International Journal of Applied Mathematics
Volume 39 No. 1s 2026,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

# Foundations of Number Theory in the Design and Security of the RSA Cryptosystem

Sonam Namdev Gawande[1] Kailas Sahadu Ahire[2]

[1]Mahatma Gandhi Vidyamandir's,
Maharaja Sayajirao Gaikwad Arts, Science & Commerce College, Malegaon,
Malegaon Camp, District Nashik, Maharashtra, India.
E-mail: sonamgawande@gmail.com
[2]Mahatma Gandhi Vidyamandir's,
Maharaja Sayajirao Gaikwad Arts, Science & Commerce College, Malegaon,
Malegaon Camp, District Nashik, Maharashtra, India.
E-mail: ksahire111@gmail.com

## 1 ABSTRACT

In today's digital communication world, protecting data from unauthorized access and cyber threats is crucial, for cryptographic techniques are to protect information security. Cryptography supplies substorage system security and secrecy, including digital signature authentication.In the field of mathematical cryptography, the Rivest, Shamir, and Adleman (RSA) Algorithm endures as one of the most secure and extensively used public-key cryptography algorithms.RSA cryptography is used to secure the encryption key between sender and receivers. The role of number n in RSA is important and depends on primes, Euler's totient function, modular inverses, and applications of Fermat's Little Theorem and Euler's Theorem. This abstract has introduced the foundations of mathematics for cryptography and the RSA public-key cryptosystem for secure communication in mathematical aspects.

## 2 Keywords

Cryptography, RSA algorithm, data security, decryption, encryption,cipher text,Key generation.

Received: August 06, 2025

International Journal of Applied Mathematics
Volume 39 No. 1s 2026,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

# 3 Introduction

If two buddies wish to talk confidentially, the first one will share it versus Hello, the term encryption refers to this coded form. express as

$$C = M^e (mod n) \tag{1}$$

Where 'c' is the ciphertext, 'd' is the private decryption key, 'n' is the public modulus, and 'M' is the original message [1].
Any conversion from plain text into cipher text is referred to as encryption,express as

$$M = C^d (mod n) \tag{2}$$

Here method to secure message is called Cryptography. Here the prefix "crypt" means "hidden" and suffix "graphy" stands for "writing".
To protect information and communication from an unauthorized person, cryptography plays a vital role.Integers greater than one that can only be divided by 1, and themselves are known as prime numbers. Prime numbers are special and very important in mathematics, especially in cryptography [2] because of their characteristic. With the help of cryptography, we can send or keep private data via unprotected networks, such as the Internet, such that only the intended receiver can read it. The science of studying and cracking encrypted communication is known as cryptanalysis, whereas the science of protecting data is known as cryptography. Analytical reasoning, mathematical tool application, and pattern recognition are all intriguingly combined in classical cryptanalysis. discovery, perseverance, willpower, and good fortune. Attackers are another name for cryptanalysts. Cryptography and cryptanalysis are both included in cryptology. The difficulty of factoring huge numbers into their original prime components is what makes prime numbers of such significance in cryptography. Multiplying two huge prime numbers yields a massive number that is very difficult to divide into the two original primes. Many existing encryption schemes are based on this challenge. Prime numbers are used in a wide range of cryptographic applications that span our digital life.Prime numbers are used in an extensive variety of cryptographic applications that span our digital life. For instance, RSA encryption is used in online transactions to safeguard personal information and credit card numbers while they are being processed. Email providers also employ encryption to protect the privacy of communications by restricting access to the email content to the intended recipient. Cryptography is divided into three types.

