http://www.newtheory.org **ISSN: 2149-1402**

Journal of New Theory

Received: 28.06.2016 *Year*:**2017**, *Number*: **16**, *Pages*: **59-67**
Published: 12.10.2017 *Original Article*

APPLICATION OF NATURAL TRANSFORM IN CRYPTOGRAPHY

Anil Dhondiram Chindhe[1,*] <anilchindhe5@gmail.com>
Sakharam Kiwne[2] <sbkdcamath@gamil.com>

[1]Department of Mathematics, Balbhim College, Beed, Maharashtra, India
[2]Department of Mathematics, Deogiri College, Aurangabad, Maharashtra, India

Abstaract — The newly defined integral transform "Natural transform" has many application in the field of science and engineering.In this paper we described the application of Natural transform to Cryptography.This provide the algorithm for cryptography in which we use the natural transform of the exponential function for encryption of the plain text and corresponding inverse natural transform for decryption.

Keywords — *Cryptography, Data encryption, Data decryption, Natural transform.*

1 Introduction

In today's world of globalization and digitalization , the security of information (data) is the most important aspect of the society.There is a commonly and widely used technique called as cryptography for the security purpose.cryptography deals with the actual securing of digital data.It is the art and science of making a cryptosystem that is capable of providing information security. The objectives of cryptography are Confidentiality,Integrity,Non-repudiation and Authentication.Different tools and techniques are used for cryptography [12, 13, 14]. There are Mathematical technique used for the cryptography are found in [8, 9, 10].

The original information is known as plain-text, and the encrypted from as cipher text. The cipher text message contains all the information of the plain-text message,but is not in a format readable to a human or computer without the mechanism to decrypt it. Cipher are usually parametrized by a piece of auxiliary information called a key. The encryption process is varied depending the key which changes the detailed operