# Mathematics Behind RSA Cryptosystem

**Gawande Sonam Namdev** snmgawande123@gmail.com

Ahire kailas Sahadu ksahire111@gmail.com
M.S.G.Arts,Science and Commerce College Malegaon camp, Dist.Nashik

## 1 Abstract

The science of employing mathematics to conceal data behind encryption is known as cryptography. Number theory is a key component of cryptog- raphy, which ensures that information cannot be easily recovered without special knowledge. There are several ways to accomplish this. The RSA (Rivest, Shamir, Adleman) technique, which uses asymmetric cryptography, commonly referred to as public-key cryptography, to o er outstanding en- cryption and performance. It is necessary to have understanding of number theory, modular arithmetic etc. in order to comprehend the RSA algorithm. Fermat's Little Theorem serves as the foundation for the proof that RSA is accurate.

## 2 Keywords

RSA, cryptography, cryptosystem, encryption, decryption, algorithm.

## 3 Introduction

The study of secret messaging techniques is known as cryptography. The communication that has to be delivered is called out as plaintext, while the
message that is received in an altered form is known as ciphertext. A process known as encryption transformation is used to change plaintext into cipher- text. An encryption transformation, de ned mathematically, is a function that maps one letter of the alphabet to another letter of the alphabet, thus jumbled alphabetic letters. Additionally, we are aware that a function can only be inverted if it is 1-1. This indicates that enciphering transformations, which are the inverse function used to decrypt the message, must be 1-1 in order to yield both encryption and decryption transformations. A cryp- tosystem is made up of the components of our alphabet, the encoding and decoding transformations, and the elements themselves. Cryptanalysis is the study of breaking cryptosystems, based on Kercho 's principal one way to ensure the integrity of a cryptosystem is through cryptanalysis.

Introduction to number theory Prime Numbers play very important role in RSA algorithm. it is de nes as a prime number is an integer greater than 1 that is divisible by no positive integers other than 1 and itself. The Greatest Common Divisor(GCD): of two or more numbers is the great- est common factor number that divides them, exactly.

## 4 Public Key Cryptography

Public key cryptography involves a pair of keys known as a public key and a private key (a public key pair), which are associated with an entity that needs to authenticate its identity electronically or to sign or encrypt data. Each public key is published and the corresponding private key is kept secret. Data that is encrypted with the public key can be decrypted only with the corresponding private key.
RSA public key pairs can be any size. Typical sizes today are 1024 and 2048 bits.
RSA Public Key Cryptography Di e and Hellman rst introduced the
idea of the public-key cryptosystem in 1976. The idea of public-key cryp- tosystems has since been implemented by a variety of proposed public-key cryptosystems.Ronald Rivest, Adi Shamir, and Leonard

Adleman created the RSA public key cryptosystem, also referred to as the RSA cryptosystem, in 1977. This method uses Fermat's theorem as a basic result

Lemma(Fermat's little Theorem);
If p is the prime number,and (a,p)=1 then

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

The complexity of locating factors of a composite positive integer, that is, the product of two large primes, is the foundation for this system's security.

Key Generation Public key methods of the AES type need computing the pair (Kpublic, Kprivate). The fact that these keys are computed mathe- matically rather than being created at random is what sets RSA apart from other encryption techniques. In contrast to most symmetric key algorithms, where the key generation step is not very di cult in terms of mathematical computations, the RSA algorithm's key creation step is highly central and signi cant.

The key generation process of the RSA Public Key Cryptosystem:

1. Choose two large prime numbers (p and q)
2. Compute n =$p \cdot q$
3. Calculate $\phi$(n) = $(p-1)\cdot(q-1)$
4. Choose an integer e such that 1 < e < $\phi$(n), and:

(a) Ensure that gcd(e,$\phi$(n)) = 1
(b) Ensure that e and $\phi$(n) are coprime

5. Compute an integer d, such that d = $e^{-1}$ mod $\phi$(n)

After completing these ve steps, we have generated two asymmetric keys that can be used for encryption and decryption further in the process: the public key consists of n and e, while the private key consists of d.

$K_{Public} = (n, e)$ $K_{Private} = (d)$

To use large numbers in the generation process for p and q, often at least 512 bits, which makes the n 1024 bits $p \cdot q$.