Received: August 06, 2025

International Journal of Applied Mathematics
Volume 39 No. 1s 2026,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

1) Symmetric key cryptography

2) Asymmetric key cryptography

3) One way hash function

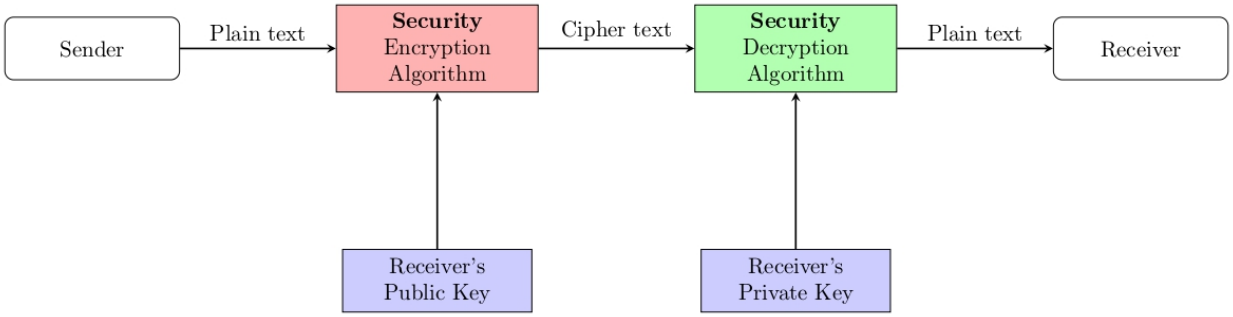


Figure 1: Encryption and Decryption algorithm

In this paper include some concept,definitions and related work to Mathematics and RSA public key cryptography from some references it includes [3] and Mathematics of Public Key Cryptography. Version 2.0 Steven D Galbraith October 31, 2018 [4]

# 4 RSA

This cryptosystem is very famous and oldest public key cryptosystem that still in used. RSA is invented in 1978 by Ron Rivest Adi Shamir and Leonard Adleman [5].In their algorithm security relies on the difficulty of factoring large composite numbers.

The history of RSA begins in 1973, when British mathematician Clifford Cocks, working at the UK intelligence agency GCHQ, discovered a method similar to what would later become RSA. However, his work remained classified until 1997 and was not known to the public.

In 1977, RSA was publicly invented by three researchers at MIT: Ron Rivest, Adi Shamir, and Leonard Adleman. Their work laid the foundation for one of the first and most widely used public-key cryptosystems. The RSA algorithm was officially published in 1978 in a landmark paper titled "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems." This paper introduced the principles of RSA encryption to the wider cryptographic community. Later, the RSA algorithm was patented in the United States under patent number 4,405,829. This patent eventually expired in 2000, after which RSA became freely available for public use, leading to its widespread adoption in secure communications around the world.

When Similar key is used for encryption and decryption then it is symmetric cryptography and different key is used for encryption and decryption is called asymmetric cryptography. A private key is a private, secret code that is used to decode messages or generate signatures, whereas a

Received: August 06, 2025

public key is used to encrypt messages or authenticate signatures and is accessible to everyone. RSA provides confidentiality,integrity,authenticity and non-reputability of communications and data storage

## Key Generation Algorithm [6]

1) Select two large prime numbers $p$ and $q$, then with the help of $p$ and $q$ calculate $n = pq$, where the length should be 1024 bits.
2) $\phi(n) = (p-1)(q-1)$
3) Choose an integer $e$ such that $1 < e < \phi(n)$, and $\gcd(e, \phi(n)) = 1$.
4) Compute the secret exponent $d$ so that

$$1 < d < \phi(n)$$

and

$$ed \equiv 1 \pmod{\phi(n)}.$$

5) Here (n,e) is public key and (d,p,q) is private key

## Computational steps for selecting the prime p and q in RSA cryptography

1) Select size 1024 bits.
2) To generate prime integer use high quality random number B/2 that is 1024
3) Choice odd number and set lowest bits.
4) Use Miller-Rabin to check if it is prime
5) Repeat for q
6) p and q should be not equal to each other
7) Compute n=pq and $\phi(n) = (p-1)(q-1)$

Received: August 06, 2025

International Journal of Applied Mathematics
Volume 39 No. 1s 2026,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

# 5 Mathematical concept behind RSA Cryptography [7]

**1.Division Algorithm for Integers-**

Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exist unique integers $q, r \in \mathbb{Z}$ such that:

$$a = bq + r, \quad \text{where } 0 \leq r < b.$$

If $r = 0$, we say that $b$ divides $a$, denoted $b \mid a$.

