ENCRYPTION AND RSA

Done By

Anas Mahmoud 202201304
Mohamed Hassan 202202037
Hossam Amir 202201217

Introduction:

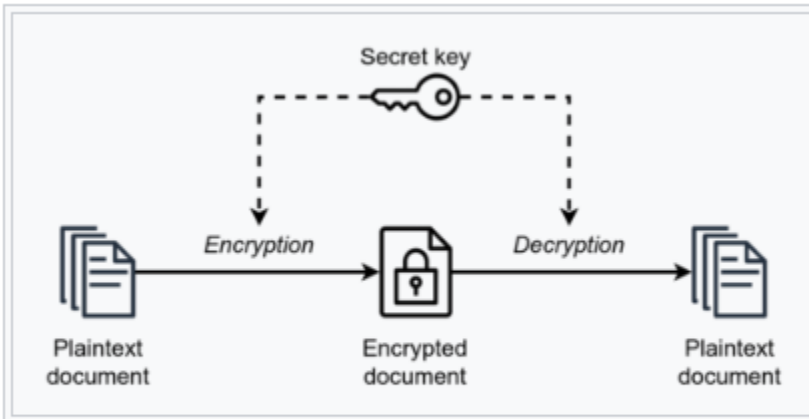
Cryptography derives from the Greek word "kryptós" and it means hiding.
Cryptography is like the art and science of securing information and communication, by converting it to meaningless(unreadable) information, to prevent unauthorized people (third parties) from accessing this data.
Throughout history the practise of trying to encrypting and decrypting information backs old civilizations it starts from simple substitution ciphers (Caesar cipher) to sophisticated encryption techniques designed(TripleDES, Towfish algoBlowfish algoAdvanced Encryption Standard (AES)) which is a very advanced ways of encryption.

Encryption has some fundamentals to ensure keeping the encrypted data safe.
1- Confidentiality: Ensuring that the information remains accessible by only the authorized people and prevents any other prying eyes.

2- Integrity: Ensuring that the information remains unchanged during transmission and description.

Encryption over time has a significant developments especially with starting of computers and internet so cryptography has two main categories:

Symmetric-key Cryptography: The symmetric-key encryption was built on the usage of single for both encryption and decryption where the same secret key is shared between the sender and receiver, like Caesar cipher and DES (Data Encryption Standard)



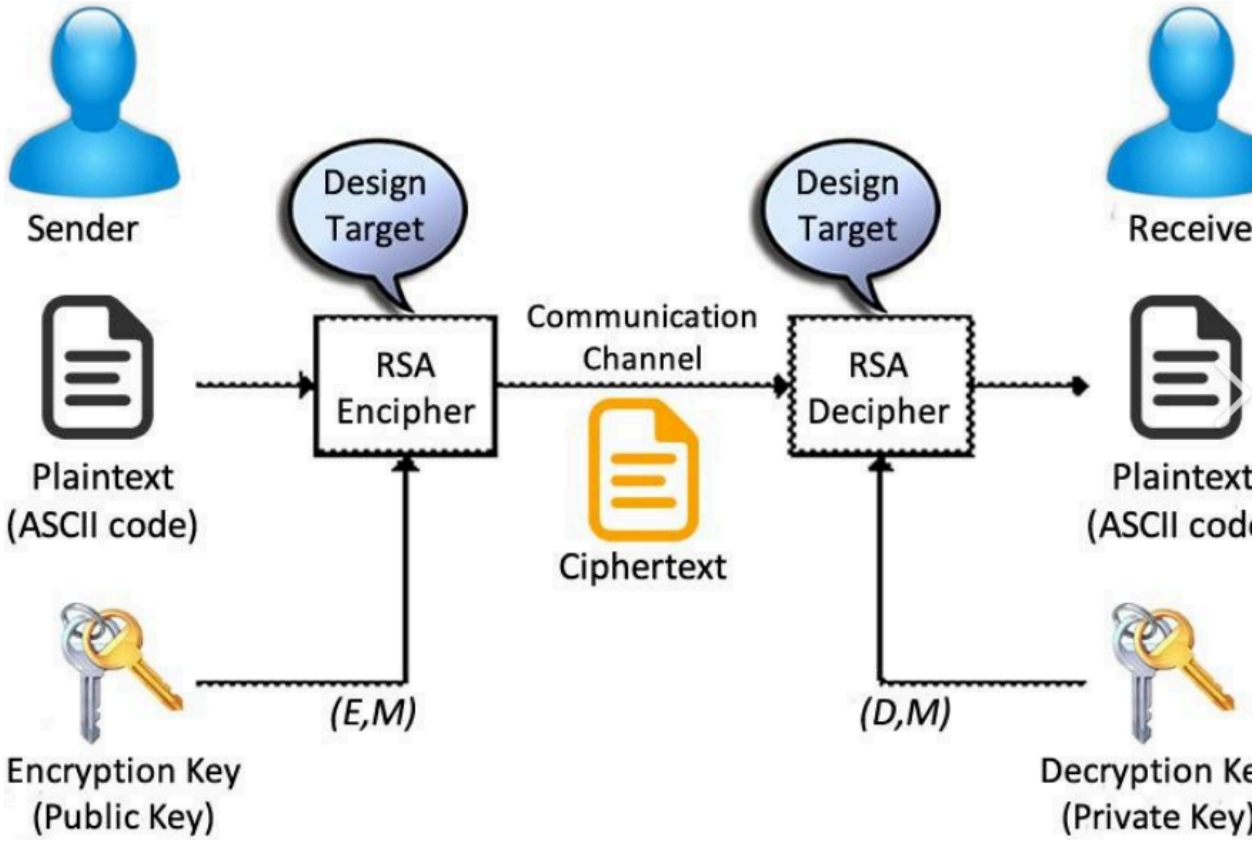
Symmetric-key encryption: the same key is used for both encryption and decryption

