Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Fermat's Theorem Application to Cryptography

Venkatesh Akurathi[1,2], Dr. Swathi Yandamuri[3], Koganti Anupama[2]

[1]Research Scholar, Andhra University Trans – Disciplinary Research Hub (A.U. TDR – HUB), Vishakhapatnam, 530003, AP, India.
[2]Department of Mathematics, P.B Siddhartha College of Arts & Science, Vijayawada, 520010, AP, India.
[3]Associate Professor, Department of Mathematics, Welfare Institute of Science, Technology & Management, Pinagadi, Pendruthi, 531173, AP, India.
Email: venkatesh.akurathi@yahoo.co.in.

In this work, cryptography is examined as a means of delivering and storing data in a certain format such that only the intended recipients may read and use it. People have been fascinated for millennia by the possibility of sending messages in a method that is undetectable to enemies. We provide an information-encoding technique that makes use of Fermat's theorem to create a highly impenetrable code. The following theorem's consequence serves as the foundation for the idea. A few elements of public key cryptography applications in number theory. In order to show how encryption and decryption work, this project used an example message.

Keywords: Cryptography, Encryption, Plane text. Decryption, Fermat's theorem

1. Introduction

The study of methods for protecting confidential information is known as cryptography. The science of researching attacks against cryptographic techniques is known as cryptanalysis. Cryptanalysis looks for ways to reveal information that has been encrypted and kept hidden without the use of a key. Under the category of cryptology are both cryptanalysis and cryptography. Thus, the science of hidden communications is known as cryptology.

The science of encryption, or cryptography, is fundamental to many aspects of our daily life and is used in pay-TV, e-commerce, mobile phone conversations, sending private correspondence, conveying financial information, ATM card security, computer passwords, and many more areas. The ideas and techniques of converting an understandable message (plane text) into an unintelligible one (cipher text) and back again are the subject of the art and

science of cryptography.

It is true that information needs to be stored securely in this day and age of ubiquitous technological connectivity, viruses, hackers, electronic eavesdropping, and fraud. Thus, there was a greater need to ensure the confidentiality of information and communications, safeguard systems against network-based attacks, and prevent the disclosure of data and resources.

The study of encoding messages such that only the intended recipient can decipher them is called cryptography. Although it is also used to secure data in computer systems, several components of cryptography are in fact highly mathematical in nature. It has a tight connection to the fields of cryptanalysis and cryptology. Every day, billions of users use it to safeguard data that is in motion as well as at rest throughout the globe.

According to Dan and Shou (2015), strong encryption can be easily integrated into a variety of applications since cryptographic systems are an essential component of standard protocols, most notably the Transport Layer Security (TLS) protocol. However, the most common association of cryptography in today's computer-centric society is with converting plaintext—also known as ordinary text, sometimes called clear text—into encrypted text.

Among the world's top mathematicians and computer scientists, cryptography has become a battleground in recent years. See, for example, Hill (1929 and 1931) and the references therein. Many countries have imposed restrictions on cryptography, ranging from limiting the use and export of software to prohibiting the public dissemination of mathematical concepts that could be used to create cryptosystems, because they do not want certain entities operating within or outside their borders to have access to means of receiving and sending hidden information that could be a threat to national interests.

However, the internet has made it possible for strong software to proliferate as well as—more importantly—the fundamental cryptographic methods, meaning that many of the most sophisticated cryptosystems and concepts are now available to the general public. In the past, symmetric encryption has been the main emphasis of cryptology in order to offer confidentiality. Other factors like digital signatures, authentication, integrity, and public-key encryption have just recently been incorporated into the theory and practice of cryptography and cryptology, dating back a few decades.

Data can be transmitted and stored using cryptography in a specific format so that only the intended recipients can read and process it. The Greek term kryptos, which means hidden, is where the name cryptography originates. According to Biggs (2008), the Egyptian use of hieroglyphic writing dates the development of cryptography back to 2000 BC. These were made up of intricate pictograms, the meaning of which was only fully understood by a select group of people at the time. The art of Egyptian hieroglyphics includes methods for concealing information during storage or transmission, such as the use of microdots and word-image fusion.