**2.Greatest Common Divisor**

Let $a, b \in \mathbb{Z}$. A positive integer $d$ is the *greatest common divisor* (gcd) of $a$ and $b$, denoted $\gcd(a, b)$, if:

$d \mid a$ and $d \mid b$,For any positive integer $c$, if $c \mid a$ and $c \mid b$, then $c \mid d$.

**3.Prime Integer**

An integer $p \geq 2$ is said to be *prime* if its only positive divisors are 1 and $p$. Primality and coprimality play a central role in the arithmetic of the RSA cryptosystem.

**4.**Every positive integer n and every a that is co-prime to n, then it must true a

$$a^{\phi(n)} \equiv 1 \pmod{n}, \quad \text{where } \phi(n) \text{ is Euler's totient function.}$$

If a and n are relatively prime, then hen it must be true for $k_1$, $k_2$ such that

$$a^k \equiv a^{(k_1 * \phi(n) + k_2)} \equiv a^{(k_1 * \phi(n))} a^{k_2} \equiv a^{k_2 (mod n)}$$

**5.Fermat little theorem-**

Ler p be the prime number and a be an integer such that $p \nmid a$ then
$a^{\phi(n)} \equiv 1 \pmod{n}$,

If n is prime, then the algebraic group $\mathbb{G}_m(\mathbb{Z}/n\mathbb{Z}) = (\mathbb{Z}/n\mathbb{Z})^*$ over the ring $\mathbb{Z}/n\mathbb{Z}$ has n-1 elements.

Received: August 06, 2025

International Journal of Applied Mathematics
Volume 39 No. 1s 2026,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

In other words, if $a$ is an integer such that $\gcd(a, n) = 1$ and

$$a^{n-1} \not\equiv 1 \pmod{n},$$

then n is not prime. Such a number $a$ is called a *compositeness witness* for n.

**6.Miller-Rabin test-**

Suppose p is an odd prime and write p-1 as $2^k - q$ where q is odd number then for any integer a co prime to p ,one o

$$a^q \equiv 1(mod p) \text{ or}$$

$$a^q, a^{2q}, a^{4q}, .....a^{2(k-1)q} \text{is -1 modulo p}$$

**7.Chinese Remainder theorem-**

A system of simultaneous linear congruences can be solved utilizing the Chinese Remainder Theorem Let $a_1, a_2, \ldots, a_k$ be integers and $m_1, m_2, \ldots, m_k$ be pairwise coprime positive integers. Let

$$M = \prod_{i=1}^{k} m_i.$$

Assuming that

$$M_i = \frac{M}{m_i}$$

for every $i$, the integer $M_i$ has a multiplicative inverse modulo $m_i$ since $\gcd(M_i, m_i) = 1$; any such inverse is indicated by $M_i^{-1}$, that is,

$$M_i M_i^{-1} \equiv 1 \pmod{m_i}.$$

Following that, the system's unique solution $y$ modulo $M$ is found as

$$\begin{aligned} y &\equiv a_1 \pmod{m_1}, \\ y &\equiv a_2 \pmod{m_2}, \\ &\vdots \\ y &\equiv a_k \pmod{m_k}. \end{aligned}$$

Received: August 06, 2025

International Journal of Applied Mathematics
Volume 39 No. 1s 2026,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

The constructive formula that achieves this is given by

$$y = \left( \sum_{i=1}^{k} a_i \, M_i \, M_i^{-1} \right) \bmod M, \qquad y \in \{0, 1, \ldots, M-1\}.$$

**8.Carmichael Number-** An integer $n \in \mathbb{N}$ is a Carmichael number if n is composite and

$$a^{n-1} \equiv 1 \pmod{n}$$

for all $a \in \ltimes$ such that $\gcd(a, n) = 1$.

