C Mini Project Presentation
on
Government document storage and distribution using blockchain

Student: Aashish Nandakumar

Guide: Dr Kiran P

Department of Computer Science and Engineering
RNS Institute of Technology
2022-23

RSA

Introduction

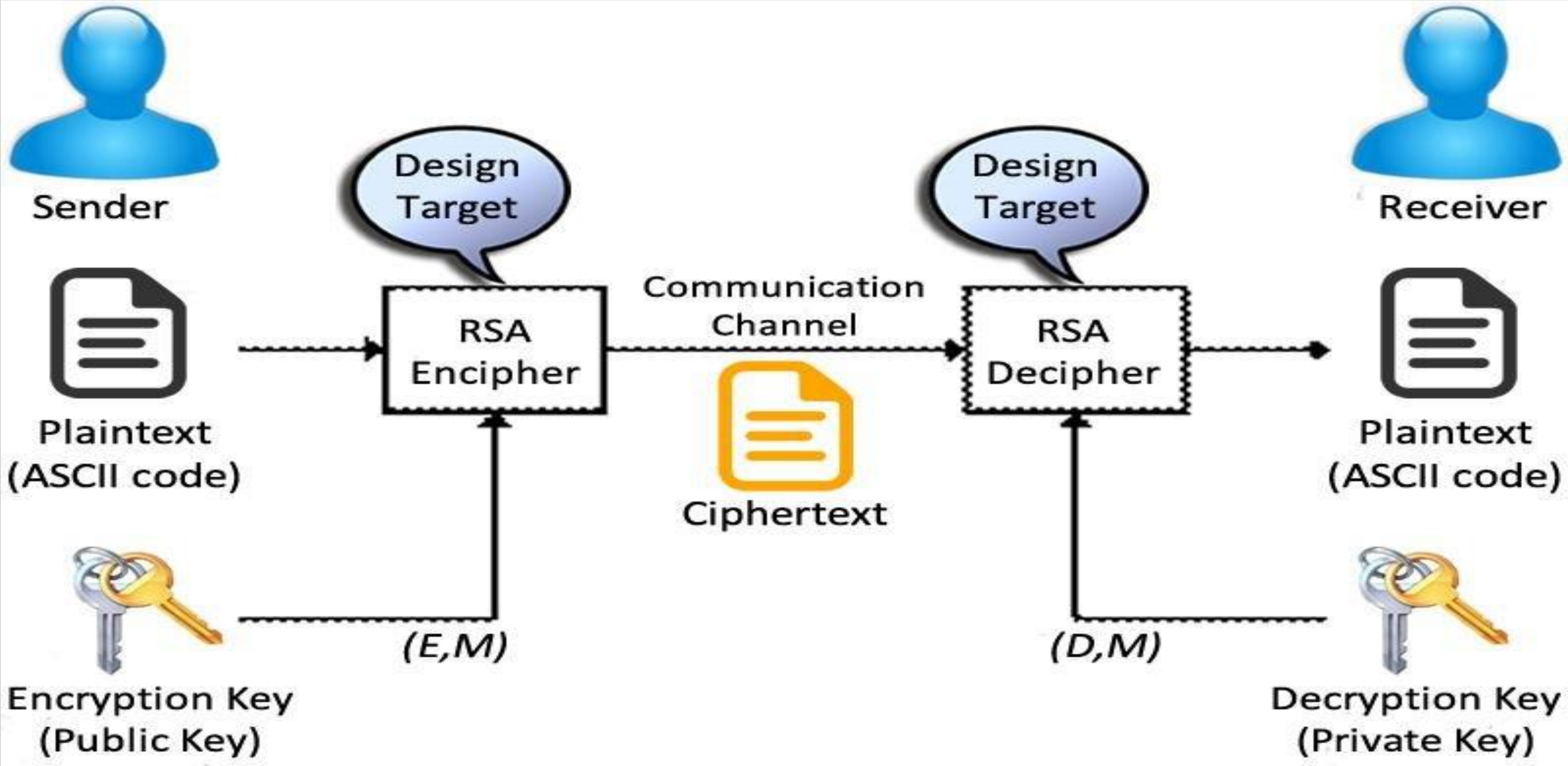
- ❑ RSA is a **public-key cryptography algorithm** used to secure data transmission.
- ❑ It is named after it's inventors Ron Rivest, Adi Shamir, and Leonard Adleman.
- ❑ The algorithm uses a pair of keys, a public key for encryption and a private key for decryption.
- ❑ It is widely used for secure online transactions such as online banking, e -commerce, and secure mail communication.
- ❑ It is believed to be secure against attacks by classical computers, but advances in quantum computing may possess a threat.

Problem Statement

The problem of secure data transmission over insecure communication channels.

- ❑ RSA enables two parties to communicate securely over the internet or any other communication channel, even if the channel is not secure or may be intercepted by an attacker.
- ❑ RSA algorithm uses a pair of key for encryption and a private key for decryption, to secure data.
- ❑ The security of the algorithm is based on the mathematical complexity of factoring large prime numbers.
- ❑ This makes it difficult for an attacker to decrypt the data without the private key.

Flowchart


Sender
Design Target
Design Target
Receiver
Communication Channel
Plaintext (ASCII code)
RSA Encipher
RSA Decipher
Plaintext (ASCII code)
Ciphertext
(E,M)
(D,M)
Encryption Key (Public Key)
Decryption Key (Private Key)

Algorithm

1. Choose two large prime numbers, p and q.
2. Calculate $n = p*q$.
3. Calculate the totient of n: $\text{phi}(n) = (p-1) * (q-1)$
4. Choose an integer e such that $1 < e < \text{phi}(n)$ and $\gcd(e, \text{phi}(n)) = 1$, this is the public key.
5. Calculate the private key d, such that $d * e = 1(\text{mod phi}(n))$.
6. The public key (n, e) and the private key is (n, d).
7. To encrypt a file we need to first convert it into bytes, once it is in bytes use the formula: $c = m ^ e \bmod n$.
8. To decrypt the ciphertext use the formula: $m = c ^ d \bmod n$.

Results

- ❑ Secure data transmission: RSA algorithm provides a secure way to transmit data over insecure communication channels
- ❑ Public key distribution: RSA algorithm allows for the distribution of public keys, which can be shared with anyone and are used for encryption.
- ❑ Digital signatures: RSA algorithm can be used to create digital signatures, which can be used to verify the authenticity of data.
- ❑ Key exchange: RSA algorithm can be used for key exchange. Which is a process of securely exchanging keys between two parties
- ❑ Slow performance: RSA algorithm is relatively slow compared to other encryption algorithms, especially for large data.

Conclusion

- ❑ RSA algorithm is based on the mathematical complexity of factoring large prime numbers, which makes it secure against attack by classical computers.
- ❑ RSA encryption can be done with different key sizes, typically ranging from 1024 bits to 4096 bits.
- ❑ It’s importance is likely to continue as society becomes more reliant on secure online transactions and communication.
- ❑ RSA algorithm has a wide range of applications:
  - ❑ Encryption for government and military uses
  - ❑ Password protection
  - ❑ Secure online transactions
  - ❑ Digital signature

Thank you