Armen Melkumyan • 1st

Technical / Solutions Architect

7mo • Edited • 🌐

···

Understanding RSA-SHA256 Digital Signatures 🔐

In modern secure systems, digital signatures ensure that data remains authentic and unaltered during transmission. One widely used combination is RSA-SHA256, a powerful duo in cryptography. Let’s break it down:

The Flow:

1️⃣ Key Generation: A pair of asymmetric keys is created— the private key (used for signing) and the public key (used for verification). These keys are mathematically linked but not interchangeable.

2️⃣ Message Signing: When a message is prepared for transmission, it’s first hashed using SHA-256. This converts the message into a fixed-length hash, ensuring that any small change to the message drastically changes the hash output. The hash is then encrypted using the sender's private RSA key, producing the signature.

3️⃣ Signature Verification: Upon receipt, the signature is decrypted using the sender’s public RSA key. The recipient independently hashes the received message using SHA-256 and compares it to the decrypted signature hash. If they match, the message is validated as authentic and untampered.

Why RSA-SHA256?

1) Integrity: SHA-256 ensures even the slightest change in the message results in a completely different hash, allowing the detection of tampering.

2) Authenticity: The use of the RSA key pair confirms that the message genuinely originated from the claimed sender.

3) Security: The combination of RSA for asymmetric encryption and SHA-256 for hashing provides strong cryptographic guarantees that are widely trusted across industries.

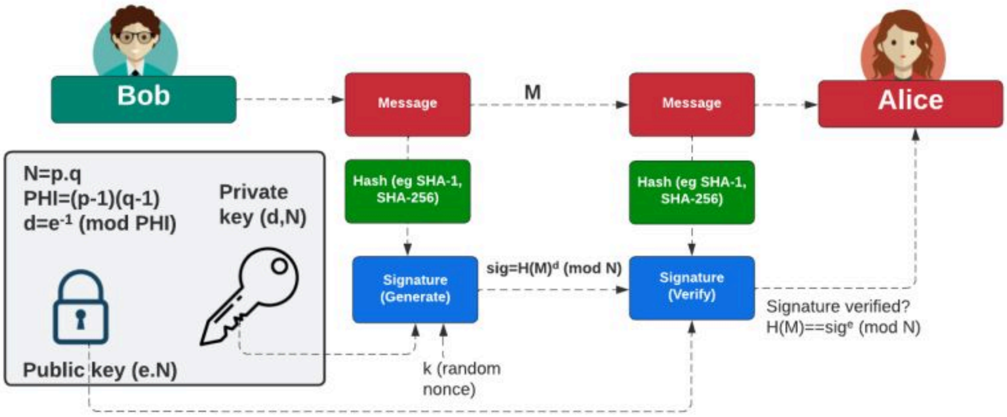
This method is commonly used in everything from secure email and software distribution to digital certificates and blockchain systems. It's a fundamental tool for ensuring that critical data remains trustworthy.

Node.js JavaScript implementation here: https://lnkd.in/d_5UwZMN

C# .Net Implementation here: https://lnkd.in/d_XWK7HZ

#Charp #DotNet #Node #JavaScript #DigitalSignatures #Cryptography #RSA #SHA256

#SecurityEssentials #DataIntegrity #Authentication #CyberSecurity #SecureData #SoftwareEngineering



41 1 repost