International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 12 Issue 7 ǁ July 2024 ǁ PP. 50-54

Application of encryption and decryption in digital signatures using RSA algorithm

PhuongAnh DaoThi[1], Hau BuiTa[1], VanTrong Thai[2]
[1]Information Technology Faculty, Hanoi University of Natural Resources & Environment, Hanoi, Vietnam
[2]School Of Mechanical and Automotive Engineering, Hanoi University of Industries, Hanoi, Vietnam

Abstract
In today's modern life, the transmission of information has become extremely important. This is especially true for organizations, businesses, or individuals who need to protect important information from external intrusion. This study includes Researching and understanding the RSA algorithm and related cryptographic concepts. Analyzing requirements and designing the application, including main functions: encryption, decryption, signature creation, and signature verification. Building the application according to the design, using appropriate programming languages and supporting libraries to implement the main functions. Testing and evaluating the application's performance, including the execution time of functions and the accuracy of results. Improving and developing the application to enhance performance and features. The research content will provide a deep understanding of cryptography and the practical application of the RSA algorithm. Additionally, the application can be used to protect personal information and important documents in organizations and businesses.

Keywords: *Encryption, decryption, digital signature, cryptography, RSA*

Date of Submission: 25-06-2024 Date of acceptance: 04-07-2024

I. INTRODUCTION

Encryption is the process of transforming original information into another form that only the recipient can read. This process is performed through an encryption algorithm and uses a key. The purpose of encryption is to ensure confidentiality and security in communication. There are two main types of encryptions: symmetric encryption and asymmetric encryption. Symmetric encryption uses the same key to encrypt and decrypt data, while asymmetric encryption uses two different keys, one for encryption and one for decryption. Decryption is the process of transforming encrypted data back into its original form using a decryption key. Only the person with the decryption key can decrypt the data. The decryption process is usually performed immediately after the encryption process ends and the information has been transmitted to the recipient. If the recipient has a decryption key that matches the encryption key, they can use that key to decrypt the data and read the original information. A key is a string of values used in the encryption and decryption process to ensure the confidentiality and security of transmitted information. In symmetric encryption, the same key is used to encrypt and decrypt information. This key is called a secret key or symmetric key. Encryption is an important means to ensure security and safety in information communication.

Some modern cryptographic forms include:

AES (Advanced Encryption Standard): Widely used in modern security applications and systems. AES uses symmetric keys and is considered one of the strongest encryption algorithms today.

RSA: Used in public key encryption systems, RSA is highly regarded for its safety and reliability. RSA uses public and symmetric keys to protect information.

Elliptic Curve Cryptography (ECC): A cryptographic system that uses elliptic curves to create keys and encrypt information. ECC provides higher security than traditional algorithms and is used in many security applications.

Quantum Cryptography: A type of cryptography that uses the properties of quantum physics to protect information. Quantum Cryptography is considered one of the safest cryptographic systems today and can be used to protect important information in military and government systems.

II. DIGITAL SIGNATURE

A digital signature is a specific type of electronic signature that acts as a virtual "fingerprint" used to authenticate the identity of the signer and the digital document they sign. When a document is electronically signed, a digital certificate is permanently embedded in the document. In addition to accurately identifying the signer and the time of signing, this digital certificate verifies whether the document has been tampered with.

Advantages of Digital Signatures:

- Identity authentication
- Ensuring integrity
- Information security
- Ease of use

Disadvantages of Digital Signatures:

- Costly
- Dependent on keys
- Difficult to popularize

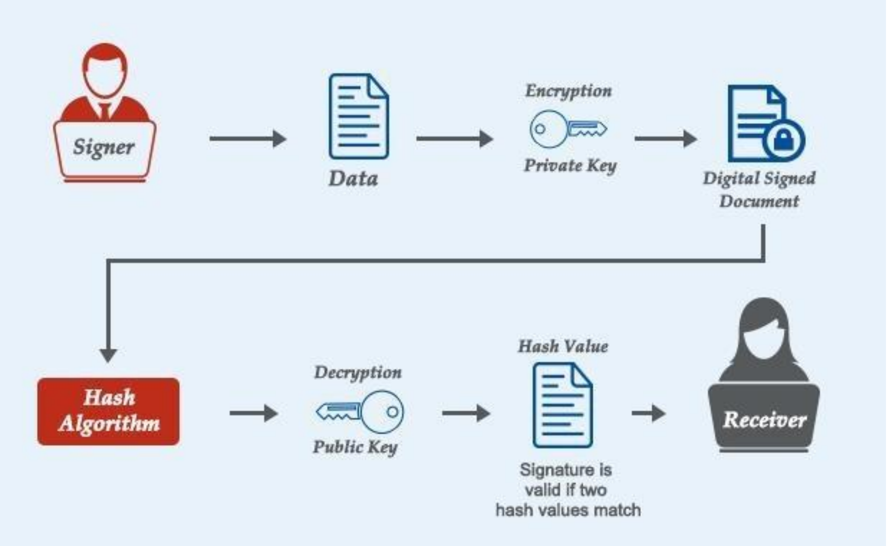

Figure1: Digital signatures diagram

Despite its disadvantages, the importance of integrity and authenticity in online transactions makes the use of digital signatures necessary and encouraged in many fields. Digital signatures have become an indispensable means of authentication in electronic communications and online transactions. They play an important role in fields such as banking, finance, healthcare, government, and business.

