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

- cipher
- algorithm
- digest
- ciphertext

Correct
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

- permutation
- data protection standard
- encryption algorithm
- integrity check

Correct
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

- cryptography
- frequency analysis
- codebreaking
- espionage

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

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

- steganography
- hashing
- encryption
- obfuscation

Correct
Steganography involves hiding messages from discovery instead of encoding them.

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

- substitution ciphers
- steganography
- asymmetric encryption
- digital signatures

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

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

- weak
- strong
- asymmetric
- symmetric

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

7. Which of the following are necessary components for encryption and decryption operations when using an asymmetric encryption system? Check all that apply. 1 / 1 point

- [x] Public key

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

- [ ] Random number generator
- [ ] Digest
- [x] Private key

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

8. To create a public key signature, use the _____ key. 1 / 1 point

- (•) private
- ( ) symmetric
- ( ) public
- ( ) decryption

Correct
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.

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

- [x] Confidentiality

Correct
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
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] Non-repudiation

Correct
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.

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

- (•) hash collision
- ( ) coincidence
- ( ) mistake
- ( ) key collision

Correct
When two different inputs yield the same hash, it is called a hash collision.