6 Symmetric Cryptography: Block Ciphers

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. Which of the following is true regarding block ciphers?
    a. They are symmetric
    b. They are asymmetric
    c. They eliminate the need for the use of a shared key
    d. Block ciphers are not as secure as stream ciphers
    e. Block ciphers are more secure than stream ciphers
    f. All of the above

2. What happens to data in an S-Box?
    a. The data in each cell of the block is swapped with data in a different cell. The overall data will be the same, but it will be located in different cells.
    b. The data in each cell of the block is transformed to a different value using a lookup table.

c. The data in each cell is used as a seed for a pseudo random number generator.
d. The data in each cell is XORed with the key.
e. None of the above.

3. What happens to data in a P-Box?
    a. The data in each cell of the block is swapped with data in a different cell. The overall data will be the same, but it will be located in different cells.
    b. The data in each cell of the block is transformed to a different value using a lookup table.
    c. The data in each cell is used as a seed for a pseudo random number generator.
    d. The data in each cell is XORed with the key.
    e. None of the above.

4. Assume that you are working with a SPN cipher. What happens in a round?
    a. All of the plain text bits are assigned to a block.
    b. All of the sub keys are generated by XORing the key with numbers from the PRNG.
    c. Either all of the S-Box processing occurs, or all of the P-Box processing occurs.
    d. A block of data is processed by an S-Box and then processed by a P-Box.

5. Which of the following is used to create diffusion in an SPN cipher?
    a. S-Box
    b. P-Box
    c. KSA
    d. Diffusion does not occur in an SPN cipher.

6. Which of the following is used to create confusion in an SPN cipher?
    a. S-Box
    b. P-Box
    c. KSA
    d. Confusion does not occur in an SPN cipher.

7. Which of the following sub-divides each block of data into two pieces during the encryption process?
    a. Substitution-Permutation Networks
    b. Feistel Network
    c. Lai–Massey Cipher
    d. Electronic Code Book
    e. Cipher Block Chaining
    f. Counter Mode
    g. Cipher Feedback Mode
    h. Output Feedback Mode

8. For each of the following, identify whether it is one of the 3 main block cipher algorithms, one the 5 Modes of Operation used for chaining the processing of blocks, an implementation of a block cipher, or none of the above.
    a. Blowfish
    b. Substitution-Permutation Networks
    c. P-Box
    d. Lai–Massey Cipher
    e. Electronic Code Book

f. PRF
g. Data Encryption Standard
h. Nonce
i. Lucifer

9. Which cipher was selected by NBS/NIST to be the Data Encryption Standard? Note – If you want Canvas to grade your answer enter it in all lower case. Only use a single space between words if there are multiple words. For example if the answer is Stevie Ray Vaughan enter stevie ray Vaughan, not Stevie Ray Vaughan or Stevie Ray Vaughan, or stevierayvaughan.

10. Which cipher was selected by NBS/NIST to be the Advanced Encryption Standard? Note – If you want Canvas to grade your answer enter it in all lower case. Only use a single space between words if there are multiple words. For example if the answer is Stevie Ray Vaughan enter stevie ray Vaughan, not Stevie Ray Vaughan or Stevie Ray Vaughan, or stevierayvaughan.

11. Which of the following Modes of Operation should not be used as it produces identical blocks of cipher text for blocks of plain text that contain identical data?
    a. Electronic Code Book
    b. Cipher Block Chaining
    c. Counter Mode
    d. Cipher Feedback Mode
    e. Output Feedback Mode

12. Which of the following Modes of Operation has/have no chaining between blocks, which allows multiple blocks to be processed in parallel?
    a. Electronic Code Book
    b. Cipher Block Chaining
    c. Counter Mode
    d. Cipher Feedback Mode
    e. Output Feedback Mode

13. Which of the following Modes of Operation turn a block cipher into a stream cipher?
    a. Electronic Code Book
    b. Cipher Block Chaining
    c. Counter Mode
    d. Cipher Feedback Mode
    e. Output Feedback Mode

14. Which of the following ciphers is the most widely used in modern encryption?
    a. RC4
    b. ChaCha20
    c. DES
    d. 3DES
    e. AES
    f. SSL/TLS
    g. None of the above

15. Which of the following is/are true regarding AES?
    a. NIST now considers it obsolete and has replaced it with 3DES.
    b. It uses an XOR function with a PRNG so it provides perfect security. Plus, since it processes data in blocks it solves the key exchange problem.
    c. It uses an XOR function with a PRNG so it provides perfect security. Plus, since it uses the Cipher Feedback (CFR) Mode of Operation it solves the key exchange problem.
    d. It uses an XOR function with a PRNG so it provides perfect security. Plus, since most modern CPUs have built-in support for AES exchanging the symmetric key is no longer a problem.
    e. It uses an XOR function with a PRNG so it provides perfect security. However, since it's a symmetric cipher key exchange is still an issue.
    f. None of the above

16. Decrypt the cipher text in the file **HW6Q14.hex**. It has been encrypted with the AES cipher using a 128 bit key. The key has been encrypted using the Caesar cipher, or a rotation cipher that rotates 3 places. Decrypt the key, and use the first 128 bits or 16 characters as the decryption key. The plain text contains instructions for doing something. What activity is covered in the plain text?

    Help and hints:
    - The encrypted key is available in the file **HW6Q14-Key.txt**
    - Only the first 128 bits of the key are required. This is 16 characters.
    - Use Cryptool to perform the AES decryption
    - You will have to convert the key to the ASCII hex values to use it in Cryptool. Use an online tool to accomplish this.
    - The cipher text is available in the file **HW6Q14.hex**.

    a. Playing the guitar
    b. Growing dreadlocks
    c. Changing a flat tire
    d. Using Cryptool
    e. Repairing a garbage disposal
    f. Grilling salmon
    g. Passing a lie detector test
    h. Installing a video card in a computer
    i. Teaching a dog to sit
    j. Setting up a Vive VR headset
    k. Buying a pumpkin pie at Costco and making it look like you baked it

17. Which of the following are true regarding a salt or seed as they are used in a block cipher that chains together the encryption of the blocks?
    a. This is a number that is used within the encryption process (SPN, Feistel, Lai–Massey).
    b. This is a number that is used by the key scheduling algorithm.
    c. This is a number that will increment for each block in the message.
    d. This number will remain fixed for every block in the message.
    e. This number must be passed to the recipient so they can decrypt the cipher text.
    f. It is not necessary to pass this number to the recipient as it always reset to its initial value it at the start of the decryption process.

18. Which of the following are true regarding a nonce as it is used in a block cipher that chains together the encryption of the blocks?
    a. This is a number that is used within the encryption process (SPN, Feistel, Lai–Massey).
    b. This is a number that is used by the key scheduling algorithm.
    c. This is a number that will increment for each block in the message.
    d. This number will remain fixed for every block in the message.
    e. This number must be passed to the recipient so they can decrypt the cipher text.
    f. It is not necessary to pass this number to the recipient as it always reset to its initial value it at the start of the decryption process.

19. Create and upload a screenshot showing the cipher suites supported by your browser. This must show all the cipher suites that the browser supports, not just the suite negotiated with any particular web server. To receive credit, the screenshot you upload must be a .jpg or .png, or you can paste the image into a word document and upload the word document.