ISSN No:-2456-2165

An Application to Cryptography using Fermat's Theorem

[1]Domven Lohcwat., [1]Kanee, Goodfaith L., [1]Agwunobi., C.J. [1]Okai, J.O., [1]Isah Abdullahi., [1]Olope, G. I., [2]Musa, G. K,.
[1]Department of Mathematical sciences, AbubakarTafawaBalewa University Bauchi, Nigeria
[2]Department of Mathematics and Statistics, Federal polytechnic Nasarawa, Nigeria

Abstract:- Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process the data.The ability to transmit messages in a way that cannot be recognized by adversaries has intrigued people for centuries. In this paper, we outline a method that uses Fermat's theorem to encode information in a way that is very difficult to break. The idea is based on the following consequence of that theorem.

Keywords:- *Cryptography, Encryption, Plane text.*

I. INTRODUCTION

Cryptography, the science of encryption, plays a central role in mobile phone communications, pay-tv, e-commerce, sending private mails, transmitting financial information, security of ATM cards, computer password, etc. and touches on many aspect of our daily lives. Cryptography is the art and science encompassing the principles and methods of transforming an intelligible message (plane text) into one that is unintelligible (cipher text) and then retransforming that message back to its original form.

In this age of universal electronic connectivity of viruses and hackers of electronic eavesdropping and electronic fraud, there is indeed a need to store the information securely. This, in turn, led to a heightened awareness to protect data and resources from disclosure, to guarantee the authenticity of data and messages, and to protect systems from network-based attack, Stallings (2005).

Cryptography is the science of transforming communications so that only the intended recipient can understand them. Certain aspects of cryptography are indeed quite mathematical in nature, though it is also used to protect information in computing systems. It is closely related to the disciplines of cryptology and cryptanalysis. It is used everywhere and by billions of people worldwide on a daily basis, to protect data at rest and data in motion.

Cryptographic systems are integral part of standard protocols, most notably the Transport Layer Security (TLS) protocol, making it relatively easy to incorporate strong encryption into a wide range of applications, Dan and Shou (2015). However, in today's computer-centric world, cryptography is most often associated with scrambling plaintext(ordinary text, sometimes referred to as clear text) into cipher text.

In recent times, cryptography has turned into a battleground of some of the world's best mathematicians and computer scientists, for example, Hill (1929 and 1931) and the references therein. Because governments do not wish certain entities in and out of their countries to have access to ways to receive and send hidden information that may be a threat to national interests, cryptography has been subject to various restrictions in many countries, ranging from limitations of the usage and export of software to the public dissemination of mathematical concepts that could be used to develop cryptosystems.

However, the internet has allowed the spread of powerful programs and, more importantly, the underlying techniques of cryptography, so that many of the most advanced cryptosystems and ideas are now in the public domain.

Historically, the focus of cryptology has been on the use of symmetric encryption to provide confidentiality. It is only in the last several decades that other considerations, such as authentication, integrity, digital signatures, and the use of public-key encryption, have been included in the theory and practice of cryptography or cryptology.

Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process the data. The word cryptography is derived from the Greek *kryptos*, meaning hidden. The origin of cryptographic system is dated back to 2000 BC, (see Biggs (2008)) with the Egyptian practice of hieroglyphics. These consisted of complex pictograms, the full meaning of which was only known to an elite who were very few by then. Egyptian practice of hieroglyphics, includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit.

The first known use of a modern cipher was by Julius Caesar (100 BC to 44 BC), Biggs (2008), who did not trust his messengers when communicating with his governors and officers. For this reason, he created a system in which each character in his messages was replaced by a character three positions ahead of it in the Roman alphabet.

Lakshmi, et al. (2011) studied cryptography as a methods of sending messages in disguised form so that only the intended recipients can remove the disguise and read the massage. According to the authors with widespread availability of computer technology, the rapid growth of wireless communications secured exchange of information has become a challenging task. The most basic of the modules in modern cryptography is that of a primitive, which may be regarded as a cryptographic building block which performs one or more desired functions, and may be combined with others to form a cryptographic protocol. They went on saying that the most well-known and perhaps the simplest primitive of encryption, which allows parties to achieve confidential data transmission over an insecure channel is by encrypting information. In the same paper they proposed a cryptographic technique using elements of a finite field and logical operators basing on the inverse property.

Yakubu, et al. (2018a) introduced a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process the data using rhotrices. The new method of sending secret messages which is very difficult to alter or break either in motion or at rest was proved to be one of the best methods of sending secret information in the present computer age.

The use of rhotrix to encode and decode messages which were respectively called the encoding rhotrix and decoding rhotrix plays very important role in cryptography. They claimed that the applications of rhotrices to polyalphabetic cipher systems proved to be one of the most secured and constructive method of analyzing protocols, prevent public or third parties called adversaries from reading or hearing the message. They claimed that no amount of unit testing can uncover a security vulnerability in polyalphabetic cipher system, particularly when using rhotrix in encrypting the information to be sent out.