If

$$N = \prod_{i=1}^{l} p_i^{e_i}$$

is composite, then

$$\mathbb{G}_m(\mathbb{Z}/N\mathbb{Z}) \cong \prod_{i=1}^{l} \mathbb{G}_m(\mathbb{Z}/p_i^{e_i}\mathbb{Z}),$$

and has order $\varphi(n)$ and exponent

$$\lambda(N) = \operatorname{lcm}\left\{ p_i^{e_i - 1}(p_i - 1) : 1 \le i \le l \right\}.$$

**9.Fixed Padding Schemes in RSA-**

One simple proposal for $\kappa$-bit RSA moduli is to take a $\kappa'$-bit message and pad it by putting $(\kappa - \kappa' - 1)$ ones to the left-hand side of it. This brings a short message to full length. This padding scheme is sometimes called fixed pattern padding. Suppose short messages (for example, 128-bit AES keys $K$) are being encrypted using this padding scheme with $\kappa = 1024$. Then

$$m = 2^{1024} - 2^{128} + K.$$

Suppose also that the encryption exponent is $e = 3$. Then the ciphertext is

$$c = m^3 \ (mod n).$$

If such a ciphertext is intercepted then the cryptanalyst only needs to find the value for $K$. In this case, we know that $K$ is a solution to the polynomial

$$F(x) = (2^{1024} - 2^{128} + x)^3 - c \equiv 0 \pmod{n}.$$

Received: August 06, 2025

International Journal of Applied Mathematics
Volume 39 No. 1s 2026,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

This is a polynomial of degree 3 with a root modulo $n$ of size at most $n^{128/1024} = n^{1/8}$. So Coppersmith's method finds the solution $K$ in polynomial time.

**10.To test Primality:**

To choose a large prime number,

$\lim_{x\to\infty} \frac{\pi(x)}{x/logx} = 1$

$\pi(x)$ stands for the number of primes that do not exceed $x$,

that is, up to $x$ there are approximately $\frac{x}{\log x}$.

If we pick a large integer n, then

$$\{n, n+1, \ldots, n+2\lfloor \log n \rfloor\}$$

# 6 Conclusion

Although it is computationally challenging to factor massive amounts of data, the RSA technique is the most safe and reliable when compared to other cryptographic algorithms [8].The prime numbers ”p” and ”q” must be approximately of the same size. There should be enough of a distinction between ”p” and ”q” to keep them from attacking. In order to ”sign” a message using RSA, the sender must generate a hash value for the message to be delivered, raise it to the power of d mod n (as in decryption), and then attach it to the message as a ”signature.” is utilized in hundreds of software products today and can be applied to digital signatures, key exchange, and small-block data encryption. There is currently no known technique that can factorize the number that is formed by two huge prime numbers that are approximately equal size in a reasonable amount of time. Users can simply raise the key size in RSA, which provides protection. Nearly every security solution currently in use on the Internet for private communications, including the majority of Public Key Infrastructure (PKI) systems at the organizational level, uses the optimal mechanism made possible by RSA.

Received: August 06, 2025

# References

[1] Bárbara Emma Sánchez Rinza and Carlos Ignacio Robledo Sánchez. Cryptographic system using rsa. *International Journal of Computer Science and Information Security (IJCSIS)*, 2020. Benemerite Autonomous University of Puebla, Mexico. Available at `https://www.ijcsis.org/`.

[2] Journal of discrete mathematical sciences and cryptography, 2024. Indexed in ESCI (Emerging Sources Citation Index), (2024).

[3] Saranya, Vinothini, and Vasumathi. A study on rsa algorithm for cryptography. *International Journal of Computer Science and Information Technologies (IJCSIT)*, 5(4):5708–5709, 2014. Available online at `http://www.ijcsit.com`.

[4] Steven D. Galbraith. *Mathematics of Public Key Cryptography*. Cambridge University Press, Cambridge, United Kingdom, 2012. Version 2.0 (2018 update available online).

[5] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[6] M. Preetha and M. Nithya. A study and performance analysis of rsa algorithm. *International Journal of Computer Science and Mobile Computing (IJCSMC)*, 2(6):126–139, 2013. Available online at `http://www.ijcsmc.com`.

[7] Joshua Pite and Yiying Zhong. The rsa cryptosystem. Expository paper, mentored by Honglin Zhu, 2024. Provides a historical and technical overview of the RSA public key cryptosystem.

[8] Xin Zhou and Xiaofei Tang. Research and implementation of rsa algorithm for encryption and decryption. In *Proceedings of 2011 6th International Forum on Strategic Technology*, volume 2, pages 1118–1121, 2011.

Received: August 06, 2025