Advanced Journal of Science, Technology and Engineering
ISSN: 2997-5972
Volume 5, Issue 2, 2025 (pp. 58-66)
www.abjournals.org

THE BASIC CRYPTOLOGY: A SIMPLE EXPLANATION OF HOW PRIME FACTORIZATION (MATHEMATICS) IS USED IN THE FIELD OF CRYPTOLOGY

Pijay Patili, Benson Mirou, Boaz Andrews, and Mohsen Aghaeiboorkheili.

School of Mathematics and Computer Science,
Papua New Guinea University of Technology, Lae, Papua New Guinea.

Cite this article:

Pijay Patili, Benson Mirou, Boaz Andrews, Mohsen Aghaeiboorkheili (2025), The Basic Cryptology: A Simple Explanation of How Prime Factorization (Mathematics) Is Used in the Field of Cryptology. Advanced Journal of Science, Technology and Engineering 5(2), 58-66. DOI: 10.52589/AJSTE-GJSHV0GH

Manuscript History

Received: 19 Jul 2025

Accepted: 29 Aug 2025

Published: 15 Sep 2025

ABSTRACT: *Mathematics has vast applications in today's technological world, which most people do not know much about, and this is a major concern. The purpose of this research is to investigate and point out the usage of Mathematics in the field of Cryptology. Mathematics has many real-world applications. By using online sources, this study delved deeply into the field of cryptology and pointed out the Mathematics used in this field. Similar investigations have been carried out by other students and scholars in other fields which are applicable to Mathematics. With the help of their papers and with ideas arising from the research, this paper is written. From the investigation, Prime Factorization is seen as the most important Mathematics that plays a major role in the field of cryptology. It influenced the way data is protected by providing necessary codes known as 'keys' in the form of numbers. This actually answers our questions regarding the applications of Mathematics in real life and in the field of cryptology.*

KEYWORDS: Cryptology, Private key**,** Public key, Encryption, Decryption, Rivest-Shamir-Adleman (RSA), Prime Factorisation theorem.

Article DOI: 10.52589/AJSTE-GJSHV0GH
DOI URL: https://doi.org/10.52589/AJSTE-GJSHV0GH

Advanced Journal of Science, Technology and Engineering
ISSN: 2997-5972
Volume 5, Issue 2, 2025 (pp. 58-66)

www.abjournals.org

INTRODUCTION

In this world of increasing technology and digital communication with advancements in new technologies which contribute towards the development of our world, the sending and receiving of data is at risk. Secure communications and data protection are an essential part of the digitalised world we are living in. Without proper protection of data, it is vulnerable to any cyberattacks, which means the general public can view or steal important information which is meant for a single institution or an individual. According to TechTarget, cryptology is defined as the mathematics, such as number theory and the applications of formulas and algorithms, that underpin cryptology and cryptoanalysis (Stallings, 2024; Diffie & Hellman, 1976). It further elaborates that cryptology is about constructing and analysing protocols that prevent third parties or the public from reading the private messages. This report aims to talk about the use of a mathematical concept called the Prime Factorisation Theorem (PFT) in the field of cryptology. It further explains the different types of keys that are used in the field of cryptology to encrypt and decrypt data and also dives into the usage of mathematical equations used in cryptology. It explains how PFT influences the keys used. PFT is simply a mathematical theorem dealing with numbers. 'Keys' refers to numbers. A pair of numbers that are generated with the help and influence of PFT. The keys are purposely used for protecting against unauthorised access to data and cyberattacks. There are two main types of keys used in cryptology. They are private and public keys. The private key is only accessible by the data recipient and the public key is accessible by anyone or the general public. Discussed below are the findings regarding the usage of Mathematics in the field of Cryptology.

METHODOLOGY

Research was conducted via the internet based on the topic Cryptology. Research was conducted and information about applications of the Prime Factorisation Theorem (PFT) in Cryptology were collected from online sources such as google, google chrome, Microsoft edge and other online platforms. Searches were made based on keywords such as Cryptology, Prime Factorisation Theorem, Encryption/Decryption and Rivest-Shamir-Adleman theorem. Information was only abstracted from the latest sources that were published this year. Information was paraphrased and additions and subtractions of information took place. All information is written using the Microsoft Word software. This research is only carried out using online sources. No books or newspapers were read to collect information and also no interviews were made to collect information regarding the research topic. The information regarding the cryptology was all over the place but only those that are necessary were collected. All information collected from the internet is referenced using APA referencing style.

