Fall 2023
CS-352 Modes of Encryption Name: _____

Block Cipher Modes of Operations, Random Numbers, and Stream Ciphers
Relevant Slides: BlockCiphers.pptx
Chapters: 6 and 7

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 Question:** What is a block cipher mode of operation?

2. **Interview Question:** What block cipher modes operation are defined in NIST *Special Publication 800-38A*?

3. **Interview Question:** What are the advantages of the **ECB** mode? What are its weaknesses? What are its applications?

4. **Interview Question:** What are the advantages of the **CBC** mode? What are its weaknesses? What are its applications?

5. **Interview Question:** What are the advantages of the **CFB** mode? What are its weaknesses? What are its applications?

6. **Interview Question:** What are the advantages of the **OFB** mode? What are its weaknesses? What are its applications?

7. **Interview Question:** What are the advantages of the **CTR** mode when compared to ECB, CBC, CFB, and OFB modes? What are its applications?

8. **Interview Question:** What is the difference in security between **ECB** and **CBC**?

9. **Interview Question:** Explain the role of random numbers in cryptography.

10. **CISSP Certification Question:** Which one of the following Data Encryption Standard (DES) operating modes can be used for large messages with the assurance that an error early in the encryption/decryption process won't spoil results throughout the communication?

    a. Output Feedback (OFB)
    b. Cipher Feedback (CFB)
    c. Electronic Code Book (ECB)
    d. Cipher Block Chaining (CBC)

11. What is a pseudo-random number generator (PRNG)?

12. What are the main advantages of the Linear Congruential Generator (LCG)?

13. Set up your own LCG and use it to generate a sequence of the first 5 random numbers.

14. What criteria do we use when choosing values of LCG parameters? In the previous question, evaluate the parameters you chose based on the aforementioned criteria.

15. Is the following a good choice of parameters for LCG: $X_0 = 27$, $a = 17$, $c = 43$, and $m = 100$? Illustrate why or why not.

16. What are the weaknesses of LCG?

17. Explain the step-by-step process used by the Blum Blum Shub (BBS) PRNG to generate random bits.

18. Generate the first 10 bits using the BBS PRNG where $p = 7$, $q = 11$, and $s = 5$.

19. Are the following parameters valid for use in the BBS PRNG: $p = 47$ and $q = 31$? Explain.

20. What are the strengths of BBS PRNG? What are its weaknesses? Give an example of an application for which BBS PRNG is well suited.

21. Explain how block ciphers can be used as PRNGs.

22. Explain the process used by ANSI X9.17 PRNG random number generator to generate random numbers. Why is it so difficult to compromise?

23. ANSI X9.17 PRNG is arguably the most secure PRNG. Explain the practical limitations of ANSI X9.17 PRNG. That is, are there applications for which ANSI X9.17 PRNG is not particularly well suited?

24. What is the difference between PRNG and a true random number generator (TRNG)?

25. TRNGS may produce sequences of random numbers that are "skewed". Explain what this means. How can the issue of skewness in TRNGs be addressed?

26. What advantage do stream ciphers have over block ciphers?

27. **Interview Question:** Analyze advantages and disadvantages of different encryption placement strategies.

28. **Interview Question:** What sort of applications would most benefit most end-to-end encryption?

29. **Interview Question:** What sort of applications would most benefit from link encryption?

30. **Interview Question:** Explain the basic approach for defeating traffic analysis.

31. **Interview Question:** What is key distribution? Why is it important?

32. **Interview Question:** What are the three common ways of distributing an encryption key? Analyze the advantages and disadvantages of each approach.

33. **Interview Question:** Consider a network with n users. Each user wants to be able to securely communicate with all other users using symmetric encryption. How many symmetric keys are needed? How many symmetric keys are needed if a key distribution authority (KDC) scheme is used where each user shares a unique master key with the KDC?

34. Interview Question: Explain each step of the key distribution scenario discussed in class. Be sure to address the importance of each step.