TO: Dr. Steve Holmes, Director of Undergraduate Technical Communications Studies At Texas Tech University

FROM: Jubilee Akputa, Undergraduate Mathematics Student

DATE: April 25, 2024

SUBJECT: RSA Encryption Algorithm

This memo will provide an overview of RSA cryptography, a popular encryption algorithm commonly used in information security. RSA (Rivest-Shamir-Adleman) is named after its inventors: Ronald Rivest, Adi Shamir, and Leonard Adleman. It is commonly used in various applications like telecommunication, authentication protocols, and digital signatures.

Components:

1. Public Key: RSA encryption relies on a pair of keys: a public key and a private key. The public key is shared and used for encryption. It is created from the product of 2 random large prime numbers, which makes it difficult to derive the private key if you have the public key.

2. Private Key: The private key is kept private and is used for the decryption. It comes from the prime factors used to create the public key. The security strength of the algorithm comes from the difficulty that comes with factoring large numbers into primes.

Encryption Steps:

1. Key Generation:
   - 2 random large prime numbers, p and q are selected.
   - Get the product (n) of p multiplied by q, n = pq.
   - Choose an integer, that is relatively prime to (p-1)(q-1). This will be the public exponent.
   - The public key is now (n, e).
   - Calculate d such that (de - 1) is divisible by (p-1)(q-1). This will be the private exponent.
   - The private key is now(n, d).

2. Encryption:
   - To encrypt a message (M), the sender gets the recipient's public key (n, e).
   - The sender then converts the message into an integer m so that $0 \leq m < n$.
   - The ciphertext is computed, C = m^e mod n.
   - The ciphertext (C) is sent to the recipient.

3. Decryption:
   - The ciphertext(C) is sent to the recipient
   - m is now computed using their private key (n,d) which now gives m = C^d mod n.
   - m is then converted back into text M, the plaintext

Conclusion

RSA cryptography is an important tool in information security, providing secure communication and protection of data. Understanding its components and encryption process is vital for its development and effective use in computer systems.

Thank you.

Jubilee Akputa