The Libyan Journal of Science

The Libyan Journal of Science- University of Tripoli Vol. 25, No. 02 (2022) 35-39

New method for cryptography using abaoub- shkheam transform

Asmaa O. Mubayrash[1*], Huda M. Khalat[1]

[1] *University of Sabratha, Faculty of Science, Sabratha /Libya*

Corresponding author: Asmaa O. Mubayrash asmaomar339@gmail.com

ARTICLE INFO

Article history:

Received 10/09/2022

Received in revised form 07/12/2022

Accepted 10/12/2022

ABSTRACT

Cryptography is very useful in a communication system for authentication and privacy. It affects many activities in our life. In this paper, we developed a new technique for cryptography using Abaoub- Shkheam transforms. Further, we apply the method of iteration for better security In this work, the Abaoub-Shkheam transform has been used as a part of a symmetric key system, by implementing a practical example in encryption and decryption; Abaoub-Shkheam transform has proven its capability to be invested in cryptography and in the data security field in general.

Keywords: Abaoub- Shkheam transform; Cryptosystem; Encryption; Decryption.

1. Introduction

Cryptography is the science of concealing information through the use of mathematics. Cryptography enables us to store sensitive information or transmit it over insecure networks (such as the internet) so that it can only be read by the intended recipient. Encryption is the process of converting readable data (called plaintext) into a form that hides its content (called cipher text). Decryption is the inverse process, in which cipher text is converted back into plaintext.Cryptography is a critical technique for securing message transmission and data protection. And is a discipline concerned with communication confidentiality. Historically, it has been used to provide secure between individuals. Several encryption algorithms were designed using the dynamics presented by Laplace transform[1,2], and many integral transforms, such as Mahgoub[3], Aboodh[4], and EL-zaki transforms [5].many others, have been used to construct cryptosystems.

The plaintext is transformed into some numerical form by most cryptographic methods that use integral transforms.

The integral transforms were widely used, as was a new integral transform known as the (Abaoub-Shkheam –transform) [6]. This transform can solve various types of integral and differential equations, and

it competes with other well-known transforms such as the Sumudu and Yang Transforms.

2. Abaoub- Shkheam Transform "Q – Transform"

Definition 1.2

Let $f(t)$ be a function defined for all $t \geq 0$, the Q-transform of $f(t)$ is the function $T(u,s)$ defined by

$$T(u,s) = Q[f] = \int_0^{\infty} f(ut)\, e^{-\frac{t}{s}}\, dt \qquad (1)$$

provided that the integral exists for some s, where $s \in (-t_1, t_2)$.

The original function $f(t)$ in Equation (1) is called the inverse transform or inverse of $T(u,s)$, and is denoted by $f(t) = Q^{-1}\{T(u,s)\}$.

If we substitute $ut = y$, then Equation (1) becomes,

$$Q[f(t)] = T(u,s) = \frac{1}{u}\int_0^{\infty} f(y)\, e^{-\frac{1}{us}y}\, dy \qquad (2)$$

2.2. Laplace-Q duality property

If the Laplace transform of the function $f(t)$ is $F(s)$, then

$$F(s) = \mathcal{L}\{f(t)\} = \int_0^{\infty} f(t)\, e^{-st}\, dt \qquad (3)$$

substitute $t = uy$ in the integral on right hand side we get

$$F(s) = \mathcal{L}\{f(t)\} = u\int_0^{\infty} f(uy)\, e^{-suy}\, dy$$

hence, from Equation (2) we get

$$F(s) = u\, T\left(u, \frac{1}{us}\right) \qquad (4)$$

also, from Equations (1) and (3) we get

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

the Equations (4) and (5) form the duality relation between these two transforms and may serve as a means to get one from the other when needed [7].

2.3. Abaoub-Shkheam transform for some basic functions

Elementary functions include algebraic and transcendental functions.

1. $Q[1] = s$.
2. $Q[t^n] = n!\, u^n s^{n+1}, s > 0, n \in \mathbb{N} \cup \{0\}$.
3. $Q[e^{at}] = \frac{s}{1-a\,u\,s}$ where $\frac{1}{s} > au$.
4. $Q\{\sin at\} = \frac{au\,s^2}{1+a^2u^2s^2}$ where $\frac{1}{s} > au$.
5. $Q\{\cos at\} = \frac{s}{1+a^2u^2s^2}$ where $\frac{1}{s} > au$.
6. $Q^{-1}\{u^n s^{n+1}\} = \frac{t^n}{n!}$.
7. $Q^{-1}\left\{\frac{au\,s^2}{1+a^2u^2s^2}\right\} = \sin at$.
8. $Q^{-1}\left\{\frac{s}{1+a^2u^2s^2}\right\} = \cos at$.
9. $Q^{-1}\left\{\frac{s}{1-a\,u\,s}\right\} = e^{at}$.

