RAMIREZ, Ishmael L.

20201132141

1. Compare and Contrast Cryptographic Ciphers

* Substitution Cipher – This type of encryption uses substitution to replace letters of a message with a different letter that follows a certain format or mapping
* Transposition cipher – is an example of a cryptographic algorithm where the order of the alphabets contained in a text is rearranged into different form to show as a cipher text.
* Stream Cipher – is a part of an encryption method wherein it works byte by byte to convert the plain texts into code that is not recognizable to anyone who doesn’t have the proper authorization or key.
* Block Cipher – is another encryption method that encrypts data blocks using a specific algorithm along with a symmetric key. Block ciphers encrypt 128-bit blocks with a key of a specified length: 128, 192, or 256 bits.
* Symmetric Cipher – a symmetric cipher uses the same algorithm or symmetric for encryption and decryption of data. Symmetric cipher uses the same key to encrypt data as well as decrypting data, making speed an advantage in this setup.
* Asymmetric Cipher – asymmetric cipher uses different keys for encryption and decryption of data. Generally, there are two keys involved and these are called public and private keys. One key is used to encrypt data, and another is used to decrypt data
* Hashing – is a method of converting any forms of data into a unique string of texts. Any data can be hashed regardless of its size or type. A hash is designed to act as a one-way function — you can put data into a hashing algorithm and get a unique string, but if you come upon a new hash, you cannot decipher the input data it represents. A unique piece of data will always produce the same hash.

1. Summarize the cryptographic Modes of Operation

The modes of operation in a cipher block are the rules of operation that could take place in other properties that provide additional security to the cipher block in cryptography.

* Cipher Block Chaining (CBC)

Provides message relying on generating ciphertext that makes the system hard to identify. Merges blocks and an initialization vector using XOR operation.

* Electronic Codebook

Is used in cryptography as a mode of operation for cipher blocks, with each working block of plaintext has an equivalent trait of a ciphertext value and vice-versa. The same plaintext will always produce the same result as the ciphertext value

* Cipher Feedback Mode

This is another mode of operation for cipher blocks wherein the desirable encryption or transfer of plaintext or original values to ciphertext are one at a time.

* Output Feedback Mode

The output of the encryption function is being directed back to the shift register in cryptography. This mode of operation functions on full blocks of plaintext and ciphertext

* Counter Mode

This is a simple counter-based cipher block wherein it records every time a counter has been started, encrypted, and has been given a value as an input to XOR with plaintext that will now produce a product of ciphertext block.

1. Summarize Cryptographic Use Cases and Weaknesses

Cryptography supports the proper handling of sensitive information with the right encryption and decryption. There are 3 types when it comes to handling confidentiality encryption:

* Hybrid Encryption
* File Encryption
* Transport Encryption

Cryptography also supports the strength and reliability. The strength of cryptography comes from:

* Integrity – usage of various hash functions and authentication passwords as a means of validating information
* Resiliency – using cryptography to ensure the authenticity and validity of messages
* Obfuscation – making things difficult for other people to understand as a way of encryption

Cryptography is not without its own weaknesses. There are certain traits that cryptography lacks. Some of these are:

* Speed
* Latency
* Size

1. Summarize Other Cryptographic Technologies

* Quantum

Quantum Cryptography uses the concept of quantum mechanics to impose the traits of cryptography into information and data making the information more secure

A sub-trait of quantum cryptography is post-quantum cryptography that refers to cryptographic algorithms that are secured to vulnerable attacks by a quantum computer

* Homomorphic Encryption

Supports the functions of data analytics while relatively keeping the process of security and privacy

* Blockchain

Blockchain refers to the blocks or collection of data that is linked or chained together by hashing. Blockchain is a growing list of records and information, and the blocks get appended to the list as time passes. These are potentially used in cryptocurrency, financial organization transactions, data storage etc.

* Steganography

This is a method of concealing a secret message inside an event that is not meant to be secret. The purpose of steganography is to hide and deceive other people without prior knowledge to the event. An example of a steganography is embedding a hidden message inside an image

References:

* <https://www.keycdn.com/blog/perfect-forward-secrecy>
* <https://www.includehelp.com/cryptography/mode-of-operation.aspx>
* <https://www.fortinet.com/resources/cyberglossary/digital-certificates>
* https://www.docusign.com/how-it-works/electronic-signature/digital-signature/digital-signature-faq