Congratulations! You passed!
TO PASS 80% or higher

Keep Learning

GRADE
100%

Week Two Practice Quiz

TOTAL POINTS 14

1. Plaintext is the original message, while ____ is the encrypted message. **1 / 1 point**

- (•) Ciphertext
- ( ) Cipher
- ( ) Algorithm
- ( ) Digest

Correct
Yep! Once the original message is encrypted, the result is referred to as ciphertext.

2. The specific function of converting plaintext into ciphertext is called a(n) _____. **1 / 1 point**

- ( ) Data protection standard
- (•) Encryption algorithm
- ( ) Integrity check
- ( ) Permutation

Correct
Nice job! An encryption algorithm is the specific function or steps taken to convert plaintext into encrypted ciphertext.

3. Studying how often letters and pairs of letters occur in a language is referred to as _____. **1 / 1 point**

- (•) Frequency analysis
- ( ) Codebreaking
- ( ) Espionage
- ( ) Cryptography

Correct
Great work! Frequency analysis involves studying how often letters occur, and looking for similarities in ciphertext to uncover possible plaintext mappings.

4. True or false: The same plaintext encrypted using the same algorithm and same encryption key would result in different ciphertext outputs. **1 / 1 point**

- ( ) TRUE
- (•) FALSE

Correct
Woho! If the plaintext, algorithm, and key are all the same, the resulting ciphertext would also be the same.

5. The practice of hiding messages instead of encoding them is referred to as _____. **1 / 1 point**

- ( ) Obfuscation
- ( ) Encryption
- (•) Steganography
- ( ) Hashing

Correct
That's right! Steganography involves hiding messages from discovery instead of encoding them.

6. ROT13 and a Caesar cipher are examples of _____. **1 / 1 point**

- ( ) Steganography
- (•) Substitution ciphers
- ( ) Digital signatures
- ( ) Asymmetric encryption

Correct
Awesome! These are both examples of substitution ciphers, since they substitute letters for other letters in the alphabet.

7. DES, RC4, and AES are examples of _____ encryption algorithms. **1 / 1 point**

- (•) Symmetric
- ( ) Strong
- ( ) Weak
- ( ) Asymmetric

Correct
Exactly! DES, RC4, and AES are all symmetric encryption algorithms.

8. What are the two components of an asymmetric encryption system, necessary for encryption and decryption operations? Check all that apply. **1 / 1 point**

- [ ] Random number generator
- [x] Public key

Correct
You got it! In asymmetric encryption systems, there's a private key used for encryption, and a public key used for decryption.

- [ ] Digest
- [x] Private key

Correct
You got it! In asymmetric encryption systems, there's a private key used for encryption, and a public key used for decryption.

9. To create a public key signature, you would use the _____ key. **1 / 1 point**

- ( ) Symmetric
- (•) Private
- ( ) Public
- ( ) Decryption

Correct
Nice work! The private key is used to sign data. This allows a third party to verify the signature using the public key, ensuring that the signature came from someone in possession of the private key.

10. Using an asymmetric cryptosystem provides which of the following benefits? Check all that apply. **1 / 1 point**

- [x] Non-repudiation

Correct
That's exactly right! Confidentiality is provided by the encryption, authenticity is achieved through the use of digital signatures, and non-repudiation is also provided by digitally signing data.

- [ ] Hashing
- [x] Authenticity

Correct
That's exactly right! Confidentiality is provided by the encryption, authenticity is achieved through the use of digital signatures, and non-repudiation is also provided by digitally signing data.

- [x] Confidentiality

Correct
That's exactly right! Confidentiality is provided by the encryption, authenticity is achieved through the use of digital signatures, and non-repudiation is also provided by digitally signing data.

11. If two different files result in the same hash, this is referred to as a _____. **1 / 1 point**

- ( ) Key collision
- ( ) Mistake
- ( ) Coincidence
- (•) Hash collision

Correct
Correct! A hash collision is when two different inputs yield the same hash.

12. When authenticating a user's password, the password supplied by the user is authenticated by comparing the ____ of the password with the one stored on the system. **1 / 1 point**

- (•) Hash
- ( ) Plaintext
- ( ) Ciphertext
- ( ) Length

Correct
Yep! Passwords are verified by hashing and comparing hashes. This is to avoid storing plaintext passwords.

13. If a rainbow table is used instead of brute-forcing hashes, what is the resource trade-off? **1 / 1 point**

- ( ) Rainbow tables use less storage space and more RAM resources
- ( ) Rainbow tables use less RAM resources and more computational resources
- ( ) Rainbow tables use less storage space and more computational resources
- (•) Rainbow tables use less computational resources and more storage space

Correct
Woho! Instead of computing every hash, a rainbow table is a precomputed table of hashes and text. Using a rainbow table to lookup a hash requires a lot less computing power, but a lot more storage space.

14. In a PKI system, what entity is responsible for issuing, storing, and signing certificates? **1 / 1 point**

- ( ) Government
- ( ) Registration Authority
- (•) Certificate Authority
- ( ) Intermediary Authority

Correct
Excellent job! The certificate authority is the entity that signs, issues, and stores certificates.