2.4. Some properties of Abaoub-Shkheam transform.

In this part, we present some properties of the Abaoub-Shkheam transform.

i. $Q\{a\,f(t) + b\,g(t)\} = aQ\{f(t)\} + bQ\{g(t)\}$, where a and b are constants.
ii. If $Q\{f(t)\} = T(s,u)$, then $Q\{f(at)\} = \frac{1}{a}T\left(\frac{s}{a}, u\right)$.
iii. $Q\{f^{(n)}(t)\} = \frac{Q\{f(t)\}}{u^n s^n} - \frac{1}{u}\sum_{k=0}^{n-1}\frac{f^{(k)}(0)}{(us)^{n-k-1}}$.
iv. $Q\{f(t) * g(t)\} = u[Q\{f(t)\}Q\{g(t)\}]$.

3. The proposed cryptographic methodology

The following are some common terms associated with the Cryptography process [8]:

a. *Plain text:* is a message or text that is understandable by the sender, receiver, and anyone else who has access to it
b. *Cipher text:* is a message that is created when a plain text message is codified using a specific scheme or algorithm.
c. *Encryption:* Encryption converts plain text messages to a cipher text.

• *Decryption:*. decryption converts a cipher text back to a plaintext.

The following are included in the proposed cryptographic methodology:

1. Before beginning the encryption process, the sender and receiver must agree on a key.
2. The plain text message is organized as a finite sequence of numbers based on the above conversion, and the most ASCII code so natural numbering in Table .1 below.
3. Take Abaoub-Shkheam transform of a polynomial.
4. Find the remainders g_n such that $g_n \equiv K'_n \; mod 26$, where $\forall n = 0,1,2,3, ...$
5. The ASCII values of remainders will be the Encrypted message.
6. Find the key c_n such that $c_n = \frac{g_n - K'_n}{26} \; for\ all\ n = 0,1,2,3, ...$

Table 1. Data included in the proposed cryptographic methodology

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**
0	1	2	3	4	5	6	7	8
J	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**
9	10	11	12	13	14	15	16	17
S	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	
18	19	20	21	22	23	24	25	

3.1. Encryption example

The following example will be used to clarify the encryption algorithm of the proposed cryptographic mathematical model.

Let the plaintext that must be sent over the unsecured channel be: **YASMEEN**.

The number of the letters in the plaintext (plaintext length), $N = 7$.
We consider the standard expansion

$$sinrx = rx - \frac{r^3x^3}{3!} + \frac{r^5x^5}{5!} - \frac{r^7x^7}{7!} + \frac{r^9x^9}{9!} - \cdots = \sum_{n=0}^{\infty} \frac{(-1)^n (rx)^{2n+1}}{(2n+1)!}$$

where r is a constant, and so

$$xsinrx = rx^2 - \frac{r^3x^4}{3!} + \frac{r^5x^6}{5!} - \frac{r^7x^8}{7!} + \frac{r^9x^{10}}{9!} - \cdots = \sum_{n=0}^{\infty} \frac{(-1)^n (r)^{2n+1}(x)^{2n+2}}{(2n+1)!}$$

where r is a constant.

We allocated 0 to A and 1 to B then Z will be 25.

the given message (plaintext) is 'YASMEEN' it is equivalent to

Y A S M E E N

24 0 18 12 4 4 13

Let $K_0 = 24, K_1 = 0, K_2 = 18, K_3 = 12, K_4 = 4, K_5 = 4, K_6 = 13, K_n = 0, \forall n \geq 7$

