International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8, Issue-1, May 2019

Information Security through Dual Transformation Techniques for the Unsecured Network

K.R.Sekar, K.Saichandan Reddy, P.Srivardhan Reddy, G.Sathiamoorthy, R.Vyshnavi sphoorthi

Abstract*: *Background: For the past two decades, cryptography techniques and methodologies play an inevitable role in the unsecured network. Intrusions and sniffing can be prevented through the above-said cryptography. In the 20th century, the inventions of the electromagnetic and complex machines are done remarkable jobs in the field of cryptography. The famous Enigma rotor machine is used to encrypt the text and the same is difficult to break. Literally speaking cryptography is the branch of number theory needs more integral solutions. Asymmetry algorithm is mainly used in prime theory. The classical cryptography and the ciphers are to protect the secrets. Objective: The objective of the research work is to maintain security to the messages and also to keep the integrity of the message. In the research arena, umpteen numbers of methods and technologies flood all the way in the cryptography technology. Method:The proposed methodology in this work is towards mathematical ideology like Laplace and Fourier transforms. By the way of above said two methodologies forward and reverse methods adopted both in Laplace and Fourier. Results: The outcome of the work shows the greater accuracy and difficult to tap the message in the unsecured network by the intruders. Mathematical implementations adopted throughout the research paper to emphasize the research outcome of the article.

Index Terms*: *Cryptography, Fourier, Inverse Fourier, Intrusions and Sniffing, Inverse Laplace, Laplace.

I. INTRODUCTION

The inter network communication across nodes in a network is an inevitable one in the fast growing world. Today, inter-network communication resolves the security related problems to a great extent. In an unsecured network, any communication can be tapped by the intruders at any point of time. Security and reliability are the chief issues affecting this scenario. The above said factors, play a vital role for secure transactions in unsecured networks. The cryptography is the good old technique still playing it's role in an unsecured network with different fragrance. Any computer will be easily attacked within a small timeframe using cryptanalysis. F-FCSR-Stream cipher is used for cryptanalysis using Mbytes of data. It allows the attack to be performed on a single pc within seconds [1]. Encryptions using mathematical transformations are to be applied for secure message transmission in a secured channel [2]. In the research work of the article, two mathematical ideologies were deployed for cryptography techniques. The first one is Laplace and the other is Fourier transforms. The methodologies bring out the encryption and decryption through forward and inverse forms. According to the empirical study of the methods, Fourier transformation is faster than other techniques. Encryption and decryption using LAPLACE transformation is applicable for Pay-TV, e-commerce, sending private emails, transmitting financial information ,security of ATM cards, computer passwords [3]. This can be used in a large-universe ABE scheme, any string can be used as an attribute of the system, and these attributes are not necessarily enumerated during setup [4]. The mathematical evaluation of the technique proposed, was performed and the results were verified. The analytical expressions were narrated with a clear example in this paper . The algorithms are incorporated for the easy understanding purpose for the upcoming researchers in the same line of art. Step by step procedures are explained through mathematical derivation. The algorithms, mathematical proof and numerical evaluation are the key factors of the research article. Abstract Functional Encryption (FE) is an exciting new paradigm that extends the notion of public key encryption. Using this, we explore the security of Inner Product Functional Encryption schemes with the goal of achieving the highest security against practically feasible attacks [5]. In multi-authority attribute-based encryption (ABE) systems, each authority manages a different attribute universe and issues the private keys to users [6]. In a functional encryption (FE) scheme, the owner of the secret key can generate restricted decryption keys that allow users to learn specific functions of the encrypted messages and nothing else [7].

II. LITERATURE SURVEY

Multivariate Public Key Cryptosystems (MPKC) are a candidate of post-quantum cryptography. The MPKC signature scheme Rainbow is endowed of efficient signature generation and verification [8]. A Cloud computing is emerging paradigm provides various IT related services. The security and privacy are two major factors that inhibits the growth of cloud computing [9].

