Spring 2024

CS-352 Classical Cryptology Name: ______________________________

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. **Interview Review Question:** What is cryptography?

2. **Interview Reiview Question:** What exactly are encryption and decryption?

3. **Interview Review Question:** What is plaintext or cleartext?

4. **Interview Review Question:** What is ciphertext?

5. **Interview Review Question:** How does the encryption process actually take place?

6. **Interview Review Question:** What is the goal of cryptography?

7. **Security+ Certification Practice Question:** The concept of public key cryptography was introduced by Julius Caesar. T/F?

8. **Security+ Certification Practice Question:** Even today only upto 20% of critical information being transmitted is really secure. T/F?

9. **CISSP Certification Practice Question:** What are two types of cipher?

a. Transposition and Permutation

b. Transposition and Shift

c. Transposition and Substitution

d. Substitution and Replacement

10. What are the essential ingredients of a symmetric cipher?

11. Describe how cryptographic algorithms are classified.

12. What is the difference between unconditional and computational security?

13. What is the only cipher that is unconditionally secure?

14. What is the difference between a bruteforce and a cryptoanalytic attack?

15. **CISSP Certification Practice Question:** The practice of breaking cryptosystems or obtaining plaintext from ciphertext without a key is?

16. **Interview Question:** What kinds of threats exist for a cryptographic system?

17. **Interview Question:** What are the goals of modern cryptography?

18. Explain the basic concepts of symmetric cryptography, public key cryptography, and hashing.

19. **Interview Question:** What is the Caesar cipher?

20. **Security+ Certification Practice Question:** Which of the following is true regarding Caesar's key value 3?

    a. It uses an offset value of 3 for sliding alphabets

    b. There is a difference of 3 between the alphabets when the sliding action occurs

    c. It uses three keys for encryption

    d. None of the above

21. What are the requirements for a secure symmetric cipher?

22. What is the primary objective of cryptoanalysis? Given a ciphertext, is it more important to recover the corresponding plaintext or the key used for encrypting the plaintext? Explain.

23. **CISSP Certification Practice Question:** Instance where two different keys generate the same ciphertext from a plaintext is __________?

24. **CISSP Certification Practice Question:** Kerckhoff's law: A crypto-system should be secure even if everything about the system, __________, is public knowledge.

a. except the receiver

b. except the administrator

c. except the key

d. except the network

25. **Microsoft Interview Question for Software Engineer/Developer:** Write code for Ceaser Cipher Algorithm to encrypt and decrypt messages.

Interview Question: What is polyalphabetic encryption?

26. What is the difference between a monoalphabetic and a polyalphabetic cipher?

27. Explain the cryptoanalytic process used to break the Monoalphabetic cipher.

28. Monoalphabetic cipher features a very large keyspace. Is it secure? Explain why or why not.

29. Encrypt text "`hello world`" using Vigenere cipher and keyword "`security`".

30. Encrypt text "`massachusetts`" using the Playfair cipher and key "`security`".

31. Explain the cryptoanalytic process used to break the Vigenere cipher.

32. Encrypt text "`cryptography is fun`" using Vigenere cipher with autokey and key "`dog`". Decrypt the resulting ciphertext.

33. Encrypt text "`this is a test`" using Railfence cipher and key `K = 3`. Decrypt the resulting cipher text.