DESIGN OF CRYPTOSYSTEM USING SHEHU TRANSFORMATION

Ravinder Kaur

School of Chemical Engineering and Physical Sciences, Lovely Professional University, Phagwara-144411, Punjab

ABSTRACT

In this paper used Shehu Transform[1] which is the generalized form of Laplace transforms for the construction of symmetric type cryptosystem. Shehu Transformation is implemented for the encryption and the corresponding inverse Shehu transformation is required for decryption.

Earlier the cryptosystems were based on the classical system but and most of the work is being done via internet or online so the security of maintaining the data is becoming challenges these days. So various fields of mathematics are playing important roles in the construction of new cryptosystem.

1.INTRODUCTION

The current era is the era of digitalization where all activities of life is being done online, be it shopping ,business , transactions etc. So data security is now a prime and critical issues so that it cannot not be hacked by unauthorized entity. So cryptography[5][6] is one of techniques to encrypt the sensitive data when it is being transmitted via the insecure channels. The main objective of the cryptography is to provide the security to the content of two persons who are communicating over insecure channels so that no adversary can trace what is being transmitted.

2.RELATED WORK AND PROPOSED METHOD

The Laplace integral transformation for the construction of cryptography schemes is being proposed by Hiwarekar[2][3][4]and Extensive work is also shown by Sachin & Bani in 2013 and by Swati Dhingra, Archana A.Savalgi and Swati Jain [7] by presenting new scheme for the cryptographic purpose by combining infinite series and Laplace transform using ASCII code. In the paper proposing the use of Shehu Transform[1]. The Shehu transform is used for encrypting the data and the corresponding inverse Shehu transform is applied for decrypting the data. Shehu Transform was introduced by Shehu Maitama and Weidong Zhao in 2019

Proposed Method:

In this paper discussed the scheme for cryptosystem using Shehu Transformation[1].

3.Shehu Transform

Definition : The Shehu transformation [1] :- consider the function $f(x)$ in set $\mathcal{A}$ defined as

$$\mathcal{A} = \left\{ f(x): \exists \mathrm{N}, \eta_1, \eta_2 > 0, |f(x)| < \mathrm{N}\exp\left(\frac{|x|}{\eta_i}\right), if\ x \in (-1)^i \times [0,\infty) \right\},$$

Then the Shehu transformation of $f(x)$ is defined as

$\mathbb{S}[f(x)] = F(\omega,u) = \int_0^\infty f(x)e^{(-\omega x/u)}dx \ \ ; \ \omega > 0$ provided integral exists

And corresponding Inverse of Shehu transform is given by

$\mathbb{S}^{-1}[F(\omega,u)] = f(x), \ \ with \ x \geq 0$

Properties of Shehu Transform

It satisfies Linearity property

$\mathbb{S}[\alpha f(x) + \beta g(x)] = \alpha\mathbb{S}[f(x) + \beta\mathbb{S}[g(x)]$

3. *Standard results required in this paper*

(i) $\mathbb{S}[1] = \frac{u}{\omega}$ and

(ii)$\mathbb{S}[x] = \frac{u^2}{\omega^2}$

(iii)$\mathbb{S}\left[\frac{x^m}{m!}\right] = \frac{u^{(m+1)}}{\omega^{(m+1)}}$ for $m = 0,1,2, \ldots$

(iv)$\mathbb{S}^{-1}\left[\left(\frac{u}{\omega}\right)^{(m+1)}\right] = \frac{x^m}{m!}$

4. **Proposed Algorithm**

(i)Encryption Algorithm:

Step1 : Converting every letter in plaintext into a number such as ; A=1; B=2;C=3….Z=26

Step 2: Obtain the sequence of numbers corresponding to each plaintext using substitution discussed in step 1. Let us consider the Plaintext HELLO with number of letters m=5

Using above substitution converting each symbol into numbers we get

H=8, E=5, L=12,L=12, O=15

So the finite sequence of plain text is:

8,5,12,12,15

Step 3: If there are m+1 number of terms in a sequence we will consider a polynomial of mth degree . As in the given example we have 5 number of terms so the consider the polynomial $p(x)$ of degree 4.