Sharma and Rehan (2013), modified the Hill cipher cryptography which is a symmetric key substitution algorithm, and is vulnerable to known plaintext attack. The presented paper provides two fold securities to the existing Hill cipher by using the elements of finite fields and logical operators. Two different keys were used in the proposed algorithm. The first key is taken as a non-singular matrix and the second key is obtained with the help of elements of finite fields.

The elements of finite fields were used in binary and polynomial form during encryption and decryption of the message. In the paper, they provided an algorithm that is very difficult to alter. The sender and receiver shares the secret key K_1, where K_1 is (n-1) × (n-1) non-singular matrix and n is a positive integer. The sender then converts the plaintext into pre-assigned numerical values and calculates $S_1 = K_1 P mod$ ($2n$-1); S_1 is the first cipher text, P is the plain text. Then the sender converts S_1 into binary string of n-bits which gives the matrix M in their paper and choose a random matrix A of order (n-1) × (n-1). The sender performs $XNOR$ operations with randomly selected rows/columns of A with each row of matrix M and gets a matrix $MXNOR$. According to the authors the sender converts the entries of $MXNOR$ into the elements of $GF(2^n)$ and multiply each entry with g^n and calculates K_2, whose entries is 1 if g has the power greater than (2^n-1) otherwise 0 and shares it with the receiver of the message. The receiver then reduces the powers of the entries to mod (2^n−1) and gets the matrix M_4. After writing it into binary form, the receiver converts the same in numerical values and then into text to get the final cipher text S_2. This method of enciphering and deciphering is very complicated and difficult to alter or break.

- **Theorem 1.[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.
  Proof: We need to show that $a^{-p} \equiv \bar{a}$ in $\mathbb{Z}_p$, because this equation is true if $\bar{a} = \bar{0}$, it suffices to showthat $\bar{a}^{p-1} \equiv \bar{1}$ in $\mathbb{Z}_p$ whenever $\bar{a} \neq \bar{0}$. But if $\bar{a} \neq \bar{0}$, then $\bar{a}$ has an inverse in $\mathbb{Z}_p$, say $\bar{b}\bar{a} = \bar{1}$. Now multiply all the nonzero elements in $\mathbb{Z}_p$ by $\bar{a}$ to obtain:
  $\bar{a}\bar{1}, \bar{a}\bar{2}, \ . \ . \ . \ , \bar{a}(\overline{p-1})$. These are all distinct (because $\bar{a}\bar{r} = \bar{a}\bar{s}$ yields $\bar{r} = \bar{s}$ after multiplicationby $\bar{b}$) and none equals $\bar{0}$, so they must be the set of all nonzero elements $\bar{1}, \bar{2}, \ . \ . \ . \ , \overline{p-1}$ in some order. In particular, the products are the same, and we obtain:
  $\bar{a}^{p-1}(\bar{1}, \bar{2}, \ . \ . \ . \ , \overline{p-1}) = \bar{1}, \bar{2}, \ . \ . \ . \ , \overline{p-1}$. But the element $\bar{1}, \bar{2}, \ . \ . \ . \ , \overline{p-1}$ is invertible in $\mathbb{Z}_p$. Hence multiplication by its inverse gives$\bar{a}^{p-1} \equiv \bar{1}$, which is what we wanted.
  Note that Fermat's theorem fails if p is not prime.
- **Theorem 2.**Let $n = pq$=pqere p and q are distinct primes, write $m = (p-1)(q-1)$, and let $e > 2$ be any integer such that $e \equiv 1 (mod\, m)$1(mod m)$x^e \equiv x (mod\, n)$ for all x such that $\gcd(x, n) = 1$.
  Proof. Because $e \equiv 1 (mod\, m)$(mod m)write$e - 1 = ym$, where y is an integer. Then $x^e = x.(x^m)^y$, so it suffices to show that$x^m \equiv 1 (mod\, n)$ whenever $\gcd(x, n) = 1$. This condition certainly implies that p does not divide x. Hence Fermat's theorem shows that $x^{p-1} \equiv 1 (mod\, p)$ and so
  $x^m = (x^{p-1})^{q-1} \equiv 1^{q-1} \equiv 1 (mod\, p)$. Similarly, $x^m \equiv 1 (mod\, q)$ and so, as p and q are relatively prime, that is; $x^m \equiv 1 (mod\, pq)$.

