SUTD 51.505: 𝔽oundations of Cybersecurity (2018)

Exercise Sheet 9
November 9, 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 9, 10:00 PM

Exercise 1
Suppose Alice and Bob are communicating using the secure channel described in FSK's Chapter 7. Eve is eavesdropping on the communications. What types of traffic analysis information could Eve learn by eavesdropping on the encrypted channel? Describe a situation in which information exposure via traffic analysis is a serious privacy problem.

Exercise 2
Compare the advantages and disadvantages among the different orders of applying encryption and authentication when creating a secure channel.

Exercise 3
For your platform, language, and crypto library of choice, implement authenticated encryption in GCM (Galois/Counter Mode).

- K = 128-bit 1
- P = `SUTD-MSSD-51.505*Foundations-CS*SUTD-MSSD-51.505`
- IV = 128-bit 0

a) What are the ciphertext C and authentication tag T?

b) Swap the the first and third blocks of C, what is the outcome of tag verification and decryption? (For decryption, ignore tag verification)

c) Remove the third block of C, what is the outcome of tag verification and decryption? (For decryption, ignore tag verification)

d) Change the last bit of C, what is the outcome of tag verification and decryption? (For decryption, ignore tag verification)

e) Discuss the security features of GCM based on the results of b) - d).

Homework due on Friday November 16, 6:59 PM

Exercise 1
Design and implement a secure channel. Use the following interface:

```
class Peer(object):
    def __init__(self, key):
        ...

    def send(self, msg):
        ...  # protect the message
        return protected_msg  # type of protected_msg is 'str'

    def receive(self, protected_msg):
        ...  # verify the message and print errors if any
        print msg  # successfuly recovered plaintext

# Example
alice = Peer("very secret key!")
bob = Peer("very secret key!")

msg1 = alice.send("Msg from alice to bob")
bob.receive(msg1)

msg2 = alice.send("Another msg from alice to bob")
bob.receive(msg2)

msg3 = bob.send("Hello alice")
alice.receive(msg3)
```

Exercise 2
Describe how SSL/TLS protect confidentiality and integrity of messages.

Exercise 3
Compare the advantages and disadvantages of using a PRNG vs a RNG.

Exercise 4
Implement a naive approach for generating random numbers in the set 0, 1, ..., 127. For this naive approach, generate a random 8-bit value, interpret that value as an integer, and reduce that value modulo 128. Experimentally generate 512 random numbers in the set 0, 1, ..., 127, and report on the distribution of results.