Revised Manuscript Received on 30 May 2019.
* Correspondence Author
K.R.Seka*r, School of Computing, SASTRA Deemed University, India
K.Saichandan Reddy, School of Computing, SASTRA Deemed University, India
P.Srivardhan Reddy, School of Computing, SASTRA Deemed University, India
G. Sathiamoorthy, SASH, SASTRA Deemed University, India
R.Vyshnavi sphoorthi, School of Computing, SASTRA Deemed University, India

As a signaling protocol for controlling communication on the internet, establishing, maintaining, and terminating the sessions, the Session Initiation Protocol (SIP) is widely used in the world of multimedia communication [10]. In this paper, we study the Learning With Errors problem and its binary variant, where secrets and errors are binary or taken in a small interval.

We introduce a new variant of the Blum, Kalai and Wasserman algorithm, relying on a quantization step that generalizes and fine-tunes modulus switching [11]. With the development of cloud computing, electronic health record (EHR) system has appeared in the form of patient centric, in which patients store their personal health records (PHRs) at a remote cloud server and selectively share them with physicians for convenient medical care [12]. We initiate a systematic treatment of the communication complexity of conditional disclosure of secrets (CDS), where two parties want to disclose a secret to a third party if and only if their respective inputs satisfy some predicate [13]. Attribute-Based Encryption (ABE) is a powerful cryptographic tool that allows fine-grained access control over data. Due to its features, ABE has been adopted in several applications, such as encrypted storage or access control systems [14].

III. APPLIED METHODOLOGY

A. Encryption Algorithm

1. Let **$f_n(x)$ =** plain text divided into words .

$l(F_n(x))$ = Total length of key divided into words at certain intervals.

$l(g(x))$ = Length of original key.

Then $l(F_n(x)) = (l(f_n(x)) / l(g(x))) + (l(f_n(x)) \% l(g(x)))$

$= F_1(x) + F_2(x) + F_3(x) + \ldots\ldots\ldots\ldots + F_n(x).$

2. Now consider $F_n(x)$

Intermediate Cipher text

$G_n(x) = [\, F_n(x) + f_n(x) \,] \bmod 25$

Where $n = 0, 1, 2, 3, \ldots, n$

3. Consider $G_n(x)$

Let $P_1(x)$ be the polynomial with coefficients of $G_1(x)$ of consecutive powers from $X^{n-1}, X^{n-2}, \ldots, 1$.

4. The Cipher text is

$C.T = L(p(x)) = L(p_1(x)) + L(p_2(x)) + \ldots\ldots\ldots + L(p_n(x))$ ----------(1)

(Or)

5. $F(p(x)) = F(p_1(x)) + F(p_2(x)) + \ldots\ldots\ldots + F(p_n(x))$ ---------- (2)

[as $p(x) = p_1(x) + p_2(x) + \ldots\ldots\ldots + p_n(x)$]

We can apply either Fourier Transforms or Laplace Transforms.

B. DECRYPTION ALGORITHM

Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand. This term could be used to describe a method of un-encrypting the data manually or with un-encrypting the data using the proper codes or keys. Decryption is the process of transforming encrypted information so that it is intelligible again. A cryptographic algorithm, also called a cipher, is a mathematical function used for encryption or decryption.

1. $L^{-1}(C.T) = p(x)$

$= p_1(x) + p_2(x) + \ldots\ldots\ldots + p_n(x)$

2. Extract the coefficients from $p_1(x), p_2(x), \ldots\ldots\ldots, p_n(x)$.

3. Group the obtained coefficients

The n we will get $G_n(x) = G_1(x) + G_2(x) + \ldots + G_n(x)$

4. $f_n(x) = [\, G_n(x) - f_n(x) \,] \bmod 25$

5. Where $n = 0, 1, 2, 3, \ldots, n$

6. From the above process we will get required plain text .

7. $F_n(x)$ = Plain Text .

8.

