International Journal of Engineering, Science and Mathematics
Vol. 9 Issue 3, March 2020,
ISSN: 2320-0294 Impact Factor: 6.765
Journal Homepage: http://www.ijesm.co.in, Email: ijesmj@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

APPLICATION OF YANG TRANSFORM IN CRYPTOGRAPHY

Dr. R. Bhuvaneswari*
Dr. K. Bhuvaneswari**

ABSTRACT

Cryptography is the science of secret communication. Mathematics algorithms to encrypt and decrypt a data play an important role in cryptography. Integral transforms plays an important role in the field of Applied mathematics. In this paper, we introduced an encryption and decryption algorithm based on Yang transform and affine ciphers.

KEYWORDS:

Cryptography;
Yang transform;
Plain text;
Cipher text;
Affine cipher.

Author correspondence:

Dr. R. Bhuvaneswari,
Assistant professor,
Post Graduate department of Mathematics,
BMS College for Women, Basavanagudi,
Bangalore, India.

1. INTRODUCTION

Cryptography is a science of secured communications. In this modern world, the utilization of internet and computers are more significant. Securing the data transferred in the communication media is an important issue. Cryptography provides methods to secure the data. Various techinques for cryptography can be found in literature [1,3]. Encryption and decryption algorithms based an integral transforms can be found in [2].

Xiao Jung Yang introducted a new integral transform known as "Yang transform" to solve steady heat transfer problem [4]. The properties of Yang transform were investigated and it is used to solve ordinary and partial differential equations.

In this paper, we introduced an encryption and decryption algorithm using the Yang transform.

2. YANG TRANSFORM

The Yang transform is defined for the function of exponential order.

Let $A = \left\{ f(t): \exists M, k_1, k_2 > 0 \ni |f(t)| \leq M e^{\frac{|t|}{k_j}} \right\}$ where M, k_1, k_2 are constants.

Here M is a finite number and k_1, k_2 may be finite or infinite.

The Yang transform of the function $f(t) \in A$ is denoted by $Y[f(t)]$ or $T(u)$ and is defined as [4]

$$Y[f(t)] = T(u) = \int_0^{\infty} f(t) e^{\frac{-t}{u}} \, dt \ , t > 0 \qquad (1)$$

provided the integral exists, where $u \in (-k_1, k_2)$.

By substituting $x = \frac{t}{u}$ in equation (1) we get

$$T(u) = u \int_0^{\infty} f(ux) e^{-x} \ dx \ , x > 0 \qquad (2)$$

The Laplace transform of $f(t)$ is

$$L[f(t)] = F(u) = \int_0^{\infty} f(t) e^{-ut} \ dt \ , t > 0 \qquad (3)$$

If we take $x = ut$, the equation (3) becomes

$$F(u) = \frac{1}{u} \int_0^{\infty} f(x/u) e^{-x} \ dx \ , t > 0 \qquad (4)$$

By the equations (2) and (4), the relation between Yang transform and the Laplace transform of $f(t)$ is

$$T(u) = F\left(\frac{1}{u}\right) \qquad (5)$$

2.1 Yang transform of some functions

1. Let $f(t) = 1$ then $Y[1] = T(u) = u$.
2. Let $f(t) = t$ then $Y[t] = T(u) = u^2$.
3. Let $f(t) = t^n$ then $Y[t^n] = T(u) = n! \ u^{n+1}$.

2.2 Properties of Yang transform

Yang transform satisfies the following property [4]

1. Linearity Property: If $Y[f(t)] = T_1(u)$ and $Y[g(t)] = T_2(u)$ then $Y[af(t) + bg(t)] = aY[f(t)] + bY[g(t)] = T_1(u) + T_2(u)$ for any constants a & b.
2. Translation property: If : If $Y[f(t)] = T(u)$ then $Y[f(ct)] = \frac{1}{c} T\left(\frac{u}{c}\right)$ for any nonzero constant c.

2.3 Inverse Yang transform

1. If $Y[f(t)] = T(u) = u$ then $f(t) = 1$.

2. If $Y[f(t)] = T(u) = u^2$ then $f(t) = t$
3. If $Y[f(t)] = T(u) = u^n$ then $f(t) = \frac{t^{n-1}}{(n-1)!}$.

3. MAIN RESULT

In this section, we provide an encryption algorithm and decryption algorithm based on Yang transform.

3.1. Encryption Algorithm

1. Assign every alphabet in the plain text as a number like A=1, B=2, C=3, …,Z=26.
2. Consider the number sequence corresponding to the plain text.
3. Replace each number x in the plain text as $E(x) = ax + b \ (mod\ 26)$ where a& b are keys for ciphers and $a$is co-prime to 26.
4. Consider a polynomial $p(t)$ of degree $n-1$ where n denote the number of terms in number sequence.
5. Apply Yang transform to $p(t)$.
6. Consider the co-efficients of $Y[p(t)]$as $q_1, q_2, \dots, q_n$.
7. Find r_i such that $q_i \equiv r_i (mod\ 26)$ and find the keys c_i, for each $i = 1,2,3, \dots, n$ where $q_i = 26c_i + r_i$
8. Consider the number sequence $r_1, r_2, \dots, r_n$
9. Convert the numbers into the corresponding alphabets we get the cipher text.

