4 Cryptography Goes Digital

Exercises

Notes:

1. Remember to check the types of input control or input box used for answers in multiple choice questions. If radio buttons are used it means you need to select the one best answer. If check boxes are used then there will be more than one correct answer.

2. Some questions have extra instructions for entering your answers. This guidance is provided because Canvas is very particular about short answer questions, and will only mark your answers as correct if they are an exact match for the expected answer(s). If you want Canvas to automatically grade your answers you must follow this guidance. If Canvas marks one of your answers as incorrect because you didn't follow the extra guidance, but you feel your answer is correct, you will have to send me an email so I will know to manually check your answer.

---

1. Is ASCII the only way to encode text to binary?
    a. Yes
    b. No
    c. It was prior to 1980
    d. It was until the introduction of XML

2. True or False. The International Standards Organization (ISO) recognizes ASCII as the standard for converting between text characters and binary numbers.

3. What is the decimal equivalent of the binary number 0011 1010? If you want Canvas to grade your answer enter your answer as a number. For example, if the answer is **1** enter **1**. Do not enter **one** or **"one"**.

4. What is the decimal equivalent of the binary number 1000 0001? If you want Canvas to grade your answer enter your answer as a number. For example, if the answer is **1** enter **1**. Do not enter **one** or **"one"**.

5. What is the binary equivalent of the decimal number 17? If you want Canvas to grade your answer enter your answer as a number in 4 bit sections, with a single space between each section. Also include any leading zeros. For example, if the answer is **0001 1111** enter **0001 1111**. Do not enter **00011111** or **11111**.

6. What is the binary equivalent of the decimal number 133? If you want Canvas to grade your answer enter your answer as a number in 4 bit sections, with a single space between each section. Also include any leading zeros. For example, if the answer is **0001 1111** enter **0001 1111**. Do not enter **00011111** or **11111**.

7. Assume that you want to convert the text string **July** to ASCII. What is the correct representation of this text if the ASCII is displayed as decimal numbers? If you want Canvas to grade your answer enter your answer as decimal numbers with a single space between each number. For example, if the answer is **12 34 154** enter **12 34 154**. Do not enter **1234154** or **12 34 154**.

8. Assume that you want to convert the text string **I am done** to ASCII. Which of the following is the correct representation of this text if the ASCII is displayed as decimal numbers?
    a. 73 32 97 109 32 100 111 114 107
    b. 73 95 97 109 95 100 111 110 101
    c. 73 32 98 101 32 100 111 110 101
    d. 73 32 97 109 32 100 111 110 101

9. What is the text equivalent of the ASCII string **110 117 109 101 114 111 32 117 110 111**? If you want Canvas to grade your answer enter your answer using the exact case and spaces specified by the ASCII codes.

10. What is the text equivalent of the ASCII string **69 100 117 99 97 116 111 114**? If you want Canvas to grade your answer enter your answer using the exact case and spaces specified by the ASCII codes.
    a. Educated
    b. Educator
    c. Edifices
    d. Editors

11. Match each of the calculations with the correct result. Note that $\oplus$ is the symbol for the XOR operator. Also note that some answers may be used more than once.

    a. 1001 0001 $\oplus$ 0010 1010

b. 1101 0111 $\oplus$ 0010 1010

c. 1000 1001 $\oplus$ 0011 1010

d. 0100 1000 $\oplus$ 1111 1011

e. 0100 1110 $\oplus$ 1111 1011

12. Assume that you have captured a string of bits that has been enciphered using the XOR function. The encrypted bits are 010. Which of the following could be the possible plain text bits?
    a. 000
    b. 001
    c. 010
    d. 011
    e. 100
    f. 101
    g. 110
    h. 111
    i. Any of the above are possibly correct.

13. Why is the XOR function used to replace the Vigenère table in the Vernam cipher instead of the AND or OR functions?
    a. Because, of the three functions, XOR is the only function that has two ways to end up with cipher bits of 1 and two ways to end up cipher bits of 0, which means it's the only function that can be reversed and used for decryption.
    b. Because it is more efficient and processes faster than the other two functions.
    c. Because of the three functions, it is the only one that can be used on any type of binary data, including images and videos.
    d. Because of the three functions, it is the only one that can be used with bits generated by a PRNG.
    e. All of the above
    f. None of the above

14. Why is the AND function not a good alternative for replacing the Vigenère table in the Vernam cipher?
    a. Because there are three ways to end up with a cipher text bit value of 0, which means that even with the key there's no way to determine the value of the plain text bit.
    b. Because there are three ways to end up with a cipher text bit value of 1, which means that even with the key there's no way to determine the value of the plain text bit.
    c. Because performing the AND function on two sets of bits is computationally inefficient and takes too long.
    d. The main assumption of the question is wrong because the AND function is actually a good alternative for replacing the Vigenère table in the Vernam cipher.

