✓ **Congratulations! You passed!**

**TO PASS** 80% or higher

Keep Learning

GRADE
100%

# Security : Encrypting and Signing

**LATEST SUBMISSION GRADE**

100%

1. Which of the following is true of security?

**1 / 1 point**

○ Perfect security is achievable and cheap

○ Perfect security is achievable but expensive

● Perfect security is unachievable and requires a trade-off with cost

○ Perfect security is unachievable but you should always choose the most expensive option

✓ **Correct**

2. What is the difference between active and passive wiretapping?

**1 / 1 point**

○ In passive wiretapping only some of the network data is altered where in active wiretapping all of the network data is altered

○ In active wiretapping the network is snooped whereas in passive wiretapping the network is altered

● In passive wiretapping the network is snooped whereas in active wiretapping the network data is altered

○ Passive wiretapping and active wiretapping are different names for network snooping

✓ **Correct**

3. Integrity is preserved if

**1 / 1 point**

○ The information you receive is probably from who you think it is and has not been modified since it was sent

○ The information you receive has not been corrupted since it was sent no matter who sent it

● The information you receive is from who you think it is and has not been modified since it was sent

○ Information you receive is from who you think it is

✓ **Correct**

4. Which of the following factors has the smallest effect on the strength of a cryptosystem?

**1 / 1 point**

● The data being transmitted

○ The key distribution technique

○ The encryption algorithm

○ The key length

✓ **Correct**

5. What is one possible advantage of public-key cryptosystems over secret-key ones?

**1 / 1 point**

○ Public-key cryptosystems can transmit more data than secret-key ones

○ Public-key cryptosystems are always more secure than secret-key ones

● Public-key cryptosystems do not have the problem of secret-key distribution

● Public-key cryptosystems do not have the problem of secure key distribution

✓ **Correct**

6. What does it mean if a cryptosystem is symmetric-key in nature? **1 / 1 point**

○ The key used for encryption is the from the key used for decryption but with a shared secret added to the end

○ The key used for encryption is the backward version of the key used for decryption

● The key used for encryption is the same as the key used for decryption

○ The key used for encryption is a shortened version of the key used for decryption

✓ **Correct**

7. The following question is encrypted using a Caesar Cipher with a shift of 13. You can use www.rot13.com to decrypt the question. **1 / 1 point**

Jub vf perqvgrq nf orvat bar bs gur vairagbef bs Rgurearg?

○ Vint Cerf

○ Tim Berners-Lee

○ Mitchell Baker

● Bob Metcalfe

✓ **Correct**

8. The following question is encrypted using a Caesar Cipher with a shift of 13. You can use www.rot13.com to decrypt the question and answers. **1 / 1 point**

Jung qbrf gur Gjvggre unfugnt #VUGF fgnaq sbe?

○ Vaqvtb, Uraan, Gnatrevar naq Fhasybjre

○ Vagreany Uvtu Grpuabybtl Fbyhgvba

○ Vagreaangvbany Uvtu Grpuabybtl Fheirl

● Vagrearg Uvfgbel, Grpuabybtl, naq Frphevgl

✓ **Correct**

9. What is the SHA-1 hash of the string below as computed by http://www.dr-chuck.com/sha1.php **1 / 1 point**

**The Transport Layer does retransmission**

● 1399edc7e55f7be8dbc7024bcb8830527722e179

○ 7024bcb8830521399edc7e55f7be8dbc7722e179

○ 7e55f7be8dbc7024bcb8830527722e1791399edc

○ 22e1791399edc7e55f7be8dbc7024

✓ **Correct**

10. What does a cryptographic hash function do? **1 / 1 point**

○ It converts input fixed-size bit strings into blocks of data

● It takes a block of data and returns a fixed-size bit string called the hash value

○ It takes a block of data and randomly changes characters to numbers

○ It computes the Hyperbolic Asymmetric Sine Harmonic (H.A.S.H.) for a sequence of audio data

✓ Correct

11. What critical element does simple digest-based Message Signing, as described in the lecture, depend upon?

1 / 1 point

● The sharing of a secret transported securely 'out of band'

○ The secret should not be longer than the message

○ The geographic proximity of the transmitter and recipient of the message

○ The message must be under 20 characters long

✓ Correct

12. What is the problem with secret key distribution via the internet?

1 / 1 point

● The communication of the secret key is insecure

○ The internet cannot handle the length of shared secret keys because they are longer than a single packet

○ There is no problem

○ The internet is too slow for sending keys

✓ Correct

13. You are going to send the message below using shared secret of **IHTS**. Use http://www.dr-chuck.com/sha1.php to compute your message digest using the technique from lecture. What will the first six characters of the digest/signature that you send along with the message?

1 / 1 point

**Be sure to drink more Ovaltine**

○ 44dbc4

○ e1c85e

○ 2b5473

● 8b4258

✓ Correct

14. Select the valid signed message from Annie if your shared secret is **IHTS**? Use http://www.dr-chuck.com/sha1.php to compute your message digests using the technique from lecture. Only the first 6 characters of the SHA1 message digest are shown below.

1 / 1 point

○ Meet me at the train station87fd2e

● Bring me cookies51be4e

○ Send money please7d47f3d4

○ It is raining5e4421

✓ Correct