (He also needs to send his certificate to Alice.)

e) After a shared key is established, the secure channel can be initiated.