According to Biggs (2008), Julius Caesar (100 BC–44 BC) was the first person to adopt a modern cipher because he did not trust his messengers when speaking with his governors and officers. He devised a mechanism whereby each character in his communications was substituted with a character three positions ahead of it in the Roman alphabet because of this.

2. Review of literature:

Michael O. Rabin (1990) conducted study on probabilistic algorithm for testing primality, they used fermat's Little Theorem to describe the primality of integers.Kevin Iga (2003) conducted to proof Fermat's Little Theorem by use of dynamical systems. Giedrius Alkauskas (2009) conducted study on classical proof of Fermat's Little Theorem by the use of properties of binomial coefficients. . Sergey Nikitin (2018) conducted a study on Eluer-Fermat algorithm and some of its applications. They used fermat's Little Theorem to prove the Euler-Carmichael function s (r,n).

Lakshmi et al. (2011) investigated the use of cryptography as a means of encrypting messages so that only the intended recipients could decipher them by taking off the disguise. The authors claim that because computers are now widely available, it is becoming more difficult to keep up with the rapid rise of wireless communications and secure information transmission. A primitive is the most fundamental module in modern cryptography. It can be thought of as a cryptographic building block that can be joined with other primitives to make a cryptographic protocol, and it can fulfill one or more desired functions.

Yakubu et al. (2018a) presented a technique for transferring and storing data in a specific format so that only the intended recipients may read and analyze it using rhotrices. In the current computer era, one of the greatest ways to transmit secret information is the new technique for transferring data that is extremely tough to change or break while moving or at rest.

A key component of cryptography is the use of rhotrix for message encoding and decoding, which are referred to as the encoding and decoding rhotrix, respectively. They stated that using rhotrices to apply polyalphabetic cipher systems has shown to be one of the safest and most effective ways to analyze protocols and stop the general public or other parties known as adversaries from reading or hearing the communication. They asserted that no amount of unit testing can find a security flaw in a polyalphabetic cipher system, especially when encrypting data to be sent out using Rhotrix.

During message encryption and decryption, binary and polynomial forms of the elements of finite fields were employed. They presented an extremely hard to change method in the study. The secret key $K1$, which is a non-singular matrix of $(n\text{-}1) \times (n\text{-}1)$ and n is a positive integer, is shared by the sender and the recipient.

3.Objectives of the Study

- To find out that which numbers have congruence relation modulo.
- To find out that how we can generate the public and private keys.
- To find out that cryptography using Fermat's theorem is proposed
- To demonstrate the phenomenon of mathematical algorithms in Public Key Cryptography
- To find out algorithms on Fermat's theorems

4. Preliminaries

Cryptographic algorithms are classified in a variety of ways. We will define words pertaining to cryptography and the mathematical formalism used in this work for its own sake. Thus, we define a few basic words related to public-key cryptography andmathematics; 4.1 The Study of Cryptology This phrase refers to the extensive field study of covertwriting. 4.2 Encryption This is the process of formulating and developing the mathematical formulas that encrypt and decrypt messages.

4.3 Cryptoanalysis This is the study of deciphering and studying encryption protocols. The goal of cryptanalysis is to crack the cryptosystem, or to discover the encryption or decryption key, or to at least devise a technique that will enable us to extract some data from encrypted messages. In this situation, it is typically believed that the cryptanalyzer is an adversarial party or an eavesdropper, and that while they are aware of the cryptosystem in use, they are unaware of the key. A cryptanalyzer might possess distinct data at their disposal: A chosen plaintext and its corresponding cryptotext (known plaintext), (CP) a chosen plaintext and its corresponding cryptotext (chosen plaintext), (KP) some, possibly random, plaintext and the associated cryptotext (known plaintext), and (CC) a chosencryptotext and the corresponding plaintext (chosen cryptotext). .

4.4 Security This is one particular application of cryptography where information is hidden by converting it into an unintelligible code. Today's daily existence involves the use of encryption. Transactions conducted over unreliable communication channels, like the Internet, typically require encryption. Data being sent between devices, including mobile phones and automated teller machines (ATMs), is likewise protected by encryption. 4.5 Cracking the Code Since it is the reverse of encryption, this is frequently categorized with them. The original data is obtained by decrypting the encrypted data.

