Veton Abazovic

NetID: va187

Computer Security

3/27/19

Assignment 7

Question 1

What is a necessary condition for perfect secrecy?

Answer: The necessary condition for perfect secrecy is for there to be as many keys as there are plaintexts.

Question 2

How did Robert Hooke use a one-way function in 1678?

Answer: Robert Hooke used a one-way function in 1678 to create an anagram of his law which described spring motion. He did this because he wanted to claim the idea while still developing his theory.

Question 3

What are the three properties of hash functions listed in the text?

Answer:

1. One-wayness
2. Output will not give any information about the input.
3. Usually it is harder to find collisions with large inputs

Question 4

What does an s-box do in a symmetric block cipher?

Answer: An s-box in a symmetric block cipher is a substitution box that will diffuse the message with the use of gates that will swap bit orders. It is more efficient and very confusing thus confusing hackers.