RAMIREZ, Ishmael L.

20201132141

1. Define Digital Signatures

This is a technique used in identifying the validity and authenticity of a certain message, software, and/or digital document. The digital signature is also similar to how handwritten signatures work in real life but offers more security

1. What is the use of Digital Certificate?

A digital certificate is used as an electronic credential or password that authorizes a person or organization to trade data over the internet with a secure connection using the public key infrastructure or PKI. Digital Certificate authenticates only entrusted devices and allows connection within the company or organization only. A digital certificate contains identifiable information, such as a user’s name, company, or department and a device’s Internet Protocol (IP) address or serial number.

1. What is the use of Perfect Forward Secrecy?

Also known as Forward Secrecy, is a process of verifying that all connections and transactions transpiring over the internet are secured. This method is a way of preventing hackers and other people with malicious intents from accessing the data of transactions even if they have the capability to hack the encryption of the transaction itself.

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.

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