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.
   False. No classical cipher can be secure against the statistical analysis.

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

3. Triple DES can provide 168-bit security if the three secret keys are independent.
   False. If the three keys are independent, the Triple DES can provide 112-bit security, due to the existence of the Meet-in-the-Middle attacks.

4. AES allows three different key sizes, while the plaintext block size is always 128-bit.
   True.

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

6. CBC mode can encrypt plaintext blocks in parallel.
   False. In CBC mode, a plaintext block encryption needs the ciphertext of the previous plaintext block. It has to run sequentially.

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

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

	MAC	Digital signature
Security services	• Message/origin authentication	• Message/origin authentication • Unforgeability • Non-repudiation

Short-Answer Questions

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

   Unicity distance $N_0 = \frac{\log_2 E}{\mathrm{d}}$, where $E = 26!$ and $d \approx 3.2$. We have $N_0 \approx 28$

   It means that we can find a unique key if at least 28 ciphertext letters are given.

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

    Unforgeability: it is hard to generate a signature for a particular message without the private key.

    Non-repudiation: signer cannot deny the signed message.