SENG2250/6250 System and Network Security
Self-Quiz Week 2, Semester 2, 2020

True/False Questions.

1. Classical cipher could be secure against statistical analysis if more complex substitution and/or permutation rules applied.

2. Block cipher takes a fixed-length input (i.e., plaintext block) and outputs a fixed-length ciphertext block.

3. Triple DES can provide 168-bit security if the three secret keys are independent.

4. AES allows three different key sizes, which are 128-bit, 196-bit, and 256-bit, respectively.

5. S-boxes of AES and DES provide non-linear transformation and increases confusion.

6. CBC mode can encrypt plaintext blocks in parallel.

7. Counter (CTR) mode can encrypt plaintext blocks in parallel.

8. Message Authentication Code (MAC) provides the same security services as digital signatures.

Short-Answer Questions

9. What is the unicity distance of the monoalphabetic substitution cipher (for English)? What does it mean?

10. What does it mean by the unforgeability and non-repudiation of a digital signature scheme?