INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

IJARIIT

ISSN: 2454-132X
Impact factor: 6.078
(Volume 6, Issue 3)
Available online at: www.ijariit.com

Use of Discrete Sumudu Transform in cryptography

Sarada Mahesh Madhukar
mahesh.sarada@gmail.com
Pimpri Chinchwad College of Engineering and Research, Pune, Maharashtra

Mundhe Ganesh Ashruji
ganumundhe@gmail.com
Army Institute of Technology, Pune, Maharashtra

Shaikh Jamir Salim
jamir.shaikh786@gmail.com
R. C. Patel Institute of technology, Shirpur, Maharashtra

ABSTRACT

Cryptography is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it. Modern cryptography uses sophisticated mathematical equations (algorithms) and secret keys to encrypt and decrypt data. Today, cryptography is used to provide secrecy and integrity to our data, and both authentication and anonymity to our communications. In this paper we have to encrypt and decrypt a secret data using discrete Sumudu transformation and congruence modulo operator relation.

Keywords*— Engineering, cryptography, encryption, decryption, Modern Sciences*

1. INTRODUCTION

Cryptography is technique of securing information and communications through use of codes so that only those people for whom the information is intended can understand it and process it. Thus preventing unauthorized access to information. More generally, cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages, various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation are central to modern cryptography. Modern cryptography uses sophisticated mathematical equations (algorithms) and secret keys to encrypt and decrypt data Applications of cryptography include ATM cards, computer passwords, and electronic commerce.

Cryptography not only protects data from theft or alteration, but can also be used for user authentication. Cryptography referred almost exclusively to encryption, which is the process of converting ordinary information (called plaintext) into unintelligible text (called cipher text). Decryption is the reverse, in other words, moving from the unintelligible cipher text back to plaintext. A cipher (or cipher) is a pair of algorithms that create the encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm and in each instance by a “encryption key” and “decryption key”. The key is a secret (ideally known only to the communicants), usually a short string of characters, which is needed to decrypt the cipher text. Many research papers are available on cryptography (see [1, 2, 3, 4, 5, 6, and 7]).

Symmetric-key Cryptography: Both the sender and receiver share a single key. The sender uses this key to encrypt plaintext and send the cipher text to the receiver. On the other side the receiver applies the same key to decrypt the message and recover the plain text.

Public-Key Cryptography: This is the most revolutionary concept in the last 300-400 years. In Public-Key Cryptography two related keys (public and private key) are used. Public key may be freely distributed, while its paired private key remains a secret. The public key is used for encryption and for decryption private key is used.

In this process we have basic Encryption and Decryption like sender send the Plaintext message by encryption method it converts into cipher text and then by decrypting method will get same plaintext message. With Sumudu Transform we use private key as a secret key for sending and receiving the secret message. Defence strategies are mostly based on machine learning and signal processing principles that either tries the classical cryptographic component in the defence. In this work, we propose a new defence mechanism based on the cryptographic principle which states that the defence and classification algorithm are supposed to be known, but not the key.

Definition of Discrete Sumudu Transform: Over the set of functions

$$A = \{f(t) \mid \exists M, \tau_1, \tau_2 > 0, |f(t)| < Me^{|t|/\tau_j}, \text{ if } t \in (-1)^j \times [0, \infty)\}$$

The Sumudu transform is defined by

$$G\ (u) = S\ [f\ (t)] = \int_0^\infty f(ut)\ e^{-t}\, dt \quad , u \in (-\tau_1, \tau_2)$$

Sumudu transform which is itself linear, preserves linear function and hence in particular does not change its unit.
Sumudu transform amplifies the coefficients of the power series function,

$$\boldsymbol{f(t)} = \sum_{n=0}^{\infty} (\boldsymbol{a_n}\ \mathbf{t^n})\ ,$$

By sending it to the power series function

$$\boldsymbol{G(u)} = \sum_{n=0}^{\infty} \mathbf{n!}\ (\boldsymbol{a_n}\ \mathbf{u^n})$$

Properties of Sumudu transform:

1. If f(t)=1 then $G(u) = S[f(t)] = 1$
2. If f(t)=t then $G(u) = S[f(t)] = u$
3. If $f(t) = \frac{t^{n-1}}{n-1!}$, $n = 1,2,3, \ldots$ then $G\ (u) = S\ [f\ (t)] = u^{n-1}$
4. If $G\ (u) = u^n$ then $S^{-1}\ [G\ (u)] = f\ (t) = 1/n!\ (\ t^n)$

2. ENCRYPTION ALGORITHM

I) Treat every letter in the plain text message as a number, so that A=1, B=2, C=3,…Z=26, [space]=0.

