International Journal of Modern Agriculture,Volume 10, No.1, 2021
ISSN: 2305-7246

Application of Sawi transform in Cryptography

R. Bhuvaneswari[11]and K. Bhuvaneswari[2]
[1,2] Assistant Professor
Postgraduate Department of Mathematics
BMS College for Women
Bengaluru, India

Abstract

Cryptography is the science of secret communication. Encryption is a process used to convert the given original text into a secret text known as cipher text. Decryption is a process of converting the cipher text into the original text. In this paper, we discuss an encryption and decryption algorithm based on Sawi transform. We illustrate the algorithms by an example.

Keywords: Sawi transform, encryption, decryption, plain text, cipher text.
Subject classification 2020: 94A60,4400

Introduction

Cryptography is the science of secret and secured communication [1]. Encryption is a process of encoding (converting) a given original text (called plain text) into a cipher text. Decryption is a process of decoding (re-converting) the cipher text into the original text [4]. Various cryptographic techniques based on mathematical algorithms have been introduced [1, 4]. Cryptography is used various fields (including agriculture) where data security is important.

Integral transforms has its applications in various fields. Recently, integral transforms has been employed in cryptography [2, 3]. Sawi transform transform was introduced by Mohand Mahgoub [5]. In this paper, we provide an encryption and a decryption algorithm based on Sawi transform and affine cipher. We also illustrate the proposed algorithm by an example.

Sawi Transform

In this section, we give the definition and basic properties of Sawi transform [5].

Let

$$A = \{f(t) : \exists M, k_1, k_2 > 0 \ni |f(t)| < Me^{\frac{|t|}{k_j}}, \text{ for } t \in (-1)^j \times [0,\infty)\}$$

where M is a finite constant and k_1,k_2 may be finite or infinite. For $f(t) \in A$, the Sawi transform $S(.)$ is defined by

$$S[f(t)] = R(v) = \frac{1}{v^2}\int_0^\infty f(t)e^{-t/v}\,dt, \quad k_1 \le v \le k_2$$

provided the integral exists.

[1] First and Corresponding author

Remark: The sufficient conditions for the existence of Sawi transform are that $f(t)$ for $t \geq 0$ be piecewise continuous and of exponential order.

Sawi transform of some basis functions

1. $f(t) = 1,\ S[f(t)] = R(v) = \frac{1}{v}$.
2. $f(t) = t$, $S[f(t)] = R(v) = 1$.
3. For $n \geq 2$, $f(t) = t^n$, $S[f(t)] = R(v) = v^{n-1}n!$.

Inverse Sawi transform

If $S[f(t)] = R(v)$ then the inverse sawi transform is $S^{-1}(R(v)) = f(t)$.

1. $S^{-1}[\frac{1}{v}] = 1$.
2. $S^{-1}[1] = t$.
3. $S^{-1}[v^{n-1}] = t^n/n!$ for $n \geq 1$.

Property

Sawi transform satisfies the linearity property.

$$S[af(t) + bg(t)] = aS[f(t)] + bS[g(t)].$$

Main Results

In this section, we give an encryption and a decryption algorithm based on sawi transform and affine cipher.

Using the table below, we convert the alphabets into numbers and viceversa.

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Here upper case and lower case alphabets are undifferentiated, special characters and spaces are not considered.

Encryption Algorithm

(i) Assign every alphabet in the plain text to a number.

(ii) Corresponding to the plain text consider the

$$E(x) = ax + b \ (mod 26),$$

where a and b are keys for ciphers and a is co-prime to 26.

(iii) Let $p(t)$ be the polynomial of degree $n-1$ with coefficients as $E(x)$. Here n is the number of terms in the plain text.

(iv) Apply Sawi transform to $p(t)$.

(v) Let $S[p(t)] = R(v) = \sum_{i=0}^{n-1} q_i v^{i-1}$.

(vi) Write $q_i = 26c_i + r_i$ for each i with $0 < r_i < 26$.
Here $c_i's$ are the keys.

(vii) By converting each r_i to its corresponding alphabet, we can get the cipher text.

Decryption Algorithm

Assume the secret keys a, b are known to the receiver.
Consider the cipher text with the keys $c_0,c_1,...,c_{n-1}$.

1. Convert the cipher text into the number sequence $r_0,r_1,...,r_{n-1}$.
2. Find $q_i = 26c_i + r_i$ for each $i = 0,1,2,\cdots,n-1$.
$$n-1$$
3. Let $R(v) = \sum_{i=0} q_i v^{i-1}$.
4. Apply inverse Sawi transform to $R(v)$ and get the polynomial $p(t)$ of degree $n-1$.
5. Consider the coefficients of $p(t)$ as a number sequence. 6. For each number y in the number sequence, calculate
$$D(y) = a^{-1}(y - b) \ (mod 26).$$
Here a^{-1} denotes the multiplicative inverse of 'a' under modulo 26.