9. C.

10. Similar process for Fourier Transformation is

$\gamma(n)$ be the Gamma function

$$\gamma(n) = \int_{-\infty}^{\infty} x^{n-1} * e^{-x}.dx$$

$$\gamma(n) = \int_{-\infty}^{\infty} (ax)^{n-1} * e^{-ax}.adx [x \longrightarrow ax]$$

$$\gamma(n) = a^n \int_{-\infty}^{\infty} x^{n-1} * e^{-ax}.dx$$

$$\frac{\gamma(n)}{a^n} = \int_{-\infty}^{\infty} x^{n-1} * e^{-ax}.dx$$

----------(3)

Now consider a=is

$$\frac{\gamma(n)}{is^n} = \int_{-\infty}^{\infty} x^{n-1} * e^{-isx}.dx = \frac{e^{-i\frac{n\pi}{2}}}{s^n}\gamma(n) \qquad (-i = e^{\frac{-i\pi}{2}})$$

$$F_c(s) = F_c(x^{n-1}) = \sqrt{\frac{2}{\pi}} \int_0^{\infty} f(x)\cos(sx).dx$$

$$= \sqrt{\frac{2}{\pi}}\int_0^{\infty} 15x^4\cos(sx).dx + \sqrt{\frac{2}{\pi}}\int_0^{\infty} 8x^3\cos(sx).dx + \sqrt{\frac{2}{\pi}}\int_0^{\infty} 6x^2\cos(sx).dx + \sqrt{\frac{2}{\pi}}\int_0^{\infty} 4x\cos(sx).dx + \sqrt{\frac{2}{\pi}}\int_0^{\infty} 24\cos(sx).dx$$

$$= \sqrt{\frac{2}{\pi}}\left(\frac{\gamma(n)}{s^n}\right)\cos\frac{n\pi}{2}$$

$$F_s(s) = F_s(x^{n-1}) = \sqrt{\frac{2}{\pi}} \int_0^{\infty} f(x)\sin(sx).dx \qquad \text{---------(4)}$$

$$= \sqrt{\frac{2}{\pi}} \int_0^{\infty} \left(15x^4 + 8x^3 + 6x^2 + 4x + 24\right) \sin(sx).dx$$

$$= \sqrt{\frac{2}{\pi}} \int_0^{\infty} 15x^4 \sin(sx).dx + \sqrt{\frac{2}{\pi}} \int_0^{\infty} 8x^3 \sin(sx).dx + \sqrt{\frac{2}{\pi}} \int_0^{\infty} 6x^2 \sin(sx).dx + \sqrt{\frac{2}{\pi}} \int_0^{\infty} 4x \sin(sx).dx + \sqrt{\frac{2}{\pi}} \int_0^{\infty} 24 \sin(sx).dx$$

$$= \sqrt{\frac{2}{\pi}} \left[15\frac{\gamma(5)}{s^5} * \sin\frac{5\pi}{2} + 8\frac{\gamma(4)}{s^4} * \sin\frac{4\pi}{2} + 6\frac{\gamma(3)}{s^3} * \sin\frac{3\pi}{2} + 4\frac{\gamma(2)}{s^2} * \sin\frac{\pi}{} + 24\frac{\gamma(1)}{s} * \sin\frac{\pi}{2} \right]$$

* For odd powers of x we take the Fourier cosine series and for even powers of x we consider the Fourier sine series

G(x)

$$\sqrt{\frac{2}{\pi}} \left[15\frac{\gamma(5)}{s^5} * \cos\frac{5\pi}{2} + 8\frac{\gamma(4)}{s^4} * \cos\frac{4\pi}{2} + 6\frac{\gamma(3)}{s^3} * \cos\frac{3\pi}{2} + 4\frac{\gamma(2)}{s^2} * \cos\frac{2\pi}{2} + 24\frac{\gamma(1)}{s} * \cos\frac{\pi}{2} \right]$$

$$= \sqrt{\frac{2}{\pi}} \left[15\frac{\gamma(5)}{s^5} * \sin\frac{5\pi}{2} + 8\frac{\gamma(4)}{s^4} * \sin\frac{4\pi}{2} + 6\frac{\gamma(3)}{s^3} * \sin\frac{3\pi}{2} + 4\frac{\gamma(2)}{s^2} * \sin\frac{\pi}{} + 24\frac{\gamma(1)}{s} * \sin\frac{\pi}{2} \right]$$