The associated polynomial would be

$p(x) = 8 + 5x + 12x^2 + 12x^3 + 15x^4$

Step 4: Apply Shehu transformation on polynomial we get

$\mathbb{S}[p(x)] = \mathbb{S}[8 + 5x + 12x^2 + 12x^3 + 15x^4]$

$= \mathbb{S}[8] + \mathbb{S}[5x] + \mathbb{S}[12x^2] + \mathbb{S}[12x^3] + \mathbb{S}[15x^4]$

$=8\frac{u}{\omega}+5\frac{u^2}{\omega^2}+12\frac{2!\,u^3}{\omega^3}+13\frac{3!u^4}{\omega^4}+15\frac{4!u^5}{\omega^5}$

$= \sum_{i=0}^{4} q_i \left(\frac{u}{\omega}\right)^{i+1}$

Step 5 : Expressing each q_i =$26k_i + r_i = r_i mod 26$, to finding the corresponding sequence of residues r_i and keys using mod26

$q_0 = 8 = 26(0) + 8 = 8mod26 = 26k_0 + r_0 mod26$ = ;

$q_1 = 5 = 26(0) + 5 = 5mod26 = 26k_1 + r_1 mod26$

$q_2 = 24 = 26(0) + 24 = 24mod26=26k_2 + r_2 mod26$

$q_3 = 78 = 26(3) + 0 = 0mod26=26k_3 + r_3 mod26$

$q_4 = 360 = 26(13) + 22 = 22mod26=26k_0 + r_4 mod26$

The sequence of keys k_i $(i = 0\ to\ 4)$ $k_0 = 0$, $k_1 = 0$, $k_2 = 0$, $k_3 = 3$, $k_4 = 13$

And the new sequence in r_i $(i = 0\ to\ 4)$ is 8, 5, 24, 0, 22

Hence the ciphertext would be HEXZV

(ii)Decryption Algorithm:

Step 1: The received cipher text and the sequence of key from sender as

Ciphertext : HEXZV and sequence of keys: 0.0,0,3,13

Step 2: Retrieve $q_i = 26k_i + r_i$ where $i = 0,1,2,3,4$

sequence in r_i $(i = 0\ to\ 5)$ obtained by converting HEWNX into numbers as 8, 5, 24, 0, 22

$q_0 = 26(0) + 8 = 8$

$q_1 = 26(0) + 5 = 5$

$q_2 = 26(0) + 24 = 24$

$q_3 = 26(3) + 0 = 78$

$q_4 = 26(13) + 22 = 360$

Step 3: Obtain the expression

$F(\omega, u) = \sum_{i=0}^{m} q_i \left(\frac{u}{\omega}\right)^{i+1}$, m=4

$F(\omega, u) = 8\left(\frac{u}{\omega}\right) + 5\left(\frac{u}{\omega}\right)^2 + 24\left(\frac{u}{\omega}\right)^3 + 78\left(\frac{u}{\omega}\right)^4 + 360\left(\frac{u}{\omega}\right)^5$

Step 4: Apply Inverse Shehu Transfrom

$\mathbb{S}^{-1}[F(\omega, u)] = \mathbb{S}^{-1}[8\left(\frac{u}{\omega}\right) + 5\left(\frac{u}{\omega}\right)^2 + 24\left(\frac{u}{\omega}\right)^3 + 78\left(\frac{u}{\omega}\right)^4 + 360\left(\frac{u}{\omega}\right)^5]$

$p(x) = 8\frac{x^0}{0!} + 5\frac{x^1}{1!} + 24\frac{x^2}{2!} + 78\frac{x^3}{3!} + 360\frac{x^4}{4!}$

$p(x) = 8 + 5x + 12x^2 + 12x^3 + 15x^4$

Step 5: Retrieve the coefficients of the polynomial $p(x)$ finite sequence

8,5,12,12,15

Step 6: Decoding the sequence of numbers into alphabet we get plaint test

HELLO

5.CONCLUSION

In the present work cryptographic scheme developed using generalized Laplace Transform know as Shehu Transform introduced in 2019 with the algebraic function using on 26 English alphabets .Under the same transformation work can be extended to use of other function with the ASII codes.

6.REFERENCES

[1] Hiwarekar A.P., A new method of cryptography using Laplace transform, International Journal of Mathematical Archive,3(3),1193-1197,(2012).

[2]A.P.Hiwarekar, Application of Laplace Transform For Cryptographic Scheme, Proceedings of the World Congress on Engineering 2013 Vol I, WCE 2013, July 3 - 5, 2013, London, U.K

[3]Hiwarekar A.P., A new method of cryptography using Laplace transform of hyperbolic functions, International Journal of Mathematical Archive,4(2),208-213,(2013).

[4]Stallings W., Cryptography and Network Security, Fourth Edition, Prentice Hall, 2005.

[5] Grewal B. S. – Higher Engineering Mathematics, Khanna Pub. Delhi, 2005.

[6]Swati Dhingra, Archana A. Savalgi, Swati Jain, Laplace Transformation based Cryptographic Technique in Network Security, International Journal of Computer Applications (0975 – 8887) Volume 136 – No. 7, February 2016.