5 Symmetric Cryptography: Stream Ciphers

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 uses the same key to decrypt a message that was used to encrypt it?
    a. Symmetric key cryptography
    b. Asymmetric key cryptography
    c. Stream ciphers
    d. Block ciphers
    e. Vernam ciphers
    f. All of the above

2. Which of the following uses one key for encryption and a different key for decryption?
    a. Symmetric key cryptography
    b. Asymmetric key cryptography
    c. Stream ciphers
    d. Block ciphers
    e. Vernam ciphers
    f. All of the above

3. True or False. All substitution ciphers are asymmetric.
    a. True
    b. False

4. Which of the following is true regarding Vigenere ciphers?
    a. They are all symmetric.
    b. They are all asymmetric.
    c. They are symmetric if the key is as long as the plain text. If the key is shorter than the plain text they are asymmetric.
    d. They are symmetric if the key is shorter than the plain text. If the key is longer than the plain text they are asymmetric.
    e. They are neither symmetric nor asymmetric as they belong to a different class of ciphers.

5. True or False. All symmetric ciphers are stream ciphers.
    a. True
    b. False

6. What group or family of ciphers is RC4 a member of?
    a. Asymmetric and Stream
    b. Asymmetric and Block
    c. Symmetric and Stream
    d. Symmetric and Block
    e. None of the above

7. What group or family of ciphers is ChaCha20 a member of?
    a. Asymmetric and Stream
    b. Asymmetric and Block
    c. Symmetric and Stream
    d. Symmetric and Block
    e. None of the above

8. Which of the following provides the best definition of a stream cipher?
    a. A cipher that uses one key to encrypt a message and a different key to decrypt the same message.
    b. A cipher that encrypts one character or one bit at a time.
    c. A cipher that encrypts multiple characters or bits at the same time.
    d. A cipher that uses a nonce.
    e. A cipher that has it’s own PRNG algorithm.
    f. None of the above.

9. Which of the following provides the best definition of the Salsa20/ChaCha20 ciphers?
    a. They are block ciphers because they generate the keystream using a block of data.
    b. They a considered hybrid ciphers, both block and stream, because they generate the keystream using a block of data while they encrypt the plain text one bit at a time.
    c. They a considered stream ciphers because they perform the encryption and decryption one bit at a time.
    d. They are asymmetric ciphers which are neither block nor stream.
    e. None of the above

10. Which of the following is/are true regarding RC4 and WEP?
    a. WEP uses RC4 with a 2048 bit key which makes it nearly uncrackable. This makes WEP the best choice for a wireless protocol.
    b. WEP uses an implementation of RC4 that only uses a 40 bit key and 24-bit IV, making it relatively simple to crack.
    c. WEP reuses the RC4 keys, making it relatively simple to crack.
    d. None of the above.

11. Which of the following is true regarding the differences between RC4 and Salsa20/ChaCha20?
    a. They both use the same PRNG, however RC4 performs encryption and decryption using the MOD function while Salsa20/ChaCha20 use the XOR function.
    b. They both use exactly the same PRNG code and encryption code, however RC4 allows a variable size key while Salsa20/ChaCha20 require the key to be 2048 bits.
    c. They both use the same PRNG and encryption code, however Salsa20/ChaCha20 adds a nonce to the key to prevent patterns from developing.
    d. None of the above.

12. In the Salsa20/ChaCha20 ciphers, what is the difference between a counter and a nonce?
    a. The counter is controlled and incremented by the encryption program, once for each message; while the same nonce is always used.
    b. The counter is controlled and incremented by the encryption program, once for each message; while the same nonce is a number that is generated from a true random source.
    c. The counter starts as a new true random number each time the encryption program starts. It is then incremented each time the PRNG generates a block of key stream bits. The nonce is also a true random number that is generated each time the encryption program starts, however it remains the same while an entire message is encrypted or decrypted.
    d. The counter and the nonce are both generated and controlled by the encryption program. The counter is reset to zero at the start of each new message and incremented each time the PRNG generates a block of key stream bits. The nonce is incremented when the encryption program starts, and the same nonce is used to encrypt or decrypt an entire message.
    e. There is no difference. They are just different terms for the same thing.

