Discrete Maths Project

28 May, 2023

Parv Patel : 202201476

Kathan kadiya : 202201175

Jenil Goswami : 202201247

Jeet Patel : 202201216

Kritarth Joshi : 202201338

Kashyap Gajera: 202201324

Topic

RSA AND DIGITAL SIGNATURES

CONTENTS:

Title

What is RSA Algorithm?

→ Full Form of RSA Algorithm is Rivest-Shamir-Adleman Algorithm. RSA Algorithm is used for encryption and decryption process using keys...BUT now the question arises in your mind is What is ENCRYPTION and DECRYPTION....Okay, Let's understand it...

- ***ENCRYPTION*** :

  → Encryption is a process to convert Plain Text into Cipher Text using keys...There are different types of cipher texts for same plain text depending on which encryption algorithm is used for this conversion...
  ⇒ There are 2 types of Encryption.

  – ***Symmetric*** :

    Here both Sender and Receiver uses the same key to encrypt and decrypt a data...

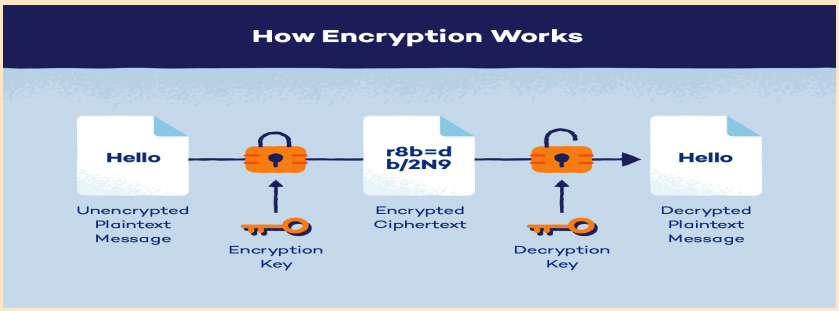
  – ***Asymmetric*** :

    Here both Sender and Receiver uses the different key to encrypt and decrypt a data...

- ***DECRYPTION*** :

  → Decryption is a process to convert Cipher Text into Plain Text using keys...its a basically reverse process of encryption..

Okay, I think you are able to understand that what is RSA and why this algo used....Let's see one image related to this process..



Title

Mathematics behind RSA Algorithm

→ Here the mathematics in this process is to calculate PUBLIC and PRIVATE key...So How to calculate it??.. let's see and understand step wise...

1. **Choose 2 Prime Numbers and calculate N.**

   Prime Number 1 ⇒ P
   Prime Number 2 ⇒ Q

$$\boxed{N = P*Q} \tag{1}$$

2. **Find Eular Totient Function of N.**

$$\boxed{\phi(N) = (P-1)*(Q-1)} \tag{2}$$

3. **Find Public key.**
   ⇒ Choose a number e such that..

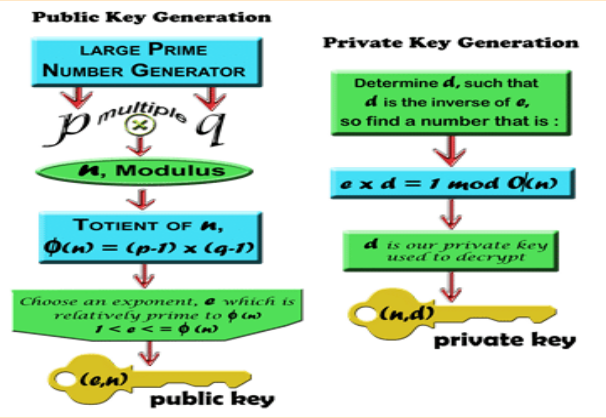
$$\boxed{1 < e < \phi(N)} \tag{3}$$

   Please note that GCD (e, ϕ(N)) = 1

4. **Find Private Key.**

$$\boxed{d \equiv e^{-1} \bmod(N)} \tag{4}$$

⇒ ***Public key is (e, N)***
⇒ ***Private key is (d, N)***



Title

Advantages and Disadvantages of RSA Algorithm

- **ADVANTAGES :**

  ⇒ The RSA algorithm can be implemented relatively quickly and efficiantely.

  ⇒ Here distribution of public keys to users is very simple.

  ⇒ Breaking the RSA algorithm is extremely challenging because mathematics involved in this process is very complex.

  ⇒ The RSA algorithm is secure and trustable for sending private information.

  ⇒ For mechanisms, sending sensitive information carries no danger because RSA is dependable and secure.

- **DISADVANTAGES :**

  ⇒ it might occasionally fail, because RSA only employs asymmetric encryption and complete encryption requires both symmetric and asymmetric encryption.

  ⇒ Sometimes, it's necessary for a third party to confirm the dependability of public keys.

  ⇒ The data transfer rate is slow.

  ⇒ RSA cannot be used for public data encryption.

  ⇒ Decryption requires in-depth processing on the receiver's end.

Title

What is Digital Signature?

⇒ let's see one example...