+

---------- (5)

IV. RESULTS AND DISCUSSIONS

In the research work two methodologies like Laplace and Fourier transformations were employed for exchanging secret messages from source to destination. In an unsecured network sent messages become vulnerable and sometimes are hacked and are also subjected to brutal force attack. The methodology deployed and employed works fine to keep the message intact.

There is no loss in the message, by the above mentioned methodologies. The Fourier transformation is bit faster than the Laplace transformation. The original message is added with salt and pepper and the message is encapsulated with a higher degree of security. The mathematical formation for the above example for a simple scenario, exhibits a correct outcome.

The Laplace and the Laplace inverse transformation and Fourier and the Fourier inverse transformation works fine in the security scenario. The 100 % retrieval of the message is possible in a faster manner. Intruders, sniffers and crypto analysts experience difficulty to break the key which was implemented with a higher degree of protection.

A. NUMERICAL EXAMPLE USING LAPLACE

Let us apply the above process to Encrypt and Decrypt a of words
"**HUMAN COMPUTER INTERFACE**".
Let us take the key as " **INTEL** ".This key is helpful to decrypt the Secret Message.

B. ENCRYPTION

```
H U M A N   C O M P U T E R  I N T E R F A C E
      +     +  +
 I N T E L    I N T E L I N T   E L I N T E L I N
----------    -------------------  ---------------------
P I G E Y     L C J T G D R L   M Y C R L J L K R
```

Consider -> P I G E Y
P=15(alphabetical order ,a=0,b=1.....p=15)
I=8,G=6,E=4,W=24
Therefore
$G(x)=15x^4+8x^3+6x^2+4x+24$

C.. USING LAPLACE

$L(G(x)) = L(15x^4)+L(8x^3)+L(6x^2)+L(4x)+L(24)$
since $L(k*X^n) = K*(n!/s^{n+1})$
$F(S)=15*(4!/s^5)+8*(3!/s^4)+6*(2!/s^3)+4*(1!/s^2)+24/s$

D. .DECRYPTION

1. Inverse Laplace
$F(S)=15*(4!/s^5)+8*(3!/s^4)+6*(2!/s^3)+4*(1!/s^2)+24/s$
$L^{-1}(F(S))=G(x)=15x^4+8x^3+6x^2+4x+24$
$L^{-1}(F(S))=L^{-1}(n-1!/S^n)=x^{n-1}*n!$
2.Consider coefficient of the polynomial
P=15,I=8,G=6,E=4,Y=24

3.Subtract key

```
P  I  G  E  Y
     (-)
I  N  T  E  L
-----------------------------------
15  8  6  4  24
     (-)
 8  13  19  4  11
---------------------------------------
 H  U  M  A  N
```

Therefore the plain text is HUMAN

B. For D encryption apply the Fourier Inverse Transformations .

$$= F_c^{-1}\left(\sqrt{\frac{2}{\pi}}\frac{\gamma(n)}{s^n} * \cos\frac{n\pi}{2}\right) + F_s^{-1}\left(\sqrt{\frac{2}{\pi}}\frac{\gamma(n)}{s^n} * \sin\frac{n\pi}{2}\right)$$

for Even powers of "S" applying inverse Cosine series we

$= 8x^3+4x$

for Odd powers of "S" applying inverse Sine series we get
$15x^4 + 6x^2 + 24$
used equation is $15x^4 + 8x^3 + 6x^2 + 4x + 24$
Therefore
P=15,I=8,G=6,E=4,Y=24
Subtract key :

```
P  I  G  E  Y
     (-)
I  N  T  E  L
-----------------------------------
15  8  6  4  24
     (-)
 8  13  19  4  11
-----------------------------------
 H  U  M  A  N
```

Therefore the plain text is HUMAN

V. CONCLUSION

The mathematical ideologies behind the work will safeguard the message and the key to a great extent. Breaking the key is not ans easy job, for the intruders to make some vulnerability to the packets. The Laplace and Fourier transforms with its respective inverse Functionalities play an inevitable role to keep the message with high protection.