We assume $r = 1$

$$f(x) = Kx(sinx) = x\left[K_0 x - K_1 \frac{x^3}{3!} + K_2 \frac{x^5}{5!} - K_3 \frac{x^7}{7!} + K_4 \frac{x^9}{9!} - K_5 \frac{x^{11}}{11!} + K_6 \frac{x^{13}}{13!}\right]$$

$$= 24x^2 - 0\frac{x^4}{3!} + 18\frac{x^6}{5!} - 12\frac{x^8}{7!} + 4\frac{x^{10}}{9!} - 4\frac{x^{12}}{11!} + 13\frac{x^{14}}{13!}$$

$$= \sum_{n=0}^{\infty} \frac{(-1)^n K_n (x)^{2n+2}}{(2n+1)!}$$

Using the Abaoub-Shkheam transform on both sides, we have

$$Q[f(x)] = Q[Kx(sinrx)] =$$

$$= 24Q[x^2] - \frac{0}{3!}Q[x^4] + \frac{18}{5!}Q[x^6] - \frac{12}{7!}Q[x^8] + \frac{4}{9!}Q[x^{10}] - \frac{4}{11!}Q[x^{12}] + \frac{13}{13!}Q[x^{14}]$$

$$= 242!\,u^2s^3 - 0\frac{4!\,u^4s^5}{3!} + 18\frac{6!\,u^6s^7}{5!} - 12\frac{8!\,u^8s^9}{7!} + 4\frac{10!\,u^{10}s^{11}}{9!} - 4\frac{12!\,u^{12}s^{13}}{11!} + 13\frac{14!\,u^{14}s^{15}}{13!}$$

$$= 48u^2s^3 - 0u^4s^5 + 108u^6s^7 - 96u^8s^9 + 40u^{10}s^{11} - 48u^{12}s^{13} + 182u^{14}s^{15}$$

Now Let us assume that

$$g_0 = 48, g_1 = 0, g_2 = 108, g_3 = -96, g_4 = 40, g_5 = -48, g_6 = 182$$

and we will obtain K'such that

$g_n \equiv K'_n mod 26$ as follows $g_n = 26c_n + K'_n \; \forall\, n = 0,1,2,3, \ldots$

$48 = 26(1) + 22$ That is $48 = 22 mod 26$

$0 = 26(0) + 0$ That is $0 = 0 mod 26$

$108 = 26(4) + 4$ That is $108 = 4 mod 26$

$-96 = 26(-4) + 8$ That is $96 = 8 mod 26$

$40 = 26(1) + 14$ That is $40 = 14 mod 26$

$-48 = 26(-2) + 4$ That is $48 = 4 mod 26$

182=26(7)+0 That is $182 = 0 mod 26$

Let $K'_0 = 22, K'_1 = 0, K'_2 = 4, K'_3 = 8, K'_4 = 14, K'_5 = 4, K'_6 = 0, K'_n = 0 \;\; \forall n \geq 7$

Hence the messages YASMEEN' get converted to WAEIOEA.

3.2.Decryption Process

This procedure is carried out at the receiver's end, where the received data is decrypted (convert back into its readable form).

1. Consider the cipher text and key received from the sender.
2. Convert the given cipher text to the corresponding finite sequence of numbers in ASCII form and select it $K'_n \;\; \forall\, n = 0,1,2,3, \ldots$
3. Use given Me keys $c_n \forall\, n = 0,1,2,3, \ldots$ and assuming $g_n = 26c_n + K'_n \;\; \forall\, n = 0,1,2,3, \ldots$
4. Apply the inverse Abaoub-Shkheam transform to $(sinrx)$.
5. After converting the numbers in the preceding finite sequence to alphabets (ASCII values), the original plain text is obtained in Table .2.

Table 2. Date obtained after decryption process

n	K_n	g_n	c_n	$K'_n = g_n - 26c_n$
0	24	48	1	22
1	0	0	0	0
2	18	108	4	4
3	12	-96	-4	8
4	4	40	1	14
5	4	-48	-2	4
6	13	182	7	0

We can generalize the result on encryption and decryption given below based on the above table2.

3.3. Decryption

We have received a message as 'WAEIOEA' which is equivalent to 22 0 4 8 14 4 0

Let $K'_0 = 22, K'_1 = 0, K'_2 = 4, K'_3 = 8, K'_4 = 14, K'_5 = 4, K'_6 = 0, K'_n = 0 \;\; \forall n \geq 7$

Using given key c_n with $c_n = \frac{g_n - K'_n}{26} \;\; for\; n = 0,1,2,3, \ldots$

Hence $c_0 = 1, c_1 = 0, c_2 = 4, c_3 = -4, c_4 = 1, c_5 = -2, c_6 = 7$

and assuming $g_n = 26c_n + K'_n \; \forall\, n = 0,1,2,3, \ldots$ we get

$$g_0 = 48, g_1 = 0, g_2 = 108, g_3 = -96, g_4 = 40, g_5 = -48, g_6 = 182$$

Now we consider

$$Q[Kx(sinrx)] = 48u^2s^3 - 0u^4s^5 + 108u^6s^7 - 96u^8s^9 + 40u^{10}s^{11} - 48u^{12}s^{13} + 182u^{14}s^{15} = \sum_{n=0}^{\infty}(-1)^n g_n u^n s^{n+1}$$

Taking the inverse Abaoub-Shkheam transform of a polynomial we get

$$f(x) = Kx(sinx)$$
$$= 24x^2 - 0\frac{x^4}{3!} + 18\frac{x^6}{5!} - 12\frac{x^8}{7!} + 4\frac{x^{10}}{9!} - 4\frac{x^{12}}{11!} + 13\frac{x^{14}}{13!}$$

Here we have

$$K_0 = 24, K_1 = 0, K_2 = 18, K_3 = 12, K_4 = 4, K_5 = 4, K_6 = 13 K_n = 0, \forall n \geq 7$$

Now, convert the numbers of the above finite sequence to alphabets (ASCII values), and the original plain text is obtained as the YASMEEN.

Then 24 0 18 12 4 4 13 is equivalent to **YASMEEN**.

3.4. Generaliztion

For encryption of a given message in terms of $K_n$we consider $f(x) = Kx(sinx)$. Taking the Abaoub-Shkheam transform and we following the procedure discussed in section3 **,**then we can convert K_n to K'_n.Where $K'_n = (-1)^n K_n (r)^{2n+1}(2n+2)\ mod 26$
And $g_n = (-1)^n K_n (r)^{2n+1}(2n+2)\ \forall n =$ 0,1,2,3, ...

with the key given by $c_n = \frac{g_n - K'_n}{26}$ $for\ n =$ 0,1,2,3, ...

For decryption of received message in terms of K'_n we consider

$$K\left[\frac{u\,s^2}{1+u^2s^2}\right] = \sum_{n=0}^{\infty}(-1)^n g_n u^n s^{n+1}$$

Taking the inverse Abaoub-Shkheam transform and using the procedure discussed in section 3, we can convert K'_n to K_n. Where the $K_n = (-1)^n \frac{26c_n + K'_n}{(r)^{2n+1}(2n+2)}$, $n = 0,1,2, \ldots$

From the numbers K_n we find the original message.

4. Conclusion

The proposed work introduces a new cryptographic scheme based on Abaoub-Shkheam transforms, with the key being the number of multiples of mod n. As a result, tracing the key with an eyedropper is extremely difficult. Section 4 results provide as many transformations as required, which are the most useful factor for changing the key.

5. References

1. G. Naga Lakshmi, Ravi Kumar B. and Chandra Sekhar A**. (**2011**).** A cryptographic scheme of Laplace transforms, International Journal of Mathematical Archive-2(12),, 2515-2519.
2. Hiwarekar A.P. (2012). A new method of cryptography using Laplace transform, International Journal of Mathematical Archive, 3(3), 1193-1197.
3. Kumar P. Senthil, Vasuki S. (2018): An Application of MAHGOUB Transform in Cryptography, Advances in Theoretical and Applied Mathematics, ISSN 0973-4554, Volume 13, Number 2, pp. 91-99.
4. Abdelilah K. Hassan Sedeeg, Mohand M. Abdelrahim Mahgoub, Muneer A. Saif Saeed, (2016). An Application of the New Integral "Aboodh Transform" in Cryptography, Int J Pure Appl Math, 5 (5), 151-154.
5. Uttam Dattu Kharde., 2017, "An Application of the Elzaki Transform in Cryptography", Journal for Advanced Research in Applied Sciences, 4(5), pp. 86 – 89.
6. A. Abaoub, and A. Shkheam,(2020). The New Integral Transform "Abaoub-Shkheam transform", Iaetsd journal for advanced research in applied science**.**
7. A.P. Hiwarekar(2013). A new method of Cryptography using Laplace transform of Hyperbolic function, International Journal of Mathematical archive, ,4(2),pp.206-213.
8. JadhavShailaShivaji, Hiwarekar A.P. (2021*).* New Method for Cryptography using Laplace-Elzaki Transform, PSYCHOLOGY AND EDUCATION (2021) 58(5), ISSN 1553 – 6939.
9. Eman A. Mansour, Emad A. Kuffi, Sadiq A. Mehdi, (2021). The new integral transform "SEE transform" and its applications, Period. Eng. Nat. Sci., 9 (2), 1016-1029