RSA Algorithm Explanation

The RSA (Rivest-Shamir-Adleman) encryption algorithm is a public-key encryption and digital signature algorithm. It was developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm is used for communication security and data protection and primarily relies on two keys: the public key and the private key.

Key Pair Generation

Selection of Prime Numbers

- The first step involves choosing two large prime numbers, p and q, which are selected randomly. This step is crucial in enhancing the security of RSA.

Calculation of the Modulus (n)

- The modulus, denoted as n, is computed as the product of the prime numbers: n = p * q. The modulus n is a component of the public key and is typically made public.

Calculation of Euler's Phi (φ) Function

- The Euler's phi function, φ(n), is used to represent Euler's totient of n and is calculated as φ(n) = (p-1) * (q-1). This value plays a crucial role in the creation of the public key.

Selection of the Public Key

- The public key is created by selecting an e (encryption key) that is coprime with φ(n). The public key is represented as (e, n) and is used for encrypting messages.

Computation of the Private Key

- The private key is determined based on the equation e * d ≡ 1 (mod φ(n)). This equation enables the use of the private key to decrypt encrypted data. The private key is represented as (d, n) and must be kept confidential.

Encryption

Encryption Process

To encrypt data or a message, the public key is used:

- The message, represented by a numerical value, is encrypted using the public key. Mathematical operations are applied to transform each character or block.
- The encryption process involves raising the message to the power of the public key (e) and taking the modulus n: c = m^e mod n, where "c" represents the encrypted message, and "m" represents the original message or data.

Decryption

Decryption Process

The encrypted data is decrypted using the private key:

- The message, represented by a numerical value, is encrypted using the public key. Mathematical operations are applied to transform each character or block.
- The encryption process involves raising the message to the power of the public key (e) and taking the modulus n: c = m^e mod n, where "c" represents the encrypted message, and "m" represents the original message or data.

Advantages and Disadvantages of the RSA Algorithm

Advantages

Ensures Secure Communication

- RSA is a public-key encryption algorithm that provides the ability to secure communication. Messages are encrypted with the public key and can only be decrypted with the private key, ensuring privacy during communication.

Can Generate Digital Signatures

- RSA can be used to create digital signatures. This is used to verify who has created documents and messages. Digital signatures indicate that a trusted individual or organization has endorsed the document or message.

Public Key Encryption

- The public key being openly available allows others to send secure messages to you. Transmitted data is encrypted with the public key and can only be decrypted with your private key.

Ease of Use

- Public key encryption can be used by anyone, and encrypted data can be decrypted with the private key to return to the original text.

Disadvantages

Slow Processing

- RSA is a public-key encryption algorithm that provides the ability to secure communication. Messages are encrypted with the public key and can only be decrypted with the private key, ensuring privacy during communication.

Key Management

- RSA requires key management. Public and private keys must be stored securely. If keys are lost or compromised, security can be jeopardized.

Complexity of Operation

- RSA algorithm involves mathematically complex operations. The selection of prime numbers and the computation of the private key can be challenging.

Large Keys

- Using large prime numbers may be necessary for better security, requiring longer keys. This, in turn, demands more processing power and storage space.

Slow Data Transmission

- Data encrypted with RSA can be larger than the original data, affecting data transmission speeds.

RSA Key Management and File Encryption Report

Objective

- This report explains a key management system and file encryption process using the RSA (Rivest-Shamir-Adleman) algorithm. This process allows users to generate public and private key pairs, encrypt files, and decrypt encrypted files.

Key Management

- RSA key management is a fundamental step for secure communication and data protection. This process includes the creation and storage of public and private keys.
- **Key Generation:**
- The “anahtar_olustur” function creates an RSA key pair.
- A public key and a private key are generated. The public key is stored openly, while the private key remains confidential.
- The public and private keys are saved in PEM format files.
- **Key Loading:**
- The “anahtar_yukle” function loads previously created keys.
- If there are public and private key files, this function loads these files.

Main Operation Loop

- A user interface is provided for key management and file operations.
- The user selects the operation they want to perform: Generate Key, Encrypt File, Decrypt File, Exit.

File Encryption

- File encryption is performed using the public key.
- The user enters the name of the file they want to encrypt.
- **File Encryption:**
- The “dosyayi_sifrele” function encrypts the selected file.
- The content of the file is read and encrypted with the public key.
- The encrypted data is written back to the same file. This prevents the encrypted data from being stored in a separate file.

File Decryption

- Decrypting encrypted files is done using the private key.
- The user enters the name of the encrypted file they want to decrypt.
- **File Decryption:**
- The “dosyayi_coz” function decrypts the selected encrypted file.
- The content of the encrypted file is read and decrypted with the private key.
- The decrypted data is written back to the same file.

ATA GÜRSEL
215060044