Fall 2023
CS-352 Block Cipher Concepts, DES, and TwoFish Name: _____
Relevant Slides: BlockCipersDESAndTwoFish_V2.pptx
Chapter: Chapter 3

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. **Review Question:** Decrypt `CPGPIOSFRTRHSOTFYOAYCLU` using the Railfence cipher and key `K = 3`.

2. **Interview Question:** Explain the term *block cipher*.

3. What are the properties of a secure block cipher operation? How are are they usually achieved in practice?

4. **CISSP Certification Preparation Question:** Rearranging the plaintext is called?

   a. Confusion
   b. Diffusion
   c. Substitution
   d. Permutation

5. **Interview Question:** What is the requirement for a reversible block cipher?

6. Consider an n-bit block ideal block cipher. What is the key size? Explain your answer.

7. Why is ideal cipher not practical for use in everyday security applications?

8. Interview Question: What is *Feistel Cipher*?

9. Interview Question: What is an iterated block cipher?

10. Why is the Feistel Cipher more practical than the ideal block cipher?

11. Explain how the Feistel cipher achieves substitution and permutation?

12. Explain how the Feistel cipher achieves confusion and diffusion?

13. Interview Question: Explain how Data Encryption Standard (DES) employs Feistel cipher design principles.

14. Consider bit string s = `10101110011000011100011101001111101110011100110001100100000111010`. What is the output of IP(s) (where IP(s) is the DES initial permutation function)?

15. Consider DES key K = `01100001110111011011110111000011101001101011010010101111100101011`. What is PC-1(K)?

16. How will DES key K be rotated in the 8^{th} stage of the DES algorithm?

17. How does DES achieve *confusion*?

18. What will be the output after passing string `010010111001110101001100010011001110011101111111` through the DES S-Boxes.

19. Describe the principles that underpin the design of DES S-Boxes?

20. How does DES achieve *diffusion*?

21. Interview Question: Has DES been broken?

22. What is the basic problem with using DES in the modern world? How is the problem solved?

23. Why is double DES encryption not significantly more secure than a single DES encryption?

24. Interview Question: What is Triple-DES (3DES)?

25. Security+ Certification Practice Question: 3DES is based on which of the following?

a. Hashing algorithm

b. Symmetric key-based algorithm

c. Asymmetric key-based algorithm

d. None of these

26. When using triple DES, why do we use E-D-E (i.e., encrypt, decrypt, encrypt) sequence instead of E-E-E?

27. Interview Question: What is differential cryptonalysis?

28. Interview Question: What is linear cryptoanalysis?

29. Is DES susceptible to *differential cryptoanalysis?* Explain.

30. Is DES susceptible to *linear cryptoanalysis?* Explain.

31. What cipher was officially chosen to replace DES?