5. Main Theorems

5.1Theorem [FERMAT'S THEOREM].

If p is a prime, then $a^{\,p} \equiv a(mod\ p)$for integers a. In fact, $a^{\,p-1} \equiv 1(mod\ p)$ for all integers a that are relatively prime to p.

5.2Theorem: Let p be an odd prime number and b a primitive root modulo p. a) then that $b^{(\frac{p-1}{2}} \equiv -1(\text{ mod p})$. Conclude that $-b \equiv b^{(\frac{p-1}{2}}$ (mod p

Solution. Note that $[\ b^{(\frac{p-1}{2}}]^2 = b^{p-1} \equiv 1(\text{ mod p})$.

Thus $b^{(\frac{p-1}{2}}$ is a solution of the congruence $x^2 \equiv 1(\text{ mod p})$. This congruence has only two solutions: 1 and −1. Thus $b^{(\frac{p-1}{2}} \equiv \pm 1(\text{ mod p})$. Since b is a primitive root modulo p, we can not have $b^{(\frac{p-1}{2}} \equiv 1(\text{ mod p})$. It follows that $b^{(\frac{p-1}{2}} \equiv -1(\text{ mod p})$. Multiplying both sides of this congruence by b, we get

$b^{(\frac{p-1}{2}} \equiv -b(\text{ mod p})$.

5.3 (Fermat's Theorem.)

Let p be prime. Then $x^{p-1} \equiv 1 \pmod{p}$ for all x satisfying gcd(x, p) = 1.

Proof List the first p−1 positive multiples of x: x, 2x, 3x, . . . ,(p−1)x. Suppose that rx and sx are the same modulo p, for $0 \leq r, s < p$.

Then we have $x(r-s) \equiv 0 \pmod{p}$. Since gcd(x, p) = 1, this can only happen

if r = s. Therefore, the p−1 multiples of x above are distinct and nonzero;

that is, they must be congruent to 1, 2, 3, . . . , p − 1 in some order. Multiply all these congruences together and we find:

$(p-1)!x^{p-1} = x \cdot 2x \cdot \ldots \cdot (p-1)x \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) = (p-1)! \pmod{p}$. Divide both side by (p − 1)! to complete the proof.

5.4Theorem: Let p, q be two distinct primes. Let n = p · q. Then $x^{(p-1)(q-1)} \equiv 1 \pmod{n}$ for all x satisfying gcd(x, n) = 1. Proof $x^{(p-1)(q-1)} \equiv (x^{p-1})^{q-1} \equiv (1)^{q-1} \equiv 1 \pmod{p}$, where $x^{p-1} \equiv 1 \pmod{p}$ from Fermat's Little Theorem. Similarly, it must be that $x^{(p-1)(q-1)} \equiv 1 \pmod{q}$. To complete the proof,

Note that the Chinese Remainder Theorem implies that the solution to the two equations is unique mod p · q. Since $x^{(p-1)(q-1)} \equiv 1 \pmod{p \cdot q}$ is one solution, the theorem follows.

5.5Theorem: Let p and q are distinct primes $a^{\emptyset(m)+1} \equiv a \pmod{p}$ and $a^{\emptyset(n)+1} \equiv a \pmod{q}$. then $a^{(\emptyset(m)+1)(\emptyset(n)+1)} \equiv a \pmod{pq}$ is valid , when n is prime .