13. Which of the following ciphers uses a nonce in the PRNG?
    a. All symmetric ciphers
    b. All asymmetric ciphers
    c. All stream ciphers
    d. All block ciphers
    e. RC4
    f. Salsa20 and ChaCha20
    g. None of the above

14. What is the main purpose of the nonce in the Salsa20/ChaCha20 cipher?
    a. To ensure that the key is long enough to prevent the message from being cracked by brute force.
    b. To add enough bits to the block or matrix used to generate the keystream to ensure that it is 8 bytes x 8 bytes.
    c. To ensure that the cipher text has a signature that allows the recipient to know the cipher text was encrypted by Salsa20 or ChaCha20.
    d. To ensure that even if the same key is used with multiple messages, the key stream generated by the PRNG will be different.
    e. None of the above

15. True or False. RC4 is considered a block cipher because it's PRNG works on a block of 256 characters to generate the keystream.
    a. True
    b. False

16. Assume a message has been encrypted using RC4. In addition to the cipher text, what information will the recipient need to decrypt the message?
    a. The key
    b. The size of the key array
    c. The initial value of the PRNG counter
    d. The nonce value

17. Assume a message has been encrypted using Salsa20 or ChaCha20. In addition to the cipher text, what information will the recipient need to decrypt the message?
    a. The key
    b. The size of the key array
    c. The initial value of the PRNG counter
    d. The nonce value

18. Encrypt the following text with the RC4 cipher using a 40 bit key of "cyber". Note that the key text is all lower case, and should not include the quotes. The text is available in the file **H5Q18.txt**. What are the first 4 hex values for the cipher text? Note – If you want Canvas to grade your answer enter it as a single 4 digit hex number, using all upper case for any values A-F. That is, if the answer is 5A D7 enter 5AD7. Do NOT enter 5aD7 or 5A D7 etc.

```
Will you have whiskey with your water
Or sugar with your tea
What are these crazy questions
That they're asking of me
This is the craziest party
That there ever could be
Oh, don't turn on the light
'Cause I don't want to see
Mama told me not to come
Mama told me not to come
That ain't the way to have fun
```

19. Assume that you are trying to use the Cryptool utility to break a message that has been encrypted with RC4 using a 40 bit key. You start the analysis using the default settings. Roughly how long will the Cryptool take to complete the analysis?
    a. It breaks the message almost instantaneously.
    b. Less than one hour
    c. More than an hour but less than one day
    d. More than one day but less than 100 days
    e. More than 100 days but less than 1 year
    f. More than 1 year but less than 50 years
    g. More than 50 years
    h. Messages encrypted with RC4 and a 40 bit key cannot be broken.

