CMC UNIVERSITY

RSA ALGORITHMS REPORT

2023

TABLE OF CONTENTS

INTRODUCTION

Currently, data is generated and collected on a massive scale from various sources, including mobile devices, personal computers, servers, IoT sensors, and social media systems.
However, managing and securing data has become a significant challenge for organizations and individuals. Data security has become increasingly critical. The RSA algorithm is one of the important algorithms forencrypting information.
RSA is a public-key crypto system that was developed in 1977 by Ronald Rivest, Adi Shamir, and Leonard Adleman. The algorithm is named after the first letter of each of their last names. RSA is widely used in information security systems to encrypt and decrypt data.
The RSA algorithm is based on the mathematical properties of large prime numbers and thedifficulty of factoring them. The algorithm uses a pair of keys, including a public key and a private key, to encrypt and decrypt messages.
The public key is used to encrypt messages, and only the owner of the private key can decrypt those messages.
The private key is used to decrypt messages, and only the owner of the private key can possess that key.
The RSA algorithm is considered one of the most secure and reliable public-key encryption algorithms, and it is widely used in various applications, including email passwords, access authentication, data encryption, and many other security systems.
In this paper, I provide a comprehensive overview of the algorithm's history, properties, and applications.

BACKGROUND

Defination - 01

The greatest common divisor is the largest natural number that divides both a and b without leaving a remainder. Synonyms for GCD include greatest common factor (GCF), highest common factor (HCF), highest common divisor (HCD), and greatest common measure (GCM).
The greatest common divisor is often written as gcd(a, b) or, more simply, as (a, b), although the latter notation is ambiguous, also used for concepts such as an ideal in the ring of integers, which is closely related to GCD.

Defination - 02

Prime numbers: RSA uses the properties of prime numbers to secure messages. Prime numbers arenumbers that can only be divided by 1 and themselves. Finding large prime numbers is an importantand difficult mathematical problem.

Defination - 03

Prime factorization: RSA uses prime factorization to create the public and private keys. Prime factorization is the processof finding prime numbers that multiply to create a natural number

EUCLIDEAN ALGORITHM

The Euclidean algorithm repeatedly divides the larger number by the smaller number and takes the remainder until there remainder is zero.

At that point, the greatest common divisor is the last non-zero remainder. The formula for theEuclidean algorithm can be expressed as follows:

GCD(A, B) = GCD (B, A MOD B)
IF B ≠ 0 GCD(A, 0) = A

Here, a mod b denotes the remainder when a is divided by b.

The Euclidean algorithm is a simpleand efficient algorithm for computing the greatest common divisor of two positive integers.

Fermat's little theorem:
If p is a prime number, then for integers any a:

$$ap \equiv a(\text{mod } p)$$

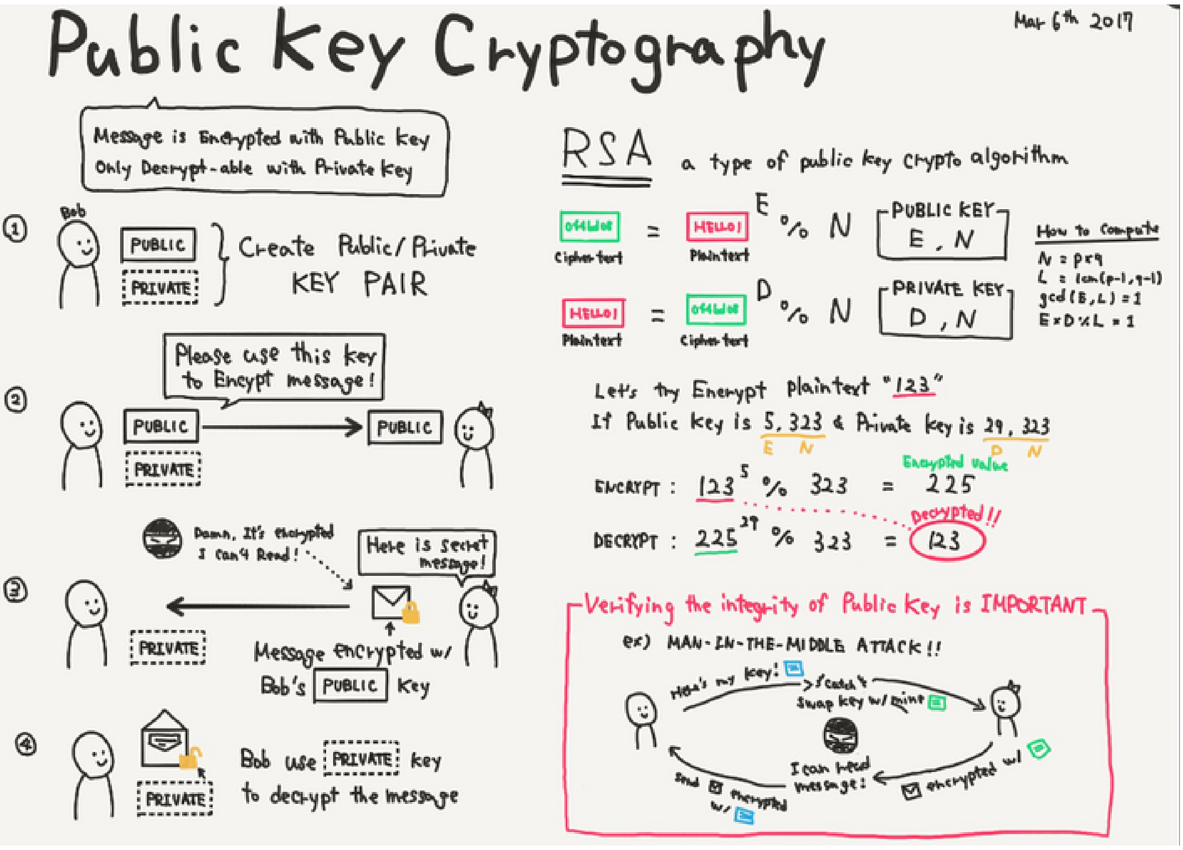
MAIN RESULT

Brief description

The RSA algorithm has two keys: the public key and the private key.

Each key is a fixed number used in the process of encryption and decryption. The public key is widely published and used forencryption. Information encrypted with the public key can only be decrypted with the corresponding private key. In other words, anyone can encrypt but only the person who knows the private key candecrypt.

A visual analogy for a public key cryptography system is as follows:
B wants to send A a secret message that only A can read. To do this, A sends B an open box andkeeps the key. B receives the box, puts a regular letter inside, and locks it (like a regular lock that cannot be opened once locked).



Public Key Cryptography
Mar 6th 2017
Message is Encrypted with Public key
Only Decrypt-able with Private key
①
Bob
PUBLIC
PRIVATE
Create Public/Private KEY PAIR
②
Please use this key to Encypt message!
PUBLIC
PRIVATE
PUBLIC
③
Damn, It's encrypted I can't Read!
Here is secret message!
PRIVATE
Message encrypted w/ Bob's PUBLIC key
④
PRIVATE
Bob use PRIVATE key to decrypt the message
RSA
a type of public key crypto algorithm
Cipher text = HELLO! E % N
Plaintext
PUBLIC KEY E , N
HELLO! = Cipher text D % N
PRIVATE KEY D , N
How to Compute
N = p×q
L = lcm(p-1, q-1)
gcd(E, L) = 1
E×D % L = 1
Let's try Encrypt plaintext "123"
If Public key is 5, 323 & Private key is 29, 323
E N
D N
Encrypted value
ENCRYPT : 123^5 % 323 = 225
Decrypted!!
DECRYPT : 225^29 % 323 = 123
Verifying the integrity of Public Key is IMPORTANT
ex) MAN-IN-THE-MIDDLE ATTACK!!
Here's my key!
catch Swap key w/ mine
I can read message!
encrypted w/
Send encrypted w/

Then, B sends the box back to A. A opens the box with their key and reads the message inside. In this example, the open box with the key plays the role of the public key, and the key itself is the private key.

HOW TO USED RSA ALGORITHMS?

Here, you can add a steps explaining your algorithm.

