Hai Hoang Minh – BIT220049

CMC UNIVERSITY

22IT1- Information Technology

RSA Algorithms project

*20 Dec,* *2023*

**RSA** **ALGORITHM**

CMC University

84 Nguyen Thanh Binh, Viet Nam

## Abstract

This paper is a study of RSA Algorithm, is a commonly used public-key encryption algorithm that is widely used. In it, I will study the theoretical basis of the algorithm and some applications

# 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 for encrypting information.

RSA is a public-key cryptosystem 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**[1]**. 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 the difficulty 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

#### Definition

*Definition* *1*: 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)**[2]**, 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.

*Definition* *2:* Prime numbers: RSA uses the properties of prime numbers to secure messages. Prime numbers are numbers that can only be divided by 1 and themselves. Finding large prime numbers is an important and difficult mathematical problem.

*Definition* *3:* Prime factorization: RSA uses prime factorization to create the public and private keys. Prime factorization is the process of finding prime numbers that multiply to create a natural number**[3]**.

#### Euclidean algorithm

The Euclidean algorithm repeatedly divides the larger number by the smaller number and takes the remainder until the remainder is zero. At that point, the greatest common divisor is the last non-zero remainder. The formula for the Euclidean algorithm can be expressed as follows:**[4]**

**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 simple and efficient algorithm for computing the greatest common divisor of two positive integers.

* 1. Fermat's little theorem: If p is a prime number, then for integers any a:**[5]**