3.2. Decryption Algorithm

Assume the receiver knows the secret keys a and b. The cipher text will be given with the corresponding keys$c_1, c_2, \dots, c_n$.

1. Convert the alphabets in the cipher text into the number sequence $r_1, r_2, \dots, r_n$.
2. Let $q_i = 26c_i + r_i$ for each $i = 1,2,3, \dots, n$.
3. Let $T(u) = \sum_{i=1}^{n} q_i\, u^i$.
4. Take the inverse Yang transform of $T(u)$ and get $p(t)$.
5. Consider the co-efficients of $p(t)$ as a finite number sequence.
6. Repace each number in that sequence by $D(y) = a^{-1}(y - b) \ \ (mod\ 26)$ where a^{-1} is the multiplicative inverse of a under modulo 26.
7. Convert the resulting sequence to alphabets we get the original plain text.

3.3. Example

Consider the plain text TEACHER

Choose $a = 7$and $b = 8$. Clearly 7 is co-prime to 26 and $a^{-1} = 15$

3.3.1 Encryption

1. The number sequence corresponding to the plain text is

Plain text	T	E	A	C	H	E	R
Plain text value x	20	5	1	3	8	5	18
$ax + b = 7x + 8$	148	43	15	29	64	43	134
$E(x) = 7x + 8(mod\ 26)$	18	17	15	3	12	17	4

2. The number sequence is 18, 17, 15, 3, 12,17, 4.
3. $n = 7$. Consider of a polynomial $p(t)$ of degree 6 as
$$p(t) = 18 + 17t + 15t^2 + 3t^3 + 12t^4 + 17t^5 + 4t^6$$
4. Take Yang transform for $p(t)$.
$$Y[p(t)] = T(u) = Y[18 + 17t + 15t^2 + 3t^3 + 12t^4 + 17t^5 + 4t^6]$$
$$= 18Y[1] + 17Y[t] + 15Y[t^2] + 3Y[t^3] + 12Y[t^4] + 17Y[t^5] + 4Y[t^6]$$
$$= 18u + 17u^2 + 15 \times 2!\ u^3 + 3 \times 3!\, u^4 + 12 \times 4!\, u^5 + 17 \times 5!\, u^6 + 4 \times 6!\, u^7$$
$$= 18u + 17u^2 + 30\, u^3 + 18u^4 + 288u^5 + 2040u^6 + 2880u^7$$
5. The coefficients of $T(u)$ are considered as
$$q_1 = 18, q_2 = 17, q_3 = 30, q_4 = 18, q_5 = 288,\ q_6 = 2040, q_7 = 2880$$
6. Apply $q_i = 26c_i + r_i$ for each i, we get the sequence $c_1, c_2, \dots, c_7$as 0, 0, 1, 0, 11, 78, 110 and $r_1, r_2, \dots, r_7$ as 18, 17, 4, 18, 2, 12, 20.
7. Therefore the cipher text corresponding to the given plain text is RQDRBLT

3.3.2 Decryption

Consider the cipher text RQDRBLT with the keys 0, 0, 1, 0, 11, 78, 110.

1. The number sequence corresponding to the cipher text is 18, 17, 4, 18, 2, 12, 20.
2. Therefore,
$$q_1 = 18, q_2 = 17, q_3 = 30, q_4 = 18, q_5 = 288,\ q_6 = 2040, q_7 = 2880$$
3. Consider $T(u) = \sum_{i=1}^{n} q_i\, u^i = 18u + 17u^2 + 30\, u^3 + 18u^4 + 288u^5 + 2040u^6 + 2880u^7$
4. Take the inverse Yang transform of $T(u)$ we get
$$p(t) = 18 + 17t + 30\ \frac{t^2}{2!} + 18\frac{t^3}{3!} + 288\frac{t^4}{4!} + 2040\frac{t^5}{5!} + 2880\frac{t^6}{6!}$$
$$= 18 + 17t + 15t^2 + 3t^3 + 12t^4 + 17t^5 + 4t^6$$
5. The number sequence is 18, 17, 15, 3, 12,17, 4.

y	18	17	15	3	12	17	4
$D(y) = 15(y - 8)\ \ (mod\ 26)$	20	5	1	3	8	5	18
Corresponding alphabet	T	E	A	C	H	E	R

6. Thus the plain text is TEACHER

4. CONCLUSION

In this paper, we have introduced an encryption and decryption algorithm based on a new integral transform Yang transform with affine cipher and congruence modulo. The results are verified.

REFERENCES

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

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

[3] Johannes A. Buchmann."Introduction to Cryptography," Fourth Edn., Indian Reprint, Springer, 2009.

[4] Yang Xiao-Jun., "A New Integral Transform Method For Solving Steady Heat-Transfer Problem," *Thermal Science*, vol. 20, Suppl. 3, pp. S639-S642, 2016.