20. Decrypt the following hex data. It has been encrypted with the RC4 cipher using a 32 bit key of “tony”. Note that the key text is all lower case, and should not include the quotes. The text is available in the file **H5Q20.hex**. The text mentions one person’s name or character’s name several times. Who is mentioned the in the decrypted text? 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, nor Stevie Ray Vaughan, nor stevierayvaughan.

```
A6 1A D1 A6 6D BA 67 E5 CA 84 6D E4 CA BF 82 87 0F F3 F1
80 4D 0C 79 21 C5 66 14 A2 92 97 86 EC B0 D7 E2 FA 36 C6
DA 2F 5A DA D0 B6 B6 E1 31 61 6D 41 AC 27 86 24 EE D3 E0
3E 42 29 F8 4A 84 46 10 AF 58 C3 3A A8 B5 22 41 71 1C 76
36 91 62 6D AC BC 7C 70 70 5C 7E B0 24 51 EB 49 02 AC 13
61 E1 A0 24 FB 9E D0 2E DC 21 94 E6 C5 59 4E FC 61 FC EF
25 42 EB E0 7B 83 4F 9A 62 79 EF 80 11 C9 4A 1B 3E C5 9D
F3 E8 8C D5 87 51 B9 7C 22 56 B9 36 4E 87 58 FD 54 A8 E0
DA 09 03 0B 0F F1 8D 02 B1 1D D0 F9 AE 3E 06 7D F9 BF 1E
27 75 3F 61 40 4F C9 DA 2F 0A A8 3D 85 67 25 40 65 A5 F3
D7 99 E9 BC 65 30 39 27 EE 4C C7 10 05 47 A6 AE FC D2 4E
C2 F7 88 9B F8 1F FF 3D 40 C1 FA 48 19 42 E6 AE EC C8 5E
E5 98 F4 2A 11 27 B6 62 F2 E7 45 A7 3F 00 F2 20 FD 54 45
0F 88 48 64 D1 93 1C E3 07 9C 51 A5 0B 80 58 13 5A 9F 47
14 1E BA CC BD F0 7B 7C C3 EA 8E FF FF A8 51 7E 06 03 A6
FB 6C 22 45 03 54 B8 1A 1B C9 71 71 C6 0F F5 9E 6A 90 86
0E 77 C8 10 76 3F 28 EF 7C 25 4B 42 94 58 83 E4 8B 96 BB
44 0B 1F 70 84 F1 F6 E1 9D CF DF 4C C4 D6 B9 17 8B C8 AD
50 1F 06 88 0E 9C DE 89 56 9D 75 75 27 BF A3 F3 37 B4 F4
4A 03 ED 07 2E 02 DB F4 FE 23 87 23 D7 5A E2 16 9E DD 2A
16 FD 51 BD D3 E4 88 5E ED A2 D9 B7 F6 FC 40 16 55 EF 80
4D 41 4A 99 CC 51 24 5D 54 88 9A 84 53 F9 69 AB 05 0D 01
D6 0D 21 00 1F F9 92 5E FD 23 17 AC 14 46 C1 EC 2B 47 DC
FE 8B F2 3E E9
```

21. What is the main goal of SSL/TLS?
    a. To provide standards for encrypting application data, such as database data.
    b. To provide standards for encrypting and securing network communications.
    c. To improve the performance of stream ciphers by providing a standard PRNG.
    d. None of the above

22. In what version of SSL or TLS was support for RC4 first prohibited?

    a. SSL 2.0
    b. SSL 3.0
    c. TLS 1.0
    d. TLS 1.1
    e. TLS 1.2
    f. TLS 1.3
    g. None of the above

23. Which of the following is the most correct regarding modern CPUs, stream ciphers, and block ciphers?
    a. The circuitry and instructions to process stream ciphers has been built into high end GPUs. If your computer has a graphics card it will process RC4/ChaCha20 faster than it will process a block cipher.
    b. All modern CPUs have added the circuitry and instructions to process stream ciphers. This makes stream ciphers more efficient and faster than block ciphers.
    c. A few modern CPUs have added the circuitry and instructions to process stream ciphers. Stream ciphers will be more efficient and faster than block ciphers on these CPUs. But block ciphers are faster and more efficient on CPUs that do not have the stream cipher feature.
    d. Most modern CPUs have added the circuitry and instructions to process the AES block cipher. AES will be more efficient and faster than stream ciphers on these CPUs. But stream ciphers are faster and more efficient on CPUs that do not have the AES feature.

24. Say that a stream cipher is used in TLS. How is the key exchanged between the sender and recipient?
    a. The sender and recipient open a secure connection using an asymmetric cipher and use this connection to exchange the key (and nonce if required) for the stream cipher. Once the key for the stream cipher is exchanged, they switch to the stream cipher.
    b. Stream ciphers are never used in TLS. Only block ciphers are used.
    c. The sender and recipient open a secure connection using a block cipher and use this connection to exchange the key (and nonce if required) for the stream cipher. Once the key for the stream cipher is exchanged, they switch to the stream cipher.
    d. The CPU on every computer that implements TLS has the capability of generating a key (and nonce if required) any time a stream cipher is used. When two devices open a connection using TLS their CPUs will generate the same key on both devices, eliminating the need to transmit the key.
    e. This is a trick question as only asymmetric ciphers are used with TLS.