II) The plain text message is organized as finite sequence of numbers based on the above conversion. For example, our text is "ATTACK AT ONCE".
Based on the above step; we know that, A=1, T=20, C=3, K=11, O=15, N=14, E=5. Therefore, our plain text finite sequence is 1,20,20,1,3,11,0,1,20,0,15,14,3,5.

III) If $n + 1$ are the number of terms in the sequence; consider a polynomial of degree n with coefficient as the term of the given finite sequence.

IV)
Above Finite sequence contains 13+1 terms. Hence consider a polynomial (t) of degree 13.

$$P\ (t) = 1 + 20\ t + 20t^2 + 1t^3 + 3t^4 + 11t^5 + 0t^6 + 1t^7 + 20t^8 + 0t^9 + 15t^{10} + 14t^{11} + 3t^{12} + 5t^{13}$$

V) Take Sumudu transform of polynomial P (t)

$$S\ \{P\ (t), u\} = S\ \{1 + 20\ t + 20t^2 + 1t^3 + 3t^4 + 11t^5 + 0t^6 + 1t^7 + 20t^8 + 0t^9\ + 15t^{10} + 14t^{11} + 3t^{12} + 5t^{13}\}$$
$$= 1 + 20u + 20(2!)u^2 + 1(3!)u^3 + 3(4!)u^4 + 11(5!)u^5 + 0(6!)\ u^6 + 1(7!)\ u^7$$
$$+20(8!)\ u^8 + 0(9!)\ u^9 + 15(10!)\ u^{10} + 14(11!)\ u^{11} + 3(12!)\ u^{12} + 5(13!)\ u^{13}$$
$$= 1 + 20u + 40u^2 + 6u^3 + 72u^4 + 1320u^5 + 5040\ u^7 + 806400\ u^8\ \ + 54432000u^{10} + 558835200\ u^{11} + 1437004800$$
$$u^{12} + 31135104000\ u^{13}$$
$$= \sum_{i=0}^{11+1} qi\ u^{i+1} \quad \text{, neglecting constant term.}$$

V) Next find r_i such that $q_i \equiv r_i\ mod\ 26$ for each, $1 \le i \le n + 1$.

Therefore,

$q_1 = 20 \equiv 20\ mod\ (26)$, $\qquad q_2 = 40 \equiv 14\ mod\ (26)$
$q_3 = 6 \equiv 6\ mod\ (26)$, $\qquad q_4 = 72 \equiv 20\ mod\ (26)$
$q_5 = 1320 \equiv 20\ mod\ (26)$, $\qquad q_7 = 5040 \equiv 22\ mod\ (26)$
$q_8 = 806400 \equiv 10\ mod\ (26)$, $\qquad q_{10} = 54432000 \equiv 12\ mod\ (26)$
$q_{11} = 558835200 \equiv 14\ mod\ (26)$, $q_{12} = 1437004800 \equiv 10\ mod\ (26)$,
$q_{13} = 31135104000 \equiv 0\ mod\ (26)$.

VI) Hence $q_i = 26k_i + r_i$
Thus we get a key k_i for $i = 1, 2, 3, \ldots n + 1$.
$\therefore k_1 = 0, k_2 = 1, k_3 = 0,\ \ k_4 = 2, k_5 = 50, k_7 = 193, k_8 = 31015,$
$k_{10} = 2093538, k_{11} = 21493661, k_{12} = 55269415, k_{13} = 1197504000$

VII) Now consider a new finite sequence $r_1, r_2, \ldots, r_{n+1}$
i.e. 20, 14, 6, 20, 20, 22, 10, 12, 14, 10, 0.

3. DECRYPTION ALGORITHM

I) Consider the cipher text and key received from sender. In the above example cipher text is "TNFTTVJLNJ" and key is 0, 1,0,2,50,193,31015, 2093538, 21493661, 55269415, 1197504000

II) Convert the given cipher text to corresponding finite sequence of numbers $r_1, r_2, \dots, r_{n+1}$.
ie. 20, 14, 6, 20, 20, 22, 10, 12, 14, 10, 0.

III) Let $q_i = 26k_i + \mathrm{r}_i, \forall i = 1, 2, 3, \dots, \mathrm{n}+1$.

