Digital Egypt Pioneers

Digital Signatures, Hashing, and Steganography

Ammar Yasser Mohamed
Course Code: ONL3_ISS2_S2
23 July 2025

1 Digital Signatures: Ensuring Authenticity and Non-Repudiation

Digital signatures are a core part of cybersecurity that ensure two things: **authenticity**, confirming the message came from the stated sender, and **non-repudiation**, meaning the sender cannot deny sending it.

Here's how it works: First, a hash of the message is created using a cryptographic hash function. Then, this hash is encrypted using the sender's private key—this encrypted hash is the digital signature. When the message is received, the recipient decrypts the signature using the sender's public key and compares the result to a freshly computed hash of the message. If they match, the message is authentic and unchanged.

The Role of PKI

Public Key Infrastructure (PKI) supports this process by linking public keys to verified identities through digital certificates. These certificates, issued by trusted Certificate Authorities (CAs), prove that a specific public key belongs to a specific individual or organization.

2 SHA-256 vs. SHA-1 in Digital Signatures

Hash functions are used to generate the message digest in digital signatures. The basic difference between SHA1 vs. SHA256 or SHA1 vs SHA2 is the length of the key used to encrypt the data transferred online. SHA1 uses 160 bit long key to encrypt data while SHA256 uses 256 bit long key to encrypt data. SHA2 is a family of algorithms developed by the US government to secure the data online.

SHA-256 is much stronger and collision-resistant, making it the safer and more reliable choice for digital signatures today.

3 Steganography vs. Encryption

Both steganography and encryption protect information, but in different ways:

- **Encryption** scrambles data so it can't be read without a key, but the presence of hidden data is obvious.
- **Steganography** hides the existence of the data itself by embedding it in something like an image or video file.

Use Cases for Steganography

Steganography is used when you want to avoid detection altogether. Examples include hiding secret messages in image files or embedding information in media files for copyright protection.

4 Combining Encryption with Steganography

Using encryption and steganography together provides stronger protection. Encryption secures the content, while steganography conceals its existence. Even if someone finds the hidden message, it will still be encrypted and unreadable without the decryption key.

This approach is useful in scenarios where security and secrecy are both critical, such as covert communication or data exfiltration prevention.