# Main result

**ap** **Ξ** **a(mod** **p)**

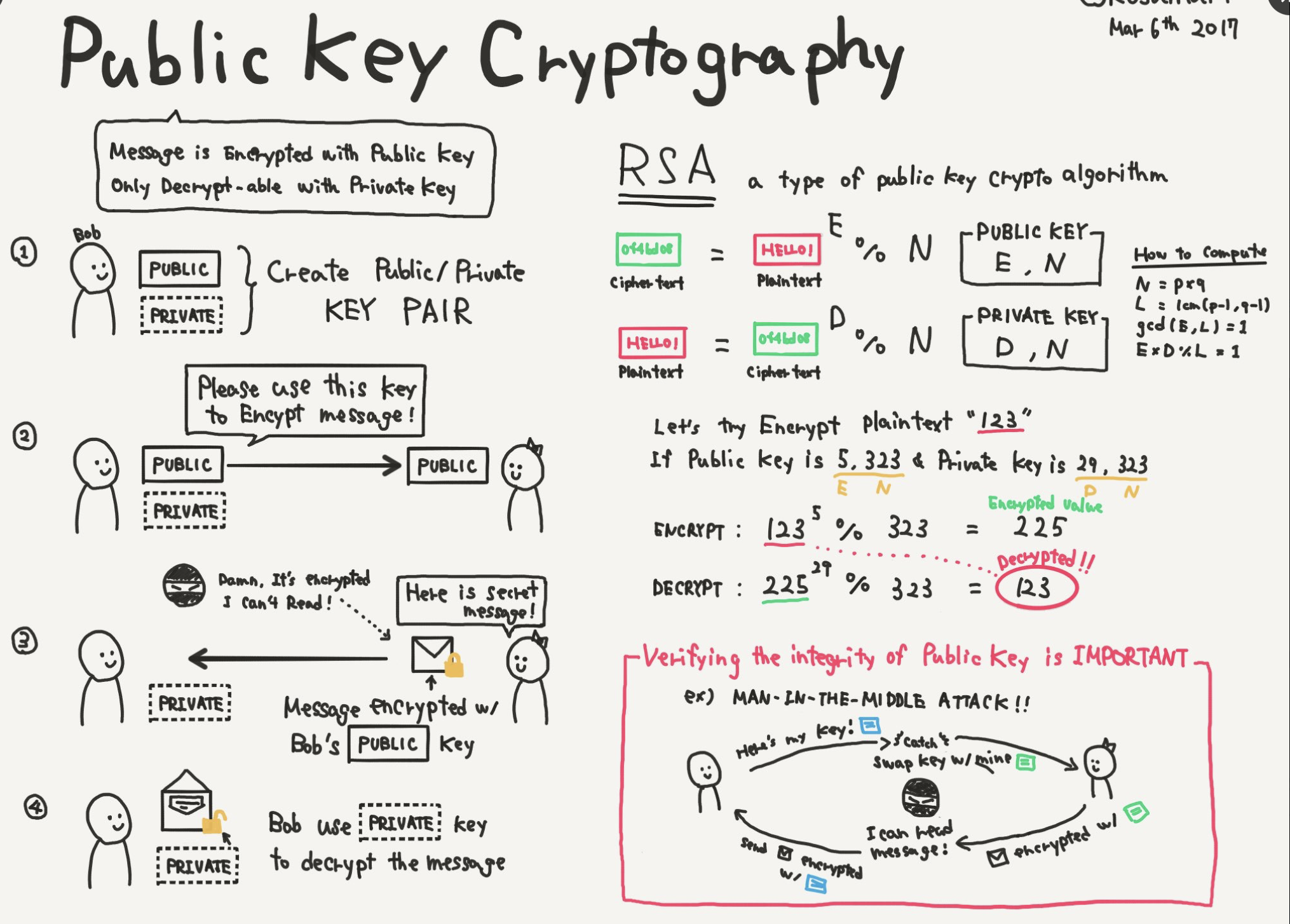
#### Brief description

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 for encryption. 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 can decrypt.

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 and keeps the key. B receives the box, puts a regular letter inside, and locks it (like a regular lock that cannot be

opened once locked). 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.



#### RSA algorithm

* + - *Key generation****[6]***

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.

Step 5: Calculate d which satisfy de ≡ e^(-1)( mod (n)).

* + - * 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*

Suppose B wants to send a message M to A. First, B converts M into a number m < n using a reversible function (from m, M can be determined) that was agreed upon beforehand.

At this point, B has m and knows n and e, which were sent by A. B will calculate c, the ciphertext of m using the formula:

c = me mod n

* + - * + *Decryption*

A receives ciphertext c from B and knows the private key d. A can obtain plaintext m from c using the following formula:

m = cd mod n

Given m, A retrieves M using the agreed-upon method. The decryption process works because we have:

cd ≡ (me)d ≡ med (mod n)

Since ed ≡ 1 (mod p-1) and ed ≡ 1 (mod q-1), (according to Fermat's little theorem), we have:

and

med ≡ m (mod p)

med ≡ m (mod q)

Since p and q are two coprime prime numbers, we can apply the Chinese remainder theorem, and we get:

med ≡ m (mod pq)

or:

#### Example

cd ≡ m (mod n).

Here is an example of the RSA algorithm:

1. 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).

1. 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.

1. Decryption:

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.

#### Some 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 is used 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 created by 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 without transmitting it over the network.

# Conclusion

In conclusion, RSA is a widely used and secure public-key encryption algorithm that is based on the difficulty 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 financial transactions, online communication, and digital signatures.

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 has been 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 and public-key cryptosystems," Communications of the ACM, vol. 21, no. 2, pp. 120-126, 1978.

### Stark 1978, p. 16

1. Rosen, K. H. (2018). Elementary Number Theory and Its Applications (7th ed.). Pearson.
2. *https://en.wikipedia.org/wiki/Euclidean\_algorithm#:~:text=In*

*%20mathematics%2C%20the%20Euclidean%20algorithm,them*

*%20both%20without%20a%20remainder.*

1. *"Elementary* *Number* *Theory"* *by* *David* *M.* *Burton* *-* *This* *is* *a* *popular* *textbook* *on* *number* *theory* *that* *covers* *Fermat's* *little* *theorem* *and* *other* *important* *topics* *in* *the* *field.*
2. *https://vi.wikipedia.org/wiki/RSA\_(encrytion)*