1 What is Cryptology?

These are the same homework questions as you will find in Canvas. You can use this document to determine your answers before starting the homework in Canvas, but you **must** enter your answers in Canvas to receive credit.

Notes on mechanics of entering answers in Canvas:

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.

Exercises

1. True or False – Most modern computer systems have cryptographic functions "built-in" to their OS code.

2. Assume you are responsible for device and network security at a company with many employees. All your servers are running on a cloud provider. You ensure that all accounts and sensitive data are password protected, and you have strong password rules in place. You keep all systems up to date with patches and updates. Which of the following is most likely to be the source of security issues?
   a. Poorly written cryptographic algorithms built into the OS
   b. Poor security practices by users
   c. Physical security breaches
   d. Nation-state attacks

3. Which of the following is the overarching science of secret writing?
   a. Arcanology
   b. Steganography
   c. Cryptography
   d. Cryptanalysis
   e. Cryptology
   f. Stegadology

g. None of the above

4. Which of the following protects unscrambled text by hiding it but leaving the text unchanged?
   a. Cryptology
   b. Steganography
   c. Cryptography
   d. Cryptanalysis
   e. None of the above

5. Which of the following is the study of methods to protect text by scrambling the characters?
   a. Cryptology
   b. Steganography
   c. Cryptography
   d. Cryptanalysis
   e. None of the above

6. Which of the following is the study of methods for breaking encryption or encoding schemes?
   a. Cryptology
   b. Steganography
   c. Cryptography
   d. Cryptanalysis
   e. None of the above

7. Which of the following provides assurance that a message has been unaltered during transmission?
   a. Confidentiality
   b. Integrity
   c. Availability
   d. Authentication
   e. Non-repudiation
   f. Repudiation
   g. Assurance
   h. Insurance

8. Which of the following can be provided by cryptology?
   a. Confidentiality
   b. Integrity
   c. Availability
   d. Authentication
   e. Non-repudiation

9. Which of the following prevent a sender from denying they sent the message?
   a. Confidentiality
   b. Integrity
   c. Availability
   d. Authentication
   e. Non-repudiation

f. None of the above

10. Which part of the CIA triad is NOT provided by cryptology? If you want Canvas to grade your answer enter your answer in all lower case.

11. What is ASCII value for the letter A? Note that this is upper case A, not lower case. Give the **hex** value, not the decimal value. If you want Canvas to grade your answer enter your answer in lower case with no spaces between the hex digits. For example, if the answer is 9F enter 9f. Do not enter 9 f.

12. Which of the following is the binary or base 2 equivalent of the decimal number 7? Note that the smallest value in the binary number is on the right.
    a. 1001
    b. 0101
    c. 1111
    d. 1110
    e. 0111
    f. None of the above.

13. Which of the following are true regarding prime numbers?
    a. All even numbers are prime.
    b. All odd numbers are prime.
    c. There are an infinite number of prime numbers.
    d. Prime numbers only have two factors, 1 and the prime number itself.
    e. Prime numbers only have an odd number of factors.
    f. Computers can quickly calculate the prime factors of any number, no matter how large the number.
    g. Calculating the prime factors of large numbers is time consuming. Even modern (non-quantum) computers take a significant amount of time to perform the calculations.
    h. None of the above.

14. What are the prime factors for the number 299? Give the two prime factors that are not 1 or 299. If you want Canvas to grade your answer enter your answer a single space between the numbers. Do not use a comma or any other delimiter. For example, if the answer is 345 and 23 enter 345 23. Hint – this is probably hard to do by hand, so find a web site that will do the calculation for you.

15. (This question requires the use of Boolean logic.) Assume you have two statements S1 and S2. For example, S1 might be “I love math”, and S2 might be “Tony likes pizza”. If S1 is true and S2 is false, what would be the result of S1 AND S2?
    a. True
    b. False
    c. There's not enough information to determine the correct answer.

16. In traditional cryptographic examples, who are the two people that are typically trying to exchange a secret message?
    a. Alice
    b. Alexis
    c. Bob
    d. Bruce

e. Chris
f. Doug
g. Eve
h. Mike
i. Zelda
j. None of the above

17. True or False. In the United States, the use of encryption by private citizens cannot be regulated by the government as this would be an infringement on the right to privacy which is guaranteed by the Bill of Rights.
    a. True
    b. False

18. Write a short summary of the Clipper Chip. What was it, and what was it supposed to accomplish? You may have to do some research on the Clipper Chip to see how it was supposed to function. You'll probably need a paragraph or two, but if you have more than 5 paragraphs, you're writing too much as this question is only worth 3 points. Make sure and answer the following questions in your summary:

    a. How was the Clipper Chip supposed to function?

    b. Do you feel the Clipper Chip proposal was a good compromise between allowing the use of cryptology for privacy purposes and providing access to encrypted information for agents of law enforcement? There's not a correct answer to this question, I'm just looking for your opinion.