**Mod 1 Quiz Answers**

The private or internal computer networks are vulnerable to the network security attacks either from internal or external attacks.

**True**

How is the OSI Architecture useful to managers?

**Way of organizing task to provide security**

All the following are example of security attacks EXCEPT:

**Setting up VLANs on a layer three switch.**

What are the two general approaches to attacking a cipher?

**Cryptoanalysis & Brute Force**

What is a Playfair cipher?

**A cipher that treats the diagrams in the plaintext as single units and translates these units into cipher**

**text diagrams.**

What is a passive attack?

**Attacks involving eavesdropping on, or monitoring of, transmissions.**

What is a Polyalphabetic cipher?

**There are multiple cipher text letters for each plaintext letter, one for each unique letter of keyword.**

All the following are three categories of the OSI security architecture EXCEPT:

**Security Enhancements**

What are the aspect of information security?

**security attack, security mechanism, security service.**

Which choice below best describes the essential ingredients of a symmetric cipher?

**Plaintext, Encryption algorithm, Secret Key, Cipher text, Decryption algorithm.**

What is Encipherment?

**The use of mathematical algorithms to transform data into a form that is NOT intelligible.**

How many keys are used in Symmetric encryption?

**One**

What is an active attack?

**Involves some modification of the data stream or the creation of a false stream**

The most famous of all rotor machines was the enigma that was broken by Alan Turing.

**True**

What are the two basic functions used in the encryption algorithm?

**Substitution and Transposition**

Define Threat.

**A potential for violation of security, which exists when there is a circumstances,**

**capability, action, or event that could breach security and cause harm.**

All the following are some common information integrity functions EXCEPT.

**Transformation**

How many keys are used in Asymmetric encryption?

**Two**

What is a Monoalphabetic cipher?

**A single cipher alphabet is used per message.**

What is a Caesar cipher?

**Involves replacing each letter of the alphabet with letter standing a fixed number of places down the alphabet.**

**Mod 1 Key Terms**

Block Cipher

**A symmetric key algorithm operating on fixed-length groups of bits called blocks.**

Brute-Force Attack

**A method of accessing an obstructed device by attempting multiple combinations of numeric/alphanumeric passwords.**

Caesar Cipher

**A type of substitution cipher in which each letter in the plaintext is replaced by a letter some**

**fixed number of positions down the alphabet.**

Ciphertext

**Encrypted or encoded information because it contains a form of the original plaintext that is**

**unreadable by a human or computer without the proper cipher to decrypt it.**

Cryptography

**Any of various mathematical techniques for encrypting and decrypting data to keep it private when transmitted or stored electronically.**

Cryptology

**The study of cryptanalysis or cryptography**

Decipher

**To decode or work out a hidden meaning**

Encipher

**To convert information into cipher or code**

Encryption

**The process of encoding information.**

Hill Cipher

**A polygraphic substitution cipher based on linear algebra.**

One-Time Pad

**An encryption technique that cannot be cracked but requires the use of a single-use**

**pre-shared key that is no smaller than the message being sent.**

Rotor Machine

**An electro-mechanical stream cipher device used for encrypting and decrypting messages.**

Plain Text

**Data that represents only characters of readable material**

Steganography

**The practice of concealing a message within another message or a physical object.**

Symmetric Encryption

**Uses the same cryptographic keys for both the encryption of plaintext and the decryption of ciphertext.**