Article DOI: 10.52589/AJSTE-GJSHV0GH
DOI URL: https://doi.org/10.52589/AJSTE-GJSHV0GH

Advanced Journal of Science, Technology and Engineering
ISSN: 2997-5972
Volume 5, Issue 2, 2025 (pp. 58-66)
www.abjournals.org

RESULTS

Discussed below are the results obtained from the research.

Prime Factorization Theorem (PFT)

A Prime Factorization Theorem is a procedure in which larger numbers are broken down to their simplified form (Koblitz, 2024). It is written in the form of **prime factors**. **Prime Numbers** are numbers that are divisible by 1 and itself. They cannot be divided by other numbers. It can be divided by other numbers but it will result in a decimal answer, which is against its general definition. According to its general definition, Prime numbers are natural numbers that are always greater than one (1>).

Prime Factorization Theorem plays a crucial role in **the Rivest-Shamir-Adleman algorithm** (1978). It is concerned with finding the prime factors of large composite numbers. If P1 and P2 are two large prime numbers. Computing power increases as more powers are put in. Multiply **P1**

and **P2** gives n.

Formula: P1×P2 = n where

P1, P2 = private key

n = public key

The difficulty arises in, given n trying to find the original P1 and P2

Figure 1: Prime Factorisation Theorem

When given P1 and P2 it is easy to compute n, but it is difficult to find P1 and P2 when n is given. The factorisation at this stage does not work. That is where the property of protecting secret files and messages is applicable. This idea is used in real life, where it makes it difficult for hackers to hack into companies' databases and other important sites.

What are private keys and public keys?

P1 and **P2** represent the **private key.** A private key is a secret key used in cryptology. It's a pseudo-generated sequence of bits that are made up of a mixture of numbers and the alphabet. Its main function is to decrypt encrypted files or messages. n represents **a public key.** Public

Article DOI: 10.52589/AJSTE-GJSHV0GH
DOI URL: https://doi.org/10.52589/AJSTE-GJSHV0GH

Advanced Journal of Science, Technology and Engineering
ISSN: 2997-5972
Volume 5, Issue 2, 2025 (pp. 58-66)
www.abjournals.org

key is the key that is used for encrypting a file or secret messages. It is the opposite of a private key (Schneier, 2023).