Proof. If p is prime , then

$a^{\emptyset(m)+1} \equiv a \pmod{p}$

Therefore

$a^{(\emptyset(m)+1)^{\emptyset(n)+1}} \equiv a^{\emptyset(n)+1} \pmod{q}$

which implies

$a^{(\emptyset(m)+1)(\emptyset(n)+1)} \equiv a \pmod{q}$

Implies q divides $a^{(\emptyset(m)+1)(\emptyset(n)+1)} - a$

Similarly

$a^{(\emptyset(n)+1)^{\emptyset(m)+1}} \equiv a^{\emptyset(n)+1} \pmod{p}$

And

$a^{\emptyset(n)+1} \equiv a \pmod{q}$

$a^{(\emptyset(m)+1)(\emptyset(n)+1)} \equiv a \pmod{p}$

Thus p divides $a^{(\emptyset(m)+1)(\emptyset(n)+1)} - a$

Which conclude that pq divides $a^{(\emptyset(m)+1)(\emptyset(n)+1)} - a$

Hence $a^{(\emptyset(m)+1)(\emptyset(n)+1)} \equiv a \pmod{pq}$

5.6THEOREM: Let m be a positive integer and a any integer with (a,m) = 1. Then $a^{\phi(m)-1}$ is an inverse of a modulo m.

5.7THEOREM: Let m be a positive integer and a any integer with (a,m) = 1. Then the solution of the linear congruence $ax \equiv b \pmod{m}$ is given by $x \equiv a^{\phi(m)-1}\, b \pmod{m}$

II.DESCRIPTION OF THE METHOD

We select two different primes, p and q, which are both quite huge in practice. Subsequently, the transmittable words (as well as punctuation symbols) are matched with unique integers $x \geq 22$. If these primes are big enough and, in reality, less than each of these primes, then it can be assumed that the numbers x were selected in a relative prime to p and q. The plan is to compute an integer $\boldsymbol{U}$ from x using p and q, and then send $\boldsymbol{U}$ instead of x. It is obvious that $\boldsymbol{U}$ needs to be selected so that x (and hence the matching word) may be extracted from $\boldsymbol{U}$. The message sender performs the transition from x to $\boldsymbol{U}$ (also known as encoding), transmits the integer $\boldsymbol{U}$, and the recipient computes x from $\boldsymbol{U}$ (also known as decoding).

A. ALGORITHM

Step 1: Given the distinct primes $p$and q, the cryptographer denotes $n = pq$ and $m = (p-1)(q-1)$and chooses any integer $k \geq 2$ such that $\gcd(k\ m) = 1$.

Step 2: Only the numbers n and k are given, if the sender wants to transmit an integer x, he or she encodes it by reducing $x\ k\ modulo\ n$, say $x\ k \equiv r(mod\ n)$where $0 \leq r < n$.

Step 3: The sender transmit r to the receiver of the message who must use it to retrieve xx

Step 4: With r and K' known, the receiver can compute x (and hence the corresponding word in the message). Note: If the receiver knows the inverse K' of k in $\mathbb{Z}m$then $K'k = 1(mod\ m)$. Hence theorem 2 (with $e = K'k$) gives$x\ K'k \equiv x(mod\ n)$ and $x \equiv x\ K'k \equiv (x\ k\ )\ K' = r\ K'$ modulo n.

Example 1. Let $p = 13$ and $q = 15$ so that $n = 195$=195and $m = 168$. Then let $k = 5$, chosen so that $\gcd(k, m) = 1$. Encode the number $x = 7$ and then decode it. Solution

Let's perform these steps:

Since N = 195 and $\emptyset(N)168$

We can the extended algorithm for this

168 = 33 x 5 +3

5= 1x3+2

3=1x2+1

1=3-1x2 = 3-1 x (5-1x3) 2x 3 -1 x 5 = 2 x (168 -33 x 5) -1 x 5 = 2 x (168 – 33 x 5) -1 x5 = 2x 168 – 67 x5

So d= -67 , but we we want a positive value , so d= 168 -67 = 101

8.encoding : $c = 7^5 \mod 195 = 1682 \mod 195 = 167$

Decoding ;$x = 167^{101} \bmod 195 = 7$

So , the encoded number x =7 and the decoded number x= 7

2. RSA Algorithm

The working of RSA can be explained in 3 stages:

Phase 1 (Public and Private Keys Generation)

- ❖ Begin by selecting two prime numbers p and q (of the order of a few hundred bits).
- ❖ Compute their product n which is the modulus for encryption and decrption.
- ❖ Next, we need the quantity, $\Phi(n)$ referred to as Euler totient of n. Compute the Euler totient function $\Phi(n) = (p - 1)(q - 1)$.
- ❖ Choose a large random number D($D > 1$ such that $(D; \Phi(n)) = 1$ (i.e, D and $\Phi(n)$ are relatively prime).