15. Assume that you have been given the following set of bits, **1000**, that are the result of an AND operation. You have also been told that one set of bits used in the AND operation is **1011**. What are the other bits that were used in the AND operation? That is, given that *nnnn* AND 1011 = 1000 find *nnnn.* Hint – there may be more than one correct answer.
    a. 1111
    b. 1011
    c. 1000
    d. 1100
    e. 0011
    f. None of the above

16. Assume you have been given a string of binary data that has been encrypted using the XOR function with a key of **0110**. How the decryption performed?
    a. AND the enciphered bits with the key 0110.
    b. AND the enciphered bits with the key 1001.
    c. OR the enciphered bits with the key 0110.
    d. OR the enciphered bits with the key 1001.
    e. XOR the enciphered bits with the key 0110.
    f. XOR the enciphered bits with the key 1001.
    g. Decrypting the message is not possible if it was encrypted with XOR.

17. Use the Vernam cipher to encrypt the four character text string **Page** using the key 1100. Enter the enciphered bits as your answer. Repeat the key bits as many times as necessary to encipher the entire string. If you want Canvas to grade your answer enter your answer in 4 digit sections and include all leading zeros. That is, if the answer is **01100001** enter **0110 0001**. Do not enter **110 0001** or **01100001**.

18. The binary data **1000 1111 1000 1110 1000 1111** has been encrypted using the Vernam cipher with a key of **1100**. What is the plain text? If you want Canvas to grade your answer enter the text in the correct case, and with the correct number of spaces if there are any spaces.

19. Use the random walk program at the site to determine which of the following seeds produces pseudo random numbers that take the longest amount of time to devolve into a pattern: https://www.khanacademy.org/computing/computer-science/cryptography/crypt/pi/random-walk-exploration
    a. 456789
    b. 6574839201
    c. 112233445566
    d. 314159265
    e. 3141592653589

20. Assume that you are working with PRNG that uses the following algorithm.

    $X_{n+1} = (787\ \ X_n)\ \text{MOD}\ 2^4$

    What is the largest number that can be generated by this algorithm? If you want Canvas to grade your answer enter your answer as a number. For example, if the answer is **1** enter **1**. Do not enter **one** or **"one"**.

21. Assume that you are working with an LCG algorithm that uses the following values for the *a*, *c*, and *m* constants.

    a = 87253764234
    c = 11332244
    m = 5

    What is the largest number that can be generated by this algorithm? If you want Canvas to grade your answer enter your answer as a number. . For example, if the answer is **1** enter **1**. Do not enter **one** or **"one"**.

22. Which of the following is currently recommended for use as a CPRNG/ CSPRNG?
    a. ELF (Encino, Latimer and Falk)
    b. Blum Blum Shub
    c. Drip Drop Boom
    d. SlipSlap
    e. Verity
    f. None of the Above

23. Assume you have some text that was encrypted with a Vernam cipher, using a CPRNG/CSPRNG to generate the bits for the one time pad. What information needs to be shared with the recipient to allow them to read the message?
    a. The type of XOR function was used to encrypt the data.
    b. All of the bits in the one time pad.
    c. The ASCII codes for the characters in the keyword.
    d. The type of truth table used to replace the Vigenère table.
    e. The encrypted text.
    f. The seed for the CPRNG/CSPRNG.
    g. None of the above

24. Which of the following is true?
    a. Messages encrypted with a Vernam cipher and one time pad are more secure than messages encrypted with a Vigenère cipher and a one time pad.
    b. Messages encrypted with a Vigenère cipher and one time pad are more secure than messages encrypted with a Vernam cipher and a one time pad.
    c. Messages encrypted with a Vernam cipher and one time pad are equally as secure as messages encrypted with a Vigenère cipher and a one time pad.
    d. None of the above are true.

25. What information is used to control the sequence of numbers or sequence of bits generated by a PRNG? That is, assume you need to regenerate the same sequence of random numbers at a later date. Which of the following would you provide to the PRNG to get it to produce the same sequence?
    a. The values of the a and b constants.
    b. The seed.
    c. The size of the keyspace.
    d. The key used to generate the XOR truth table.
    e. The size of the XOR truth table.
    f. None of the above.