Network Security

Exercises 2
Question 1

Tobias Famos
16-933-764

March 7, 2022

- Symmetric encryption is a crypto-mechanism where encryption and decryption are performed using different keys.
  True
  This is true, opposued to asymmetric encryption where the decryption and encryption are done using different keys.

- With the use of symmetric encryption, the principal security problem is maintaining the secrecy of the key.
  True
  Maintaining the secrecy of the key is a principal concern of any encryption method, thus also of the symmetric encryption.

- The process of converting from plaintext to ciphertext is known as deciphering or decryption.
  False
  By definition the **de**cryption is turning a cyphertext into plaintext and **en**cryption is turning a plaintext into a cypthertext.

- The algorithm will produce a different output depending on the specific secret key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key.
  True
  The exact substitution and transformation depends on the key and algorithm (e.g. which bit or byte will be replaced by which bit or byte or moved where). This is true for all the symmetric encryption algorithms.

- When using symmetric encryption it is very important to keep the algorithm secret.
  False

As in any encryption or security concern it is bad practice ensuring security by obscurity. The encryption should be secure even if the algorithm is known.

- Ciphertext generated using a computationally secure encryption scheme is impossible for an opponent to decrypt simply because the required information is not there. **True**
  A cypther is considered computationally secure, if it is not crackable in a reasonable amount of time. As a cypher can not be decoded without the key this is true. Also the explanation because the information is not there seems reasonable, as the key is the piece to the puzzle that is needed to solve it. There are a few algorithms that are crackable but most of the time this has to do with cryptoanalysis (e.g. based on the distribution of the letters in a text or some other knowledge about the plaintext)