Encryption and decryption

RSA encryption: A considers the $K_{Public} = (n, e)$ of B. The message m to be encrypted is taken modulo n.The Plaintext m is encrypted by A into the Ciphertext c as

$$c \equiv m^e \pmod{n}$$

RSA decryption: B considers the ciphertext c received from A. B decrypts c and obtains plaintext m by computing

$$m \equiv c^d \pmod{n}$$

The decryption is based on the following theorem:

Lemma[3] : Let n= pq, p and q are distinct primes and $1 \leq e \leq \phi(n)$ with (e, $\phi$(n)) = 1. If d is a multiplicative inverse of e modulo $\phi(n)$\$, *then*

$$m^{ed} \equiv m \pmod{n}$$

Through a simple example of the RSA algorithm with step-by-step encryption and decryption,
Suppose Consider Word "Welcome" and Apply RSA for Encryption and Decryption.
Let p=19 and q=37 Using RSA encode word "WELCOME" as key s=25 Key Generation:

1. Choose two large prime numbers (p and q) p=19
   q=37
2. Compute n =$p \cdot q$
   n=19 ·37=703
3. Calculate $\phi$(n) = $(p-1) \cdot (q-1)$
   $\phi$(n)=18 ·36=648
4. Choose an integer e for public key such that 1 < e < $\phi$(n), e and $\phi$(n) are coprime e=17
5. Compute an integer d as private key
   $(d \times e) = 1 \pmod{\phi(n)}$
   d=385
   So the public key (n=703,e=17) private key (n=703,d=385) Encryption:

1. Convert Message to Numeric(ASCII):
   W=119,E=101,L=108,C=99,O=111,M=109,E=101
   Encrypt values:

$$c_W \equiv 119^{17} \pmod{703}$$
$$c_E \equiv 101^{17} \pmod{703}$$
$$c_L \equiv 108^{17} \pmod{703}$$
$$c_C \equiv 99^{17} \pmod{703}$$
$$c_O \equiv 111^{17} \pmod{703}$$
$$c_M \equiv 109^{17} \pmod{703}$$

$c_E \equiv 101^{17} \pmod{703}$

Then resulting ciphertext values :

Decryption:
Decrypt each Ciphertext value:

$c_W = 320$
$c_E = 118$
$c_L = 563$
$c_C = 671$
$c_O = 255$
$c_M = 616$
$c_E = 118$

$M_W \equiv C^{385} \pmod{703}$ W
$M_E \equiv C^{385} \pmod{703}$ E
$M_L \equiv C^{385} \pmod{703}$ l
$M_C \equiv C^{385} \pmod{703}$

$M_O \equiv C^{385}$ (mod 703)
O

$M_M \equiv C^{385}$ (mod 703)
M

$M_E \equiv C^{385}$ (mod 703)
E

Then resulting decrypt values :

$$M_W = 119$$
$$M_E = 101$$
$$M_L = 108$$
$$M_C = 99$$
$$M_O = 111$$
$$M_M = 109$$
$$M_E = 101$$

2. Convert Numeric to Characters:
Then the Decrypted message is "WELCOME"

# 5 Summary

The best random number generators are being used to generate candi- dates for the necessary primes, and that the most recent version of the RSA technique is being used, is immune to assaults using the selected ciphertext, the di culty of factoring large integers plays a crucial role in RSA encryption security.

Over the years, the strength of integer factorization methods has in- creased, requiring RSA cryptography to rely on ever-longer encryption keys and ever-larger integer modulus values.

This makes RSA inappropriate for encryption/decryption of actual message content for high data-rate communication links.

RSA is ideal for the exchange of secret keys that can subsequently.

# References

1. A Method for Obtaining Digital Signatures and Public-Key Cryptosys- tems by R. L. Rivest, A. Shamir, and L. Adleman, Communications of the ACM, Vol. 21, No. 2, February 1978.

2. S. Singh, Arab Code Breakers, SimonSingh.net, 2012, accessed Febru- ary 14, 2013. http://simonsingh.net/media/articles/maths-and-science/arabcode- breakers.

3. N. A. Lal, A Review Of Encryption Algorithms-RSA And Di e-Hellman, Int. J. Sci. Technol. Res., vol. 06, no. 07, pp. 84 87, 2017.

4. Buchmann, J.A., Butin, D., G opfert, F., Petzoldt, A. (2016). Post- Quantum Cryptography: State of the Art. In: Ryan, P., Naccache, D., Quisquater, JJ. (eds) The New Codebreakers. Lecture Notes in Com- puter Science(), vol 9100. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978- 3-662-49301-46.

5. R. Kumar. A Survey on Post-Quantum Cryptography for Constrained Devices. International Journal of Applied Engineering Research. 14. 2608-2615. 2019.