7. By converting the resulting number sequence into alphabets, we can get the original text.

Illustrative Example

Consider the plain text

"**DELIGHT**"

Take $a = 11$ and $b = 13$. Then clearly 11 is co-prime to 26 and $a^{-1} = 19$.

Encryption

1. The number sequence corresponding the plain text after applying affinecipher is given below.

Plain text	D	E	L	I	G	H	T
Number sequence	4	5	12	9	7	8	20
$ax + b = 11x + 13$	57	68	145	112	90	101	233
$E(x) = 11x + 13(mod 26)$	5	16	15	8	12	23	25

Therefore, the number sequence is 5,16,15,8,12,23,25.

2. Here $n = 7$.
Let $p(t) = 5 + 16t + 15t^2 + 8t^3 + 12t^4 + 23t^5 + 25t^6$.

3. By applying Sawi transform to $p(t)$, we get

$$\begin{aligned} S[p(t)] = R(v) &= S[5 + 16t + 15t^2 + 8t^3 + 12t^4 + 23t^5 + 25t^6] \\ &= S[5] + 16S[t] + 15S[t^2] + 8S[t^3] + 12S[t^4] + 23S[t^5] + 25S[t^6] \\ &= 5\frac{1}{v} + 16 + 15 \times 2!v + 8 \times 3!v^2 + 12 \times 4!v^3 + 23 \times 5!v^4 + 25 \times 6!v^5 \\ &= \frac{5}{v} + 16 + 30v + 48v^2 + 288v^3 + 2760v^4 + 18000v^5 \end{aligned}$$

Thus $q_0 = 5, q_1 = 16, q_2 = 30, q_3 = 48, q_4 = 288, q_5 = 2760, q_6 = 18000$

4. For each i, write $q_i = 26c_i + r_i$. We get $c_0 = 0, c_1 = 0, c_2 = 1, c_3 = 1, c_4 = 11, c_5 = 106, c_6 = 692$ and $r_0 = 5, r_1 = 16, r_2 = 4, r_3 = 22, r_4 = 2, r_5 = 4, r_6 = 8$

5. Convert the number sequence $r_0, r_2, r_2, r_3, r_4, r_5, r_6$ into alphabets

5	16	4	22	2	4	8
E	P	D	V	B	D	H

Thus the cipher text is "**EPDVBDH**"

Decryption

Consider the cipher text "**EPDVBDH**" with the keys $c_0 = 0, c_1 = 0, c_2 = 1, c_3 = 1, c_4 = 11, c_5 = 106, c_6 = 692$

1. The number sequence corresponding to the cipher text is $r_0 = 5, r_1 = 16, r_2 = 4, r_3 = 22, r_4 = 2, r_5 = 4, r_6 = 8$
2. For each i, write $q_i = 26c_i + r_i$. Then we get $q_0 = 5, q_1 = 16, q_2 = 30, q_3 = 48, q_4 = 288, q_5 = 2760, q_6 = 18000$
3. Take $R(v) = \sum_{i=0}^{n-1} q_i v^{i-1}$. Then

$$R(v) = \frac{5}{v} + 16 + 30v + 48v^2 + 288v^3 + 2760v^4 + 18000v^5$$

4. Apply inverse Sawi transform to $R(v)$, we get

$$S^{-1}[R(v)] = p(t) = 5 + 16t + 15t^2 + 8t^3 + 12t^4 + 23t^5 + 25t^6.$$

5. Consider the coefficients as a number sequence. Then we get the number sequence as 5,16,15,8,12,23,25.

6. For each y in the number sequence, calculate $D(y) = 19(y-13) \pmod{26}$

	5	16	15	8	12	23	25
$19(y-13)$	-152	57	38	-95	-19	190	228
$D(y) = 19(y-13) \pmod{26}$	4	5	12	9	7	8	20
Plain text	D	E	L	I	G	H	T

Thus the plain text is "**DELIGHT**"

Conclusion

In cryptography, mathematical techniques have been employed to secure messages. In this paper, we have introduced an encryption algorithm using Sawi transform and a decryption algorithm using inverse Sawi transform.. We illustrated the proposed algorithm by an example.

References

[1] Barr T.H., "Invitation to Cryptography", Prentice Hall, 2002.

[2] Bhuvaneswari R and Bhuvaneswari K., "Application of Yang transform in cryptograpy", *International Journal of Engineering, Science and Mathematics*, Vol. 9 Issue 3, (March 2020), pp. 41 - 45.

[3] Hiwarekar A.P., "Application of Laplace Transform for Cryptographic Scheme", *Proceeding of World Congress on Engineering*, Vol. II 2013, LNCS, pp. 95 - 100.

[4] Johannes A. Buchmann., “Introduction to Cryptography”, Fourth Edn., Indian Reprint, Springer, 2009.

[5] Mohand M. Abdelrahim Mahgoub “The New Integral Transform ”Sawi Transform” ”, *Advances in Theoretical and Applied Mathematics*, Vol 14, No. 1 (2019), pp. 81-87.