Computer Security Fundamentals – Spring 2023

Introduction to Cryptography **Total: 5 points**

Q1. What is the major difference between symmetric key cryptography and asymmetric key cryptography? (1 pt)

Q2. What is the major difference for Stream ciphers vs. Block ciphers in Symmetric key cryptography? (1 pt)

Q3. What is hashing collision? (0.5 pt)
How to prevent the collision? Can you give me an example of that? (0.5 pt)

Q4. DSA vs. RSA, what's the major difference? (0.5 pt)
They are very similar in the process of execution.
So basically, in the end of the execution, they will need to verify something.
For example, see if h1 == h2? Tell me why it is designed in this way? (0.5 pt)
(Hint: You can try to explain that by using the process of data transmission.
Sender → Receiver)

Q5. Briefly tell me what are the jobs "SSL handshake" will do in the 4 phases? (1 pt)