Key generation

100

readers appreciate accurate information

100

readers appreciate accurate information

STEP 1

Choose two big prime p, q (p ≠q) randomly r and independent

STEP 2

Calculate n = pq

STEP 3

Calculate (n) = (p- 1)(q - 1)

STEP 4

Choose a integer number e which satisfy 1 < e < (n); e and (n) is co-prime

Calculate d which satisfy de ≡ e^(-1)(mod (n)).

STEP 5

- **Public key**

The specified pair of numbers n and e forms the RSA public key

- **Private key**

Includes n and d, where d is the decryption function and is kept secret.

§ Encryption

ap Ξ a(mod p)

§ Decryption

m = cd mod n

EXAMPLES

01 — Key Generation

Choose two distinct prime numbers p and q: p = 11 and q = 3.
Compute n = p*q: n = 33.
Compute (n) = (p-1)(q-1): (n) = 20.
Choose an integer e such that 1 < e < (n) and e is coprime to (n): e = 7.
Compute the integer d such that d ≡ e^(-1) (mod (n)): d = 3.
The public key is (n, e) = (33, 7)and the private key is (n, d) = (33, 3).

02 — Encryption

Suppose we want to encrypt the message M = 5.

- Convert M into a number m such that 0 < m < n: m = 5.
- Compute the ciphertext c = m^e (mod n): c = 5^7 (mod 33) =29.

The ciphertext is c = 29.

03 — Decrytion

To decrypt the ciphertext c = 29, we use the private key (n, d) = (33, 3).

- Compute the plaintext m = c^d (mod n): m = 29^3 (mod 33) = 5.

The plaintext is m = 5, which is theoriginal message M that was encrypted

APPLICATIONS

Secure communication: The RSA algorithm is widely used in secure communication protocols to ensure the confidentiality and integrity of data transmitted over the internet.
It isused in protocols such as SSL/TLS, SSH, and PGP to encrypt and decrypt messages.

Digital signatures: The RSA algorithm can be used to create digital signatures, which are used to verify the authenticity and integrity of digital documents. A digital signature is createdby encrypting a message digest with the sender's private key. The recipient can verify the signature by decrypting it with the sender's public key.

Key exchange: The RSA algorithm can be used for key exchange in symmetric-key cryptography. Two parties can use the RSA algorithm to exchange a shared secret key withouttransmitting it over the network.

CONCLUSION

In conclusion, RSA is a widely used and secure public-key encryption algorithm that is based on thedifficulty of factoring large prime numbers. One of the strengths of RSA is that it provides both confidentiality and authentication. It is often used to secure sensitive data such as financialtransactions, online communication, and digital signatures.

HIGHLIGHT 1

- RSA is a widely used and secure public-key encryption algorithm that is based on the difficulty of factoring large prime numbers.

HIGHLIGHT 2

- One of the strengths of RSA is that it provides both confidentiality and authentication.
- It is often used to secure sensitive data such as financialtransactions, online communication, and digital signatures.

HIGHLIGHT 3

- However, RSA is not perfect and has some limitations. One of the main challenges is the key size,which needs to be sufficiently large to provide adequate security.

Additionally, RSA is vulnerable to certain attacks such as side-channel attacks and chosen ciphertext attacks.
Despite its limitations, RSA remains an important and widely used cryptographic algorithm. It hasbeen instrumental in enabling secure communication and e-commerce on the internet and will likely continue to play a critical role in cybersecurity for years to come.

REFERENCE

[1] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures andpublic-key cryptosystems," Communications of the ACM, vol. 21, no. 2, pp. 120-126, 1978.

[2] Stark 1978, p. 16

[3]   Rosen, K. H. (2018). Elementary Number Theory and Its Applications (7th ed.).Pearson.

[4] https://en.wikipedia.org/wiki/Euclidean_algorithm#:~:text=In%20mathematics%2C%20the%20Euclidean%20algorithm,them%20both%20without%20a%20remainder.

[5] "Elementary Number Theory" by David M. Burton - This is a popular textbook on numbertheory that covers Fermat's little theorem and other important topics in the field.

[6]   https://vi.wikipedia.org/wiki/RSA_(encrytion)

Thank you for reading with various details about RSA algorithms to support in our project report

Contact

22IT1 - BIT220049

CMC University
84 Nguyen Thanh Binh,
Viet Nam

CMC UNIVERSITY