Asymmetric-key Cryptography (Public-key Cryptography): This algorithm was built based on a pair of distinct keys, a public key for encryption and private key for decryption. This way provides enhanced encryption and security. The **RSA** algorithm is one of the most popular algorithm in public-key cryptography

Introduction to RSA (Rivest-Shamir-Adleman) Encryption Algorithm

RSA is a public key cryptosystem, the algorithm named after **Rivest–Shamir–Adleman** the scientist who described the algorithm in 1977 but recently it was known that in 1973 there was an English mathematician Clifford Cocks who had developed an equivalent system for Government Communications Headquarters (GCHQ). In a public key cryptosystem the encryption is public and differs from the private key which is kept secret. The public key generated based on 2 large prime numbers will be explained in the math section. The security of the RSA algorithm relies on the difficulty of how to factorize the product of the 2 large prime numbers (that's why it should be large). The encryption process includes transforming plaintext(eg. message) into ciphertext using the public

key (any one can encrypt the message but not every can decrypt it)



The mechanism behind the RSA algorithm
Key Generation:

- Selection of two large prime numbers, denoted as 'p' and 'q'.
- Computation of 'n' as the product of 'p' and 'q'.
- Selection of 'e', a value coprime with '(n)', typically small, and less than '(n)'.
- Calculation of 'ϕ(n)' being equal to '(p-1)(q-1)'.

Select 2 prims large prime numbers eg.(p,q)
Now calculate n -> p*q
then get e -> **1 <e< ϕ(n)**
ϕ(n) =(P-1)(Q-1)

Then our public key is made from (n,e)
Generating the private key
$d = (k*\Phi(n) + 1) / e$ for some integer k .Then the private key is d

For example

Private Key(d = 2011) Now we will encrypt **“HI”**:

```
Convert letters to numbers : H  = 8 and I = 9
    Thus Encrypted Data c = (89^e)mod n
Thus our Encrypted Data comes out to be 1394

Now we will decrypt 1394 :
    Decrypted Data = (c^d)mod n
Thus our Encrypted Data comes out to be 89

8 = H and I = 9 i.e. "HI".
```

Below is the implementation of the RSA algorithm for

Advantages:

- **Security:** RSA algorithm is considered to be very secure and is widely used for secure data transmission.
- **Public-key cryptography:** RSA algorithm is a public-key cryptography algorithm, which means that it uses two different keys for encryption and decryption. The public key is used to encrypt the data, while the private key is used to decrypt the data.
- **Key exchange:** RSA algorithm can be used for secure key exchange, which means that two parties can exchange a secret key without actually sending the key over the network.
- **Digital signatures:** RSA algorithm can be used for digital signatures, which means that a sender can sign a message using their private key, and the receiver can verify the signature using the sender’s public key.
- **Widely used:** Online banking, e-commerce, and secure communications are just a few fields and applications where the RSA algorithm is extensively developed.
- Disadvantages:
- **Large key size:** RSA algorithm requires large key sizes to be secure, which means that it requires more computational resources and storage space.
- Vulnerability to side-channel attacks: RSA algorithm is vulnerable to side-channel attacks, which means an attacker can use information leaked through side channels such as power consumption, electromagnetic radiation, and timing analysis to extract the private key.