I assume that you have a crush and she sends you a message (I LOVE YOU) then how you verify that this message is sent by your Girlfriend or any other person do this with your crush's phone.. (Don's say you trust her..)...for solving this problem we should use digital signature that message is sent by your sender or any third party person...we will see that how we generate Digital signature..

let's move on the Proper Definition of Digital Signature.

DEFINITION :

⇒ A Digital signature is a mathematical technique used to validate the authenticity and honesty of a digital document, message or software.

⇒ It's the digital equivalent of a handwritten signature or stamped seal, but it offers far more structural security.

⇒ A digital signature is intended to solve the problem of tampering and impression in digital communications.

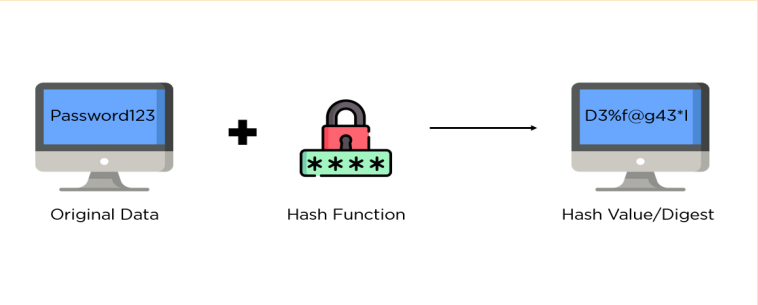
In short Digital Signature are digital equivalent of a handwritten signature and used in digital communication for verification and solve tampering problems..

Title

SHA - 256 Algorithm

⇒ it's basically a HASH FUNCTION...Now the question arises is what is hash function?

⇒ Hash function is the function which converts message(original data) into digest/hash value..



What is SHA-256 Algorithm?

→ The Secure Hash Algorithm, or SHA, family of algorithms includes the SHA 256 algorithm. The NSA and NIST collaborated on this 2001 publication in an effort to replace the SHA 1 family, which was gradually becoming less resistant to brute force attacks.

→ The 256 in the name refers to the final hash digest value, meaning that regardless of the amount of plaintext or cleartext present, the hash value will always be 256 bits.

→ The other algorithms in the SHA family are more or less similar to SHA 256.

Note

Output value of SHA-256 is ***hexadecimal number of 64 Digits(256 bits)***.

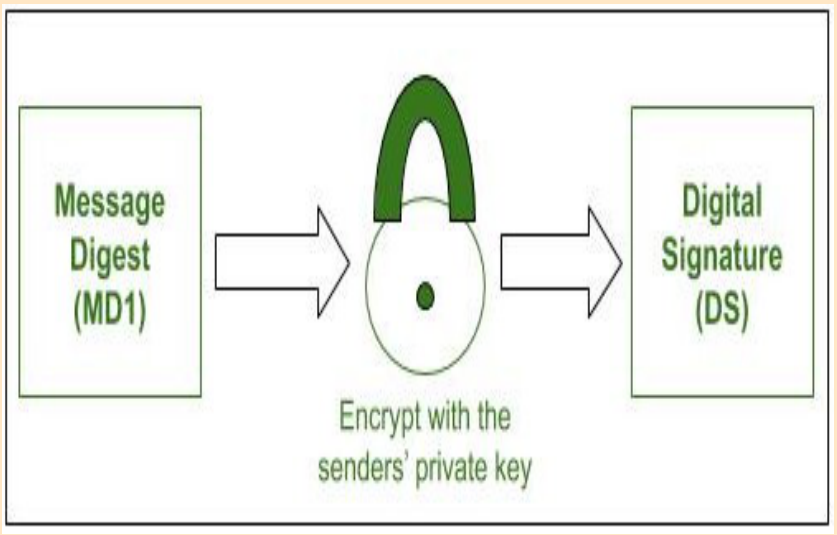
Title

Full Procedure

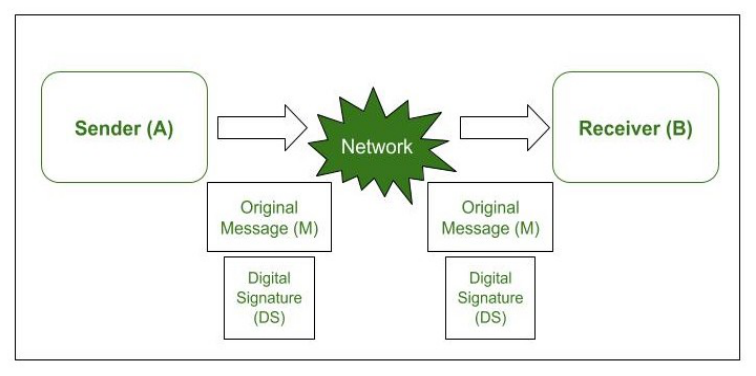
1. Step 1 : Conversion in Digest message by Sender using hash function SHA-256.

