Spring 2024
CPSC-352 Basic Principles of Cryptography Name: ______________________________

Relevant Slides: Basic Cryptography Principles
Chapter: Chapter 1

Please note: handouts *will not* be collected and graded. However, *you are expected to complete them.* The material on the handouts is a fair game for exams, quizzes, and assignments. It is in your best interest to use handouts during lectures. The instructor will be happy to assist you.

1. What are cryptography, cryptoanalysis, and cryptology?

2. Interview Question: What is the meaning of cipher in cryptography?

a. An algorithm that performs encryption
b. An algorithm that generates a secret code
c. An algorithm that performs encryption/decryption
d. Secret code

3. Interview Question: What is a block cipher?

4. Interview Question: What is exhaustive key search?

5. How would you classify the AES-256 encryption algorithm (i.e., block or stream; and public or symmetric; and substitution, transposition, or product).

6. What are fundamental requirements for secure symmetric encryption?

7. CISSP Certification Practice Question (source: www.briefmenow.org): What is Kerckhoffs principle and why is it relevant?

a. One-time pads should be just as long as the message, otherwise patterns will be shown.
b. A public key needs to associated with an individual's identity for true non-repudiation.
c. The only secret portion to a cryptosystem should be the key so that the algorithms can be stronger.
d. More than one alphabet should be used in substitution ciphers to increase the workfactor.

8. CISSP Certification Exam Practice Question (source: wentzwu.com): Your company needs a software cipher to encrypt data symmetrically. If security is a priority and licensing and costs are also concerns, which of the following is the best acquisition source?

a. Outsourcing
b. Open Source
c. In-house Development
d. Commercial-Off-The-Shelf (COTS)

9. Use the `openssl` program in Linux to encrypt a file using AES-256 symmetric key algorithm.

10. Does symmetric cryptography provide authenticity? Explain.

11. Security+ Certification Exam Practice Question (adopted from exampremium.com): The public key is used to perform which of the following? (Select THREE).

a. Computing hashes
b. Validate the identity of an email sender
c. Encrypt messages
d. Perform key recovery
e. Decrypt messages
f. Implementing transposition ciphers

12. Illustrate how to use `openssl` to generate keys, encrypt/decrypt using AES, encrypt and decrypt using RSA, and how to use hashes, MACs, and digital signatures.