$q_1 = 26 \times 0 + 20 = 20$, $q_2 = 26 \times 1 + 14 = 40$
$q_3 = 26 \times 0 + 6 = 6$, $q_4 = 26 \times 2 + 20 = 72$
$q_5 = 26 \times 50 + 20 = 1320$, $q_7 = 26 \times 193 + 22 = 5040$
$q_8 = 26 \times 31015 + 10 = 806400$, $q_{10} = 26 \times 2093538 + 12 = 54432000$
$q_{11} = 26 \times 21493661 + 14 = 558835200$, $q_{12} = 26 \times 55269415 + 10 = 1437004800$
$q_{13} = 26 \times 1197504000 + 0 = 31135104000$

IV) The inverse discrete sumudu transform f (t) of the power series

$$\mathrm{G}(\mathrm{u}) = \sum_{n=0}^{\infty} \boldsymbol{b_n}\ \boldsymbol{u^n} \text{ is given by, } \boldsymbol{S^{-1}}[\mathbf{G}(\boldsymbol{u})] = \boldsymbol{f}(\boldsymbol{t}) = \sum_{n=0}^{\infty} (\mathbf{1}/\mathbf{n}!)\boldsymbol{b_n}\ \boldsymbol{t^n}$$

Let S {P (t), u} = $\sum_{i=0}^{11+1}(\boldsymbol{q_i}\ \mathbf{u}^{\mathbf{i+1}})$

$$\mathrm{P}(\mathrm{t}) = 1 + 20\mathrm{u} + 40u^2 + 6u^3 + 72u^4 + 1320u^5 + 5040\,u^7 + 806400\,u^8 \quad + 54432000u^{10} + 558835200\,u^{11} + 1437004800\,u^{12} + 31135104000\,u^{13}$$

V) Now take the Inverse Sumudu transform of

$$\therefore \mathrm{S}^{-1}\ \{\mathrm{P}(\mathrm{t}), \mathrm{u}\} = \mathrm{S}^{-1}\{1 + 20\mathrm{u} + 40u^2 + 6u^3 + 72u^4 + 1320u^5 + 5040\,u^7 + 806400\,u^8 \quad + 54432000u^{10} + 558835200\,u^{11} + 1437004800\,u^{12} + 31135104000\,u^{13}\}$$

$$\mathrm{P}(\mathrm{t}) = 1 + 20\,\mathrm{t} + 20\mathrm{t}^2 + 1\mathrm{t}^3 + 3\mathrm{t}^4 + 11\mathrm{t}^5 + 0\mathrm{t}^6 + 1\mathrm{t}^7 + 20\mathrm{t}^8 + 0\mathrm{t}^9 + 15\mathrm{t}^{10} + 14\mathrm{t}^{11} + 3\mathrm{t}^{12} + 5\mathrm{t}^{13}$$

VI) Consider the coefficient of a polynomial P (t) as a finite sequence.

1,20,20,1,3,11,0,1,20,0,15,14,3,5.

VII) Now translating the number of above finite sequence to alphabets. We get the original plain text as “ATTACK AT ONCE”

4. CONCLUSION

In the proposed work a new cryptographic scheme is introduced using discrete Sumudu Transform and the private key is the number of multiples of mod n.

5. REFERENCES

[1] F. B. M. Belgacem, A. A. Karaballi, and S. L. Kalla, “Analytical investigations of the Sumudu transform and applications to integral production equations,” *Mathematical Problems in Engineering*, vol. 2003, no. 3, pp. 103–118, 2003.

[2] Shaikh. J. S. and Mundhe G. A. on “Application of "El-Zaki Transform in cryptography" *International Journal of Modern Sciences and Engineering Technology*, Vol 3, no 3, 2016.

[3] Tarig. M. Elzaki and Salih M. Ezaki, On the Connections between Laplace and ELzaki Transforms, Advances in Theoretical and Applied Mathematics, Vol 6 , 2011, pp. 1-10

[4] Tarig. M. Elzaki and Salih M. Ezaki, Application of New Transform "Elzaki Transform" To Partial Differential Equations, Global Journal of Pure and Applied Mathematics, Vol 7, 2011, Page Numbers 65-70.

[5] G. Naga Lakshmi, B. Ravi Kumar and A. Chandra Sekhar, A Cryptographic scheme of Laplace transforms, International Journal of Mathematical Achiever, vol 2011, pp. 65-70.

[6] A.P. Stakhov, “The golden matrices and a new kind of cryptography”, Chaos, Solutions and Fractals

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