Phase 2 (Encryption)

Choose an integer E with $1 < E < \Phi(n)$ such that $(E; \Phi(n)) = 1$. (i.e E and $\Phi(n)$ are relatively prime).

Phase 2 (Decryption) Find the integer D with $1 < D < \Phi(n)$ such that $D * E = 1(\text{mod} n)$

RSA Set-Up

To begin, we must associate each letter of the alphabet with a unique number. This will allow us to convert our message into series of numbers which we can perform operations on. Let us use the following for this,

CODE			
letter	Numbers	letter	Number
A	00	N	13
B	01	O	14
C	02	P	15
D	03	Q	16
E	04	R	17
F	05	S	18
G	06	T	19
H	07	U	20
I	08	V	21
J	09	W	22
K	10	X	23
L	11	Y	24
M	12	Z	25

It's evident that we equated A to 00 rather than allowing it to equal 0. This is because we began utilizing double digits when we reached K. Reverting to our initial message would be impossible if we had a combination of single and double numbers. It's also helpful to use a number to indicate the spacing between words. In order to make things clearer, we shall utilize a "dash" rather of a gap between words.

6. CONCLUSION

Euler generalized Fermat's Little Theorem, which is a fundamental theorem in elementary number theory that makes power calculations of integers modulo prime numbers easier to compute.

2. This theorem, which is an extension of Euler's theorem, is helpful in applications of elementary number theory, such as primality checks and labor-saving devices in certain computations.It is suggested to use Fermat's theorem in cryptography. Keep in mind that the sender really just needs to know n and k.

3. Should someone intercept the transmission, they are unable to obtain x without K', since computing it necessitates $p\ and\ q$. Factoring $n = pq$ is in reality time-consuming if the primes $p\ and\ q$ are large, even if the third party is able to extract the integers $n\ and\ k$ from the sender

Hence the transformation is even more secured as it is very difficult to determine the various powers of r. Hence the code is extremely difficult to break.

7. Recommendation

- ❖ We can find the units digit of 5^{100} by the use of Fermat's theorem.
- ❖ with Fermat's Little Theorem we can confirm that some integers are absolute pseudoprimes.
- ❖ For any integer a , we can verify that a^7 and have the same units digit.
- ❖ When the base of the exponentiation is allowed to be a non-integer, such bases we call Fermat factors.
- ❖ To find out that irrational factors Satisfying the Fermat's Little Theorem.
- ❖ To find out whether we can calculate labor-saving device in certain calculations with Fermat's LittleTheorem.
- ❖ To find out whether we can test the primality of a given integer number.

References

[1.] Stallings, W (2005) Cryptography and network security, 4th edition prentice Hall.
[2.] Dan, B. and Victor, S. (2015), A Graduate Course in Applied Cryptography, 7- 23.
[3.] Hill, L.S. (1929), Cryptography in an algebraic alphabet, The American Mathematical Monthly, 36 (6) 306 – 312.
[4.] Hill, L. S. (1931), Concerning certain linear transformation apparatus of cryptography, The Amer. Math. Monthly,38 (3) 135 – 154.
[5.] Biggs, N. (2008), An introduction to information communication and cryptography. Springer page 171.
[6.] Lakshmi, G. N.,Kumar, B. R.,Suneetha, C. and Sekhar, A. C. (2011), A cryptographic scheme
[7.] of finite fields using logical operators, Intern. J. Comput. Applic. 31 (4) 1 – 4. [8.] Yakubu, D. G., Mathias, L. B., Lucy, B. G. and LohcwatDomven. (2018) Extension of Affine Hill cipher using rhotrices in the polyalphabetic cipher systems,Abacus J. Math. Asso. Niger. 45(1) 273-284.

[9.] Sharma, P.L. and Rehan, M. (2013),On security of Hill cipher using finite fields, Inter. J.
[10.] Compu. Applic. 71(4) 30 – 33.
[11.] Introduction to Abstract Algebra, fourth edition by W. Keith Nicholson, University of Calgary, Alberta Canada.