**Mod 2 Quiz Answers**

Confidentiality is one of the main tenets of information security and concentrates on which choice below?

**Encryption/decryption algorithms**

What makes the relation between the key and the ciphertext as complex as possible?

**Confusion**

This attack consists of trying every possible code, combination, or password until you find the right one.

**Brute-force Attack**

What attack is first published attack that is capable of breaking DES in less than 255 complexity.

**Differential cryptanalysis attack**

How many keys are required for two people to communicate via a asymmetric cipher?

**2**

What cipher eliminates the need to pad a message to be an integral number of blocks?

**Stream**

What is the transformation makes use of the inverse of S-box?

**Round Key**

Any encryption scheme has two inputs, enciphering and deciphering with the encryption function?

**True**

Diffusion refers to the property that the statistics structure of the ciphertext is dissipated into long range statistics of the plaintext.

**False**

Which attack scenario on ciphers below is where the attacker has only ciphertext(s).

**Ciphertext only attacks**

What has each 64-bit plaintext is mapped to respective 64-bit ciphertext, and each such possible pair represents 1 page of the codebook?

**Electronic CodeBook Mode**

What is the Forward substitute byte transformation is called?

**SubBytes**

Which attack scenario on shift ciphers below is where You know that HELLO encrypts to MJQQT?

**Known plaintext attacks**

Authenticity is one of the main tenets of information security and concentrates on which choice below?

**Digital signatures, digital certificates**

What is AES?

**Symmetric Cipher**

AES must be a symmetric block cipher with a block length of 128-bits and support for key lengths of 128, 192, and 256-bits.

**True**

The four different stages used in the AES algorithm is Substitute bytes, Shift rows, Mix columns, and add a round key.

**True**

The Data Encryption Standard (DES) is a cipher (a method for encrypting information) selected what official standard for the United States in 1976.

**Federal Information Processing Standard (FIPS)**

Which choice below best describes Kerckhoffs's principle of security?

**Security by Obscurity**

Integrity is one of the main tenets of information security and concentrates on which choice below?

**Hash Functions**

How many keys are required for two people to communicate via a symmetric cipher?

**1**