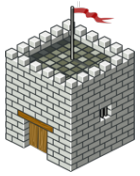
𝔽oundations of Cybersecurity
Exercise Sheet 8
Singapore University of Technology and Design
November 1, 2017



- 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 1, 10:00 PM

Question 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)
```

Homework due on Wednesday November 8, 6:59 PM

Question 1

For your platform, language, and cryptography library of choice, summarize how the cryptographic PRNG works internally. Consider issues including (but not limited) to the following: how the entropy is collected, how reseeding occurs, and how the PRNG handles reboots,... .

Question 2

Modify your design for the secure channel in this chapter to use a dedicated, single-key mode for providing both encryption and authentication (e.g., GCM, OCB, CCM, or CWC). Compare and report efficiency of these two implementations.