II. DESCRIPTION OF THE METHOD

Two distinct prime p and q are chosen, each very large in practice. Then the words available for transmission (and punctuation symbols) are paired with distinct integers $x \geq 22$ The integers x used may be assumed to be chosen relatively prime to p and q, if these primes are large enough and, in practice, to be smaller than each of these primes. The idea is to use p and$q$ to compute an integer r from x and then to transmit r rather than x. Clearly, r must be chosen in such a way that x (and hence the corresponding word) can be retrieved from r. The passage from x to r (called encoding) is carried out by sender of a message, the integer r is transmitted, and the computation of x from r (decoding) is done by the receiver.

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 $p = 11$ and $q = 13$ so that $n =$ 143=143and $m = 120$. Then let $k = 7$, chosen so that $\gcd(k, m) = 1$. Encode the number $x = 9$ and then decode it.

Solution

The sender reduces $x^k = 9^7$ (mod$n$).

Thus;143: $9^2 \equiv 81$, $9^3 \equiv 14$, $9^4 \equiv 126, 9^5 \equiv 133, 9^6 \equiv 53, 9^7 \equiv 48$. Hence $r = 48$ will be transmitted. The receiver thenfinds $K^{'}$; the inverse of $k = 7\ (mod\ m)$. In fact by Euclidean algorithm one will get: $1 = 120 - 17(7)$, so $K^{'} \equiv -17 \equiv 103(mod\ 120)$ is the required inverse. Hence, $x$is retrieved (mod n) by: $x = r^{K^{'}} \equiv 48^{103}(mod\ 143)$.

Note that 103≡ 1100111100111nary, and so $103 = 1 + 2 + 2^2 + 2^5 + 2^6$. Then the receiver compute 48^t, where t is a power of 2 by successive squaring of 48 modulo 143. That is;

$48^2 \equiv 16, 48^{2^2} \equiv 113, 48^{2^3} \equiv 42, 48^{2^4} \equiv 48, 48^{2^5} \equiv 16, 48^{2^6} \equiv 113$. Again working modulo 143 gives: $x \equiv 48^{103} \equiv 48^{1+2+2^2+2^5+2^6} = 48\,.\,16\,.\,113\,.\,16\,.113 \equiv 9$; which retrieves the original 9.

Example 2. Let $p = 41$ and $q = 43$ so that $n = 1763763$ and $m = 1680$=1680n let $k = 23$, chosen so that $\gcd(k, m) = 1$. Encode the number $x = 11$ and then decode it.

Solution

The sender reduces $x^k = 11^{23}$ (mod n).

Thus; 1763: $11^2 \equiv 121$, $11^3 \equiv 1331$,$11^4 \equiv 537, 11^5 \equiv 618, 11^6 \equiv 1509, 11^7 \equiv 732$, $11^8 \equiv 1000$, $11^9 \equiv 422$, $11^{10} \equiv 1116$, $11^{11} \equiv 1698$, $11^{12} \equiv 1048$, $11^{13} \equiv 950$, $11^{14} \equiv 1635$, $11^{15} \equiv 355$, $11^{16} \equiv 379$, $11^{17} \equiv 643$, $11^{18} \equiv 21$, $11^{19} \equiv 231$, $11^{20} \equiv 778$, $11^{21} \equiv 1506$, $11^{22} \equiv 699$, $11^{23} \equiv 637$ Hence $r = 637$ will be transmitted. The receiver then finds $K^{'}$; the inverse of $k = 23\ (mod\ m)$. In fact by Euclidean algorithm one will get: $1 = 1680 - 73(23)$1680-73(23)$K^{'} \equiv -73 \equiv 1607(mod\ 1763)$ is the required inverse. Hence, $x$is retrieved (mod n) by: $x = r^{K^{'}} \equiv 637^{1607}(mod\ 1763)$.

Note that 1607≡ 11001000111000111nary, and so $1607 = 1 + 2 + 2^2 + 2^6 + 2^9 + 2^{10}$. Then the receiver compute637^t, where t is a power of 2 by successive squaring of 637 modulo 1763. That is;

$637^1 \equiv 637, 637^2 \equiv 279\ ,637^{2^2} \equiv 269, 637^{2^6} \equiv 551, 637^{2^9} \equiv 379, 637^{2^{10}} \equiv 838$,Again working modulo 1763gives:$x \equiv 637^{1607} \equiv 637^{1+2+2^2+2^6+\ 2^9+2^{10}} = 637\,.\,279\,.\,269\,.\,551\,.379\,.838 \equiv 11$; which retrieves the original 11.

III. CONCLUSION

In this paper, an application of cryptography using Fermat's theorem is proposed. Note that all the sender really has to know are $n\ and\ k$. A third party intercepting the message $r$cannot retrieve $x$without $K^{'}$, and computing it requires $p\ and\ q$. Even if the third party can extract the integers $n\ and\ k$ from the sender, factoring $n = pq$ in practice is time consuming if the primes $p\ and\ q$ are large. 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.

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.