Architecture of Digital Signatures

The architecture of digital signatures is usually built on public key cryptography technology and uses a pair of keys consisting of a private key and a public key.

The process of creating a digital signature begins by hashing the original data using a hashing algorithm. The hash result is then signed with the private key of the digital signature owner. When the digital signature is sent to the recipient, they use the owner's public key to verify the authenticity of the digital signature by comparing the hash result of the original data with the result decrypted from the digital signature using the public key.

System Diagram of Digital Signatures

The system diagram of digital signatures includes the following main components:

- User: The user creates and uses the digital signature to authenticate data.
- Hash Algorithm: The hash algorithm is used to create a unique hash value of the data to be signed.
- Private Key: The private key is used to sign the digital signature and is only known to its owner.
- Public Key: The public key is used to decrypt the digital signature and can be provided to anyone to verify the digital signature.
- Digital Signature: The digital signature is the result of signing the data with the private key and is used to verify the correctness of the data.
- Digital Signature Verification: The process of verifying the digital signature is performed by the recipient using the public key to decrypt the digital signature and compare the hash value of the original data with the hash value signed by the private key.

III. ANALYSIS AND DESIGN OF RSA ENCRYPTION AND DECRYPTION SYSTEM

Concept of RSA Encryption System

The RSA algorithm is based on the use of a pair of keys: a public key and a private key. The public key can be widely shared and is used to encrypt messages, while the private key is only held by the owner and is used to decrypt messages.

The RSA algorithm operates based on the difficulty of factoring a large integer into its prime factors. During key generation, the key creator generates a large integer n by selecting two large prime numbers p and q, then calculating n = p*q. The key creator then generates the public key and private key based on n and other parameters.

To encrypt a message, the sender uses the recipient's public key to encrypt the message into an unreadable cipher, called RSA encryption. The recipient then uses their private key to decrypt the message and read the content.

Operation of RSA Encryption System

RSA is a public key cryptography algorithm used to encrypt and decrypt data. In the RSA system, each user has a pair of keys, including a public key and a private key.

Step 1: Generate Key Pair Step 2: Encrypt Message Step 3: Decrypt Message After the message is encrypted, the recipient uses their private key to decrypt the message. When decryption is performed, the recipient can read the content of the message.

In practice, RSA is also used to sign and verify digital signatures. In this case, the signer uses their private key to create a digital signature for the document, and the verifier uses the signer's public key to verify the authenticity of the digital signature.

Architecture of RSA Encryption System

RSA is built based on a trio of keys including a public key, a private key and a session key. The main architecture of the RSA cryptographic system includes:

Public Key:

The public key consists of two components: an integer e and an integer n.

The integer e is chosen such that $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$, where $\phi(n)$ is the Euler's Totient function of n.

The integer n is calculated by taking the product of two large random prime numbers p and q: n = p * q.

Private Key:

The private key consists of an integer d.

The integer d is calculated from the public key e, the integer n, and the Euler's Totient function $\phi(n)$ using the modular inverse operation: d ≡ e^(-1) (mod $\phi(n)$).

Encryption Process:

The sender uses the recipient's public key to encrypt the message.

Encrypt the message m by calculating c = m^e (mod n), where m is the original message and c is the encrypted message.

Decryption Process:

The recipient uses their private key to decrypt the encrypted message.

Decrypt the message c by calculating m = c^d (mod n), where m is the decrypted message and d is the private key.

The architecture of RSA is based on the difficulty of two problems in number theory: factoring a large integer into its prime factors and calculating the modular inverse. By choosing large prime numbers and performing complex operations, RSA provides a strong encryption and decryption mechanism, widely used in protecting information and authentication in modern cryptographic systems.

Decrypting Digital Signatures Use Case Name:

Decrypting RSA Digital Signatures Description: This use case describes the process of decrypting a message using a private key and RSA digital signature. Actor: User Preconditions:

The user must have a private key to decrypt the digital signature.

The digital signature must be encrypted with the sender's public key.

Main Event Flow:

The user selects the function to decrypt the digital signature.

The system requests the user to provide the digital signature to be decrypted.

The user provides the digital signature.

