Fall 2023
CS-352 Advanced Encryption Standard Name: _____
Chapter: Chapter 5

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:** Why was a replacement for DES needed?

2. **Interview Question:** What are some advantages that the Advanced Encryption Standard (AES) has over DES?

3. **Interview Question:** AES is a _____-bit block cipher which can work with _____-bit, _____-bit, and _____-bit keys. This is different from DES which only works with _____-bit blocks and _____-bit keys (where only _____-bits of the key are actually used).

4. **Interview Question:** Is AES based on the Feistel Cipher? Explain.

5. **Security+, PenTest+, CISSP, CySA Question:** Which one of the following is a key size not supported by AES?

   a. 128

   b. 512

   c. 192

   d. 256

6. **Security+ Certification Question:** An organization needs an encryption method that supports 256-bit keys. Which of the following approaches would an organization use?

   a. DES

   b. 3DES

c. RC4

d. AES

7. Security+ Certification Question: Which of the following algorithms encrypts data in 64-bit blocks?

a. AES

b. DES

c. Twofish

d. RC4

8. Consider the following 128-bit plaintext block `FA 41 4D FF 14 37 33 3C 67 78 89 EC 89 6A BD D6`. Rewrite the block as a 4x4 matrix using the column major format in order to obtain the initial AES "state".

9. Consider the 128-bit key `56 73 94 FD 40 D4 54 D5 B3 70 3A A6 45 7A 04 BD`. Write the key as a 4 x 4 matrix using column major format. XOR the key matrix with the state in the previous question.

10. Perform the AES `SubByte` transformation on the following state matrix: $\begin{bmatrix} DC & AE & 78 & 90 \\ 45 & 10 & 89 & EF \\ 46 & DC & 32 & AA \\ 56 & DF & 84 & BF \end{bmatrix}$.

11. Perform the AES `ShiftRows` transformation on the following state matrix: $\begin{bmatrix} AE & DC & EF & FF \\ 04 & 21 & 19 & 9A \\ 65 & AD & 83 & BA \\ 19 & DD & 71 & 93 \end{bmatrix}$.

12. Multiply the following 4x4 matrices (do not actually evaluate your answers). All numbers are hexadecimal.

$$\begin{bmatrix} 1 & 1 & 2 & 2 \\ 1 & 1 & 2 & 2 \\ 1 & 1 & 2 & 2 \\ 0 & 0 & 1 & 1 \end{bmatrix} \times \begin{bmatrix} 0 & 1 & 0 & 1 \\ 2 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 2 \end{bmatrix}$$

13. In the AES `MixColumns` transformation, what matrix is multiplied by the state?

14. Compute the product of

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \times \begin{bmatrix} EA & 76 & 33 & 56 \\ 67 & 89 & 12 & BA \\ 02 & 89 & 43 & 96 \\ 03 & 1A & 26 & 08 \end{bmatrix}$$

in the finite field $GF(2^8)$ as done in the AES `MixColumns` step.

15. Convert the 128-bit AES key `0F 15 71 C9 47 D9 E8 59 0C B7 AD D6 AF 7F 67 98` into a vector of four 4-byte words: $\begin{bmatrix} w_0 & w_1 & w_2 & w_3 \end{bmatrix}$.

16. What round constant is used in the 8^{th} round of AES?

17. Using the key in the question preceding the previous question, derive the key vector $\begin{bmatrix} w_4 & w_5 & w_6 & w_7 \end{bmatrix}$ to be used in the next stage.

18. **Interview Question:** In DES, the decryption algorithm is similar to the encryption algorithm; decryption is identical to encryption, except the round keys are applied in the reverse order. Explain why this is so. Is the same true of AES? i.e., is the decryption process similar to the encryption process?