2. Step 2: Conversion in digital signature using private key of sender.

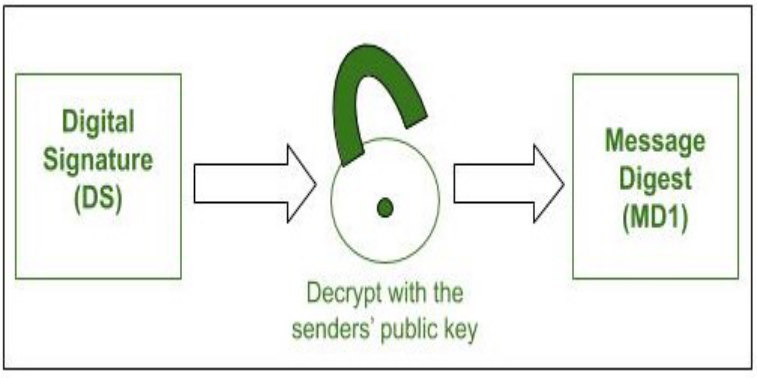
$$\boxed{Signature \equiv (\textbf{Digested message})^{d} \textbf{mod(N)}}$$



3. Step 3 : Pass Digital Signature along with Digested message of sender to receiver...



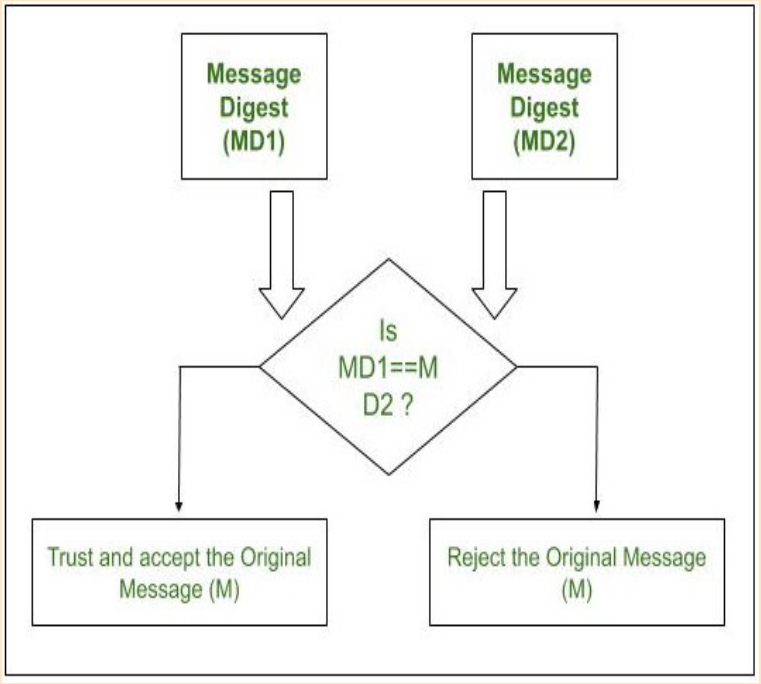
4. Step 4 : Receiver decrypt a digital signature using public key of sender.. and get a digested message..(MD1)



$$\boxed{Digestedmessage \equiv \textbf{(signature)}^{e}\textbf{mod(N)}}$$

5. Step 5 : same as step 1 receiver also coverts message in digested message using SHA-256(MD2).

6. Step 6 : Compare both MD1 and MD2.



Title

Real life applications

Authentication

A Pair of cryptographic keys-a private key and a public key-are created using the RSA algorithm when you want to digitally sign a document or conduct an online transaction. While the public key is distributed to others, the private key is kept private and only known to you.

Signing

Using your private key, you encrypt the document's hash (a distinctive representation) to digitally sign it. The digital signature is then appended to the document using this encrypted hash.(here we use SHA-256 as a hash function)

Verification

The receiver uses your public key to decrypt the digital signature and retrieve the hash in order to confirm the legitimacy of the document and the signature. They next perform their own computation of the received document's hash. The document has not been tampered with, and the digital signature is legitimate, if the two hashes match.(we already discussed a process).

Title

Commercialization

- ***Digitally sign and Encrypt PDFs and E-mails***

  ⇒ Let's think that 1 pdf is shared by your friend by post then how you verify that....i know your ans is by signature of your friend on post...am i right? then if this process is done digitally then you can do it with digital signature..

  ⇒ Create a software or website(we are trying to do that) that offers digital signature services. This platform should provide the necessary tools for users to generate RSA public and private keys, create digital signatures, and verify digital signatures.

- ***Attendence Marking Process***

  ⇒ Employees check-in Process : Provide employees with a means to make entry when they arrive at work. This can be done through a website interface, a mobile app.

  ⇒ Signature Capture Process : Once an employee make entry, tell them to provide their unique identifier (e.g., employee's office ID) and capture their digital signature using the previous integrated digital signature functionality.

  ⇒ Attendance Recording Process : Store the attendance record in the system, including the employee's unique identifier and it's corresponding digital signature.

  ⇒ Verification Process : Develop a process to verify the attendance. This may involve comparing the digital signatures against the corresponding public keys to ensure their validity and integrity of that employee.

⇒ Contributions :

Creation of latex File → Parv Patel & Kashyap Gajera
Creation of Website → Jenil Goswami & Kathan Kadiya
Creation of PPT → Jeet Patel & Kritarth Joshi