The system uses the private key to decrypt the digital signature.

The system displays the decrypted message.

The user reads the decrypted message.

Postconditions:

The message has been decrypted and can be read.

Exceptions:

The private key is invalid or insufficient to decrypt the digital signature.

The digital signature is invalid or has been altered from the original version.

Method for generating private and public keys

```
    // Phương thức tạo khóa bí mật và khóa công khai
        private void buttonGenerate_Click(object sender, EventArgs e)
        {
            SaveFileDialog saveFileDialog = new SaveFileDialog();
            saveFileDialog.Filter = "XML Key Files (*.xml)|*.xml|Private Key Files (*.priv)|*.priv|Public Key
Files (*.pub)|*.pub|All files (*.*)|*.*";
            saveFileDialog.Title = "Chọn vị trí lưu khóa";
            if (saveFileDialog.ShowDialog() != DialogResult.OK)
                return;
            RSACryptoServiceProvider rsa = new RSACryptoServiceProvider();
            publicKeyServer = rsa.ToXmlString(false);
            privateKeyServer = rsa.ToXmlString(true);
            File.WriteAllText(saveFileDialog.FileName + ".pub", publicKeyServer);
            textBoxPublicServer.Text = saveFileDialog.FileName + ".pub";
            File.WriteAllText(saveFileDialog.FileName + ".priv", privateKeyServer);
            textBoxPrivateServer.Text = saveFileDialog.FileName + ".priv";
            MessageBox.Show("Khóa đã được tạo và lưu thành công");
```

Method to create digital signature

```
    private void buttonStartSignServer_Click(object sender, EventArgs e)
        {
            if (privateKeyServer == null)
            {
                MessageBox.Show("Không tìm thấy khóa bí mật");
                return;
            }
            using (var rsa = new RSACryptoServiceProvider())
            {
                rsa.FromXmlString(privateKeyServer);
                var data = File.ReadAllBytes(filePathToSign);
                var signature = rsa.SignData(data, HashAlgorithmName.SHA256,
RSASignaturePadding.Pkcs1);
                var signatureFilePath = Path.ChangeExtension(filePathToSign, ".sig");
                File.WriteAllBytes(signatureFilePath, signature);
            }
            MessageBox.Show("File đã ký thành công.");
```

Digital signature authentication method

```
    private void buttonStartVerifyClient_Click(object sender, EventArgs e)
        {
            if (publicKeyClient == null)
            {
                MessageBox.Show("Không tìm thấy chữ ký");
                return;
            }
            using (var rsa = new RSACryptoServiceProvider())
            {
                rsa.FromXmlString(publicKeyClient);
                var data = File.ReadAllBytes(filePathToVerify);
                var signature = File.ReadAllBytes(filePathDigitalSignature);
                var verified = rsa.VerifyData(data, signature, HashAlgorithmName.SHA256, RSASignaturePadding.Pkcs1);
                if (verified)
                {
                    MessageBox.Show("Chữ ký hợp lệ.");
                }
                else
                {
                    MessageBox.Show("Chữ ký không hợp lệ. Chữ ký có thể đã bị giả mạo.");
                }
            }
        }
```

IV. CONCLUSION

The RSA algorithm used in encryption and decryption applications in digital signatures brings many important advantages. First of all, this algorithm provides a strong security mechanism, ensuring the integrity and confidentiality of information. The use of a public and private key pair allows for secure transmission of data over public networks without worrying about theft or modification. Building encryption and decryption applications in digital signatures using the RSA algorithm brings flexibility and diversity to information encryption.

Although the RSA algorithm has many advantages, it also has some disadvantages that need to be considered. First, the RSA algorithm requires the use of complex arithmetic operations, including exponential and large modulo operations. This can increase the computational complexity of the application and consume a lot of computational resources. The size of the key has a big impact on performance and security. To ensure high security, it is necessary to use large sized keys, which means increasing the size of the data to be transmitted and the encryption and decryption time.

REFERENCES

[1]. Sercurity (2005), “Cryptography and Network security principles and Pratices” by Wlliam Stalling

[2]. DAN BONEH (1999), “Twenty Year of Attacks on RSA”, Stanford University.

[3]. S. Castano, M.Fugina, G.Martella, P.Samarati,“Database Sercurity”, 1994

[4]. https://www.researchgate.net/figure/Asymmetric-encryption-primitive_fig2_321123382

[5]. https://www.geeksforgeeks.org/classical-cryptography-and-quantum-cryptography/

[6]. https://www.researchgate.net/figure/Timeline-of-quantum-cryptography_fig1_357334488

[7]. https://www.makemydigitalsignature.com/category/technology/

[8]. https://bizflycloud.vn/tin-tuc/hash-la-gi-cac-dang-hash-code-20181024154415208.htm