- Limited use in some applications: RSA algorithm is not suitable for some applications, such as those that require constant encryption and decryption of large amounts of data, due to its slow processing speed.
- **Key Management:** The secure administration of the private key is necessary for the RSA algorithm, although in some cases this can be difficult.

- **Complexity:** The RSA algorithm is a sophisticated mathematical technique that some individuals may find challenging to comprehend and use.

Challenges of RSA

1. **Complexity**: RSA is a complex mathematical method that can be difficult for some people to understand and implement1 O(N**3).
2. **Key Size**: RSA requires large prime numbers as part of the encryption process. The larger the prime numbers, the more secure the encryption, but it also increases the key size and processing time.(AspiringYouths, 2023)
3. **Speed**: RSA can be slower than other encryption methods, especially when encrypting large amounts of data.(Franklin, 2022)
4. **Vulnerability to Quantum Computing**: RSA is vulnerable to attacks by quantum computers, which can potentially break the encryption .(AspiringYouths, 2023)
5. **Key Management**: RSA requires the secure management of the private key, which can be a challenge in certain scenarios.

CASE Study:

A leading bank implements RSA encryption to secure its online banking transactions and protect sensitive customer information.

Implementation: The bank employs RSA public-key cryptography to establish secure communication channels with customers during online transactions.
Each customer has a unique public-private key pair, with the public key used for encryption and the private key for decryption.

Applications:

Online Banking Transactions:

- RSA is extensively used to secure online banking transactions and protect customer financial data.

Secure Communication:

- SSL/TLS Protocols: RSA is commonly used in the SSL/TLS protocols to secure communication over the internet. It provides a way to establish a secure and encrypted connection between a web browser and a server, ensuring the confidentiality and integrity of data.
- Email Encryption: RSA is used in email encryption to secure the content of emails, ensuring that only the intended recipient can decrypt and read the message.

Digital Signatures:

- Authentication: RSA is employed for digital signatures to verify the authenticity of digital messages or documents. Digital signatures created using RSA can ensure that the sender is who they claim to be and that the message has not been altered during transmission.
- Document Signing: In various applications, RSA is used for digitally signing documents. This is common in legal and business contexts where the authenticity of documents is crucial.

Secure Key Exchange:

- Key Establishment in Symmetric Cryptography: RSA is often used to securely exchange symmetric encryption keys between parties. Once the keys are exchanged using RSA, a more efficient symmetric algorithm is often used for the actual data encryption.

Secure Transactions:

- Digital Currency Transactions: RSA is utilized in various digital currencies and blockchain systems to secure transactions. It helps ensure the integrity and authenticity of transactions in decentralized systems.

How to enhance RSA

Combining Algorithms: RSA can be combined with other algorithms like Diffie-Hellman or ElGamal for enhanced security.(*Analysis and Design of Enhanced RSA Algorithm to Improve the Security*, 2017)

Multiple Prime Numbers: Modifying RSA to include three or four prime numbers can also enhance its efficiency.(AspiringYouths, 2023)

Exponential Powers and Multiple Public Keys: A modified approach includes exponential powers, n prime numbers, multiple public keys, and K-NN algorithm.(AspiringYouths, 2023)

Conclusion

In summary, this project aims to enhance understanding and practical proficiency in cryptography and secure communication by implementing custom algorithms alongside the RSA encryption algorithm. By exploring prime number generation, key generation, and encryption and decryption processes, the project aims to simplify the complex workings of RSA. As we navigate the complexities of modern communication and transactions, understanding the principles of cryptography becomes important. The RSA algorithm, with its elegant blend of security and efficiency, exemplifies the power of cryptographic techniques in ensuring confidentiality, integrity, and authenticity.

References

Discrete Mathematics and Its Applications
Book by Kenneth H. Rosen

Bhattacharya, A. (2020, September 23). What is RSA? How does an RSA work?

Encryption Consulting. *Encryption Consulting*.

https://www.encryptionconsulting.com/education-center/what-is-rsa/

AspiringYouths. (2023, December 7). *Advantages and Disadvantages of RSA Algorithm*.

https://aspiringyouths.com/advantages-disadvantages/rsa-algorithm/

Franklin, R. (2022, November 14). *AES vs. RSA Encryption: What Are the Differences?*

Precisely. https://www.precisely.com/blog/data-security/aes-vs-rsa-encryption-differences

How can I enhance the security level of my RSA code? (n.d.). Cryptography Stack Exchange.

https://crypto.stackexchange.com/questions/90029/how-can-i-enhance-the-security-level-of-my-rsa-code