004_Non-repudiation - CompTIA Security+ SY0-701 - 1.2

Video: https://youtu.be/XxnCxPEllMg?si=jgtd4mkC6483-1BG

Non-Repudiation in Cryptography

Introduction

Non-repudiation ensures that a party in a digital communication or transaction cannot deny the authenticity of their signature or the sending of a message. It is a critical function of cryptography used to provide verifiable and tamper-proof evidence that specific actions or communications occurred. Non-repudiation is especially important in legal, financial, and security-sensitive contexts.

1. Hashing

What is hashing?
Hashing is a cryptographic process that transforms an input (e.g., a message or file) into a fixed-size string of characters, often referred to as a hash or digest. A hash is unique to the input data, meaning even a slight change in the input results in a drastically different hash.

Key properties of hashing:
- Deterministic: The same input always produces the same hash.
- Fast computation: Hashing algorithms are efficient to compute.
- Collision resistance: It is computationally infeasible to find two different inputs that produce the same hash.
- Irreversibility: A hash cannot be converted back to the original input.

Relevance to non-repudiation:
Hashes ensure data integrity by proving that the original data has not been altered. For non-repudiation, the hash is often used as a basis for verifying that the original message is authentic.

2. Digital Signatures

What are digital signatures?
A digital signature is a cryptographic mechanism used to verify the authenticity and integrity of digital messages or documents. It is akin to a handwritten signature or a stamped seal but much more secure.

How it works:
1. The sender creates a hash of the message using a hashing algorithm.
2. The hash is encrypted with the sender's private key, creating the digital signature.
3. The digital signature and the message are sent to the recipient.

Verification process:
- The recipient decrypts the digital signature using the sender's public key to retrieve the hash.
- The recipient then hashes the received message independently and compares it to the hash retrieved from the signature. If the hashes match, the message is verified as authentic.

Relevance to non-repudiation:
Digital signatures ensure that the sender cannot deny having signed the message because only the sender's private key could have created the signature.

3. Non-Repudiation

What is non-repudiation?
Non-repudiation ensures that a sender cannot deny sending a message and that a recipient cannot deny receiving it. This is achieved by combining hashing and digital signatures.

How non-repudiation works in practice:
- The digital signature, created with the sender's private key, provides evidence that the sender authored or agreed to the message.
- Hashing ensures that the message has not been tampered with.
- Public key infrastructure (PKI) provides a system for managing keys and verifying the authenticity of the sender's public key.

Applications of non-repudiation:
- Emails: Ensuring that the sender cannot deny having sent an email.
- Contracts: Providing tamper-proof digital signatures for agreements.
- Financial transactions: Preventing denial of payments or orders.

Summary

Non-repudiation relies on a combination of hashing (to ensure integrity) and digital signatures (to verify authenticity and identify the sender). Together, they create a robust system for securing digital communications and transactions, ensuring that neither party can dispute their actions. This is essential in a wide range of applications, including legal, financial, and security-sensitive operations.