In this work, the methods implement the job quickly, with high precision. The unauthorized person or the attacker can steal the information between source and destination. In this research work, it is clearly employed in all the segments with 360 degree security provided by the mathematical source..

REFERENCES

1. Martine Hell and Thomas Johnson, "Breaking the Stream Cipher F-FCSR-H and F-FCSR-16 in Real Time", Journal of Cryptology, October 2009.
2. G.Naga Lakshmi, B.Ravi Kumar and A.Chandra Sekhar, "A CRYPTOGRAPHIC SCHEME OF LAPLACE TRANSFORMS",International Journal Of Mathematical Archive-2(12),2011
3. A.P. Hiwarekar,"A NEW METHOD OF CRYPTOGRAPHY USING LAPLACE TRANSFORM",International Journal of Mathematical Archive-3(3), 2012.
4. Yannis Rouselakis, Brent Waters,"Efficient statically-secure large-universe multi-authority attribute-based encryption".International Conference on Financial Cryptography and Data Security, 315-332, 2015.
5. Shashank Agrawal, Shweta Agrawal, Saikrishna Badrinarayanan, Abishek Kumarasubramanian, Manoj Prabhakaran, Amit Sahai,"On the practical security of inner product functional encryption",IACR International Workshop on Public Key Cryptography, 777-798, 2015.
6. Qi Li, Jianfeng Ma, Rui Li, Jinbo Xiong, Ximeng Liu,"Large universe decentralized key-policy attribute-based encryption,Security and communication Networks"8 (3), 501-509, 2015.
7. Prabhanjan Ananth, Zvika Brakerski, Gil Segev, Vinod Vaikuntanathan",From selective to adaptive security in functional encryption",Annual Cryptology Conference, 657-677, 2015.
8. Takanori Yasuda, Kouichi Sakurai,"A multivariate encryption scheme with rainbow,International Conference on Information and Communications Security", 236-251, 2015.
9. N Saravana Kumar, GV Rajya Lakshmi, B Balamurugan,"Enhanced attribute based encryption for cloud computing",Procedia Computer Science 46, 689-696, 2015.
10. Zezhong Zhang, Qingqing Qi, Neeraj Kumar, Naveen Chilamkurti, Hwa-Young Jeong,"A secure authentication scheme with anonymity for session initiation protocol using elliptic curve cryptography,Multimedia Tools and Applications" 74 (10), 3477-3488, 2015.
11. Paul Kirchner, Pierre-Alain Fouque,"Improved BKW algorithm for LWE with applications to cryptography and lattices",Annual Cryptology Conference, 43-62, 2015.
12. Fatos Xhafa, Jingwei Li, Gansen Zhao, Jin Li, Xiaofeng Chen, Duncan S Wong,"Designing cloud-based electronic health record system with attribute-based encryption,Multimedia Tools and Applications" 74 (10), 3441-3458, 2015.
13. Romain Gay, Iordanis Kerenidis, Hoeteck Wee,"Communication complexity of conditional disclosure of secrets and attribute-basedencryption",Annual Cryptology Conference, 485-502, 2015.
14. Moreno Ambrosin, Mauro Conti, Tooska Dargahi,"On the feasibility of attribute-based encryption on Smartphone devices",Proceedings of the 2015 Workshop on IOT challenges in Mobile and Industrial Systems, 49-54, 2015,