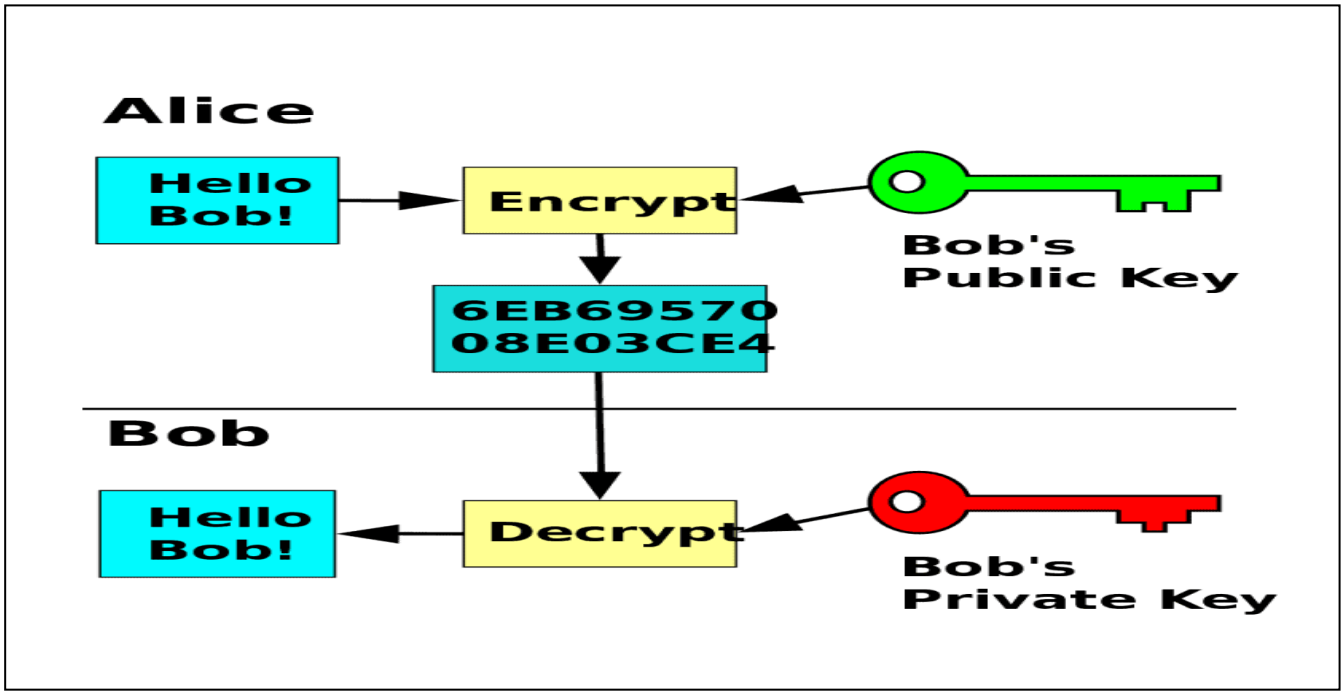

Figure 2: How private and private key works

What is the Rivest-Shamir-Adleman Algorithm (RSA)?

The RSA got its name from the people who came up with this algorithm. They are Ron Rivest, Adi Shamir, and Leonard Adleman. It is an algorithm that is widely used today because of its reliability and effectiveness. RSA deals with both the public and private keys. The keys are purposely for encrypting and decrypting, respectively. Private keys are restricted from unauthorised individuals. They are only kept by trusted agents, whereas public keys are accessible by the public or anyone.

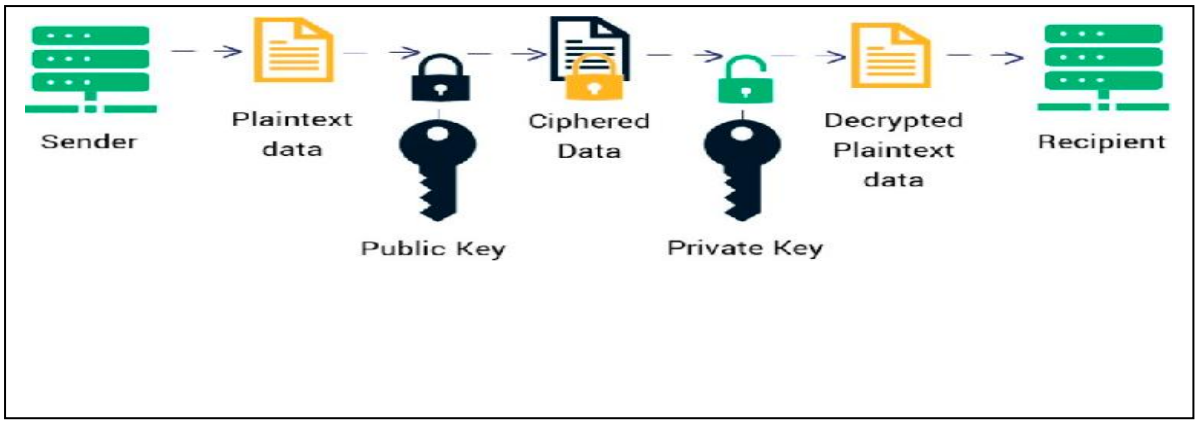

Figure 3: RSA Algorithm

Article DOI: 10.52589/AJSTE-GJSHV0GH
DOI URL: https://doi.org/10.52589/AJSTE-GJSHV0GH

Advanced Journal of Science, Technology and Engineering
ISSN: 2997-5972
Volume 5, Issue 2, 2025 (pp. 58-66)
www.abjournals.org

The RSA process in cryptology

(i) The key processing

It is the main process where most of the data encryption and decryption takes place. Where the prime factorisation theorem is most applicable and is used in the field of cryptology (Hoffstein, Pipher & Silverman, 2019). Discussed below is the process:

First of all, any two random prime numbers are selected. Let's say P1 and P2 and the two prime numbers must be different. After that private key and public key are calculated.

Private key: (n, d) Public key: (n, e)

Where n = RSA module, e= encryption exponent, d= decryption exponent

To find the two keys, the value of n is calculated first. With the help of the formula in *Figure 1* (prime factorisation), the value of n is calculated.

$P1 \times P2 = n$ where P1 and P2 are two randomly selected primes

The values of **d** and **e** in **the private key (n, d)** and **public key (n, e)** are calculated using the Euler phi function φ. It calculates how many numbers are less than (<) or equal (=) to n that are coprime to n. Coprime refers to numbers that have 1 as their divisor.

$$\Phi(n) = (P1-1)\,(P2-1)$$

The **phi function Φ** is calculated using the above formula with the help of two randomly selected prime numbers (P1 and P2). Then coprime to Φ(n) is chosen. The chosen value is **e** in **the public key (n, e)** and it is strictly the coprime of Φ.

$$\gcd(e, (P1-1)\,(P2-1)) = 1$$

The number **d** in **the private key (n, d)** is simply the **multiplicative inverse** of e. Which means when computing the product **d.e** the answer is 1, and also if we compute mod Φ(n).

$(e.d) \bmod \Phi(n) = 1$

To find d, the formula can be simply rearranged:

$d \bmod \Phi(n) = 1/e$

$d = 1/(e \bmod \Phi(n))$ private key (n, d)

Article DOI: 10.52589/AJSTE-GJSHV0GH
DOI URL: https://doi.org/10.52589/AJSTE-GJSHV0GH

Advanced Journal of Science, Technology and Engineering
ISSN: 2997-5972
Volume 5, Issue 2, 2025 (pp. 58-66)
www.abjournals.org

After all the above calculations are done, it leads to the two keys. Private (n, d) and public key (n, e). These keys are used for encrypting and decrypting data in the field of cryptology.

(ii) The usage of private (n, d) and public keys (n, e).

In this section the usage of the two keys is discussed with the formulas they are used with. Keys are simply used for encryption and decryption.

Encryption (n, e)

Encryption is the process where normal texts which are in the form of numbers are converted to ciphertext. Ciphertexts are texts which are only readable by computers. The public key **(n, e)** is used for encoding texts. Formula used is:

Encoding: $M = m^e \bmod n$

Where M = Cyphertext, m= message, public key (n, e)

Encryption is the conversion of a message (m) to ciphertext (M) with the help of a public key (n, e).

Decryption (n, d)

Decryption is done with the help of a private key. It is the opposite of encryption. In decryption, cipher texts are converted to human-readable form. The formula below is used:

Decryption: $m = M^d \bmod n$

Where m = message, M = cyphertext private key **(n, d)**

The idea behind decryption is to convert ciphertext to a human-readable format. The small letter 'm' represents the message and M stands for ciphertext. With the help of the private key **(n, d),** the cipher text M is finally decoded to a human-readable format**.**

Article DOI: 10.52589/AJSTE-GJSHV0GH
DOI URL: https://doi.org/10.52589/AJSTE-GJSHV0GH

Advanced Journal of Science, Technology and Engineering
ISSN: 2997-5972
Volume 5, Issue 2, 2025 (pp. 58-66)
www.abjournals.org

iii) Example of RSA Algorithm

(i)Randomly selected prime numbers are: P1=3, P2=11

Calculate n= P1*P2 = 33

(ii)Calculate Φ(n): = (P1-1) (P2-1) = (3-1) (11-1)

Φ(n) = 20

(iii)For e = 7 because it cannot be divided by the two primes of 20 (2 and 5).

gcd (e, (P1-1) (P2-1)) = 1

gcd (7,20) = 1

(iv)Calculate value of d:

(e.d) mod Φ(n) = 1

(7d) mod 20 =1

d =3

Public key = (n, e) = (33,7) **Private key** = (n, d) = (33,3)

Figure 4: Public and private key production

Encrypt the message with the public key (33, 7):

Random value is chosen to represent the text sent. Let us say 17, where m= 17. It is the numerical representation of the text sent. So, with the public key values (n, e) = (33, 7), substitution is made into the encryption formula below to obtain the value of M, where M represents the ciphertext. The purpose of the encryption is to convert the text into the ciphertext M, which is already computed (M=8).

Cipher text M = m^e mod n

M = 2 ^7 mod 33

M = 128 mod 33

M = 8

Decrypt the message with the private key (33,3):

In this process (decryption), ciphertext (M=8) is converted to text (m=17). With the help of Private key (n, d) = (33,3) and the **ciphertext(M=8)**.

Decrypted Text m = M^d mod n

m = 8^3 mod 33

m = 512 mod 33

m = 17

Article DOI: 10.52589/AJSTE-GJSHV0GH
DOI URL: https://doi.org/10.52589/AJSTE-GJSHV0GH

First of all, the text was represented by m=17 in the encryption stage; it was encrypted to ciphertext, and then in the decryption process, ciphertext (M=8) is converted back to original text (m=17). This depicts how public and private keys are used in the field of cryptology. It shows how messages are sent without any alteration along the way. The messages sent are well protected and only the intended individual or institution with the right key can view the protected text or data (Menezes, van Oorschot, & Vanstone, 1996).

DISCUSSION

Mathematics plays a crucial role in the encryption and decryption process of data. After research on the use of Mathematics in cryptology, it shows that Mathematics is very important in cryptology. This research is also in contrast with a paper written by Prof. S.P. Waghmare and Prof. V. N. Agme titled *A Study of Mathematical Cryptology*. This research also talked about how private and public keys are generated and used in encryption and decryption processes (Kaye, Laflamme, & Mosca, 2024). Furthermore, it elaborated on how important math is in conversions of texts to ciphertext and then to texts for humans to read. Math creates a safer communication channel and allows information to flow safely without any hindrance. There is a variety of Mathematics used in the field of cryptology, but in this report, the prime factorisation theorem is discussed. This report focused mainly on the use of the prime factorisation theorem in cryptology. In future, to know more, researchers can further carry out similar research on other Mathematics also used in the field of cryptology.

CONCLUSION

The study concludes that the Prime Factorisation theorem (Mathematics) is very important in the field of cryptology. It plays a major role in the encryption and decryption process of data. All in all, it is the blueprint for safer communication and data transmission. Cryptology would not survive without Mathematics.

REFERENCES

Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, *22*(6), 644–654. https://doi.org/10.1109/TIT.1976.1055638

Hoffstein, J., Pipher, J., & Silverman, J. H. (2019). *An introduction to mathematical cryptography*. Springer.

Kaye, P., Laflamme, R., & Mosca, M. (2024). *An introduction to quantum computing*. Oxford University Press.

Koblitz, N. (2024). *A course in number theory and cryptography* (2nd ed.). Springer.

Menezes, A., van Oorschot, P., & Vanstone, S. (1996). *Handbook of applied cryptography*. CRC Press.

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, *21*(2), 120–126. https://doi.org/10.1145/359340.359342

Article DOI: 10.52589/AJSTE-GJSHV0GH
DOI URL: https://doi.org/10.52589/AJSTE-GJSHV0GH

Schneier, B. (2023). *Applied cryptography: Protocols, algorithms and source code in C* (20th anniversary ed.). Wiley.
Stallings, W. (2024). *Cryptography and network security: Principles and practice* (8th ed.). Pearson.

ACKNOWLEDGMENT

I just want to say a sincere thank you to my college and lecturers who have helped me during the research. First, I thank my subject coordinator Professor Hasan Gumral for his guidance throughout the project and I also appreciate my colleague, Jacob Kerekere and Jordan Duma who discussed and shared ideas with me. Special thanks to the School of Mathematics and Computer Science for providing a conducive learning environment. Thank you all for your support.

Article DOI: 10.52589/AJSTE-GJSHV0GH
DOI URL: https://doi.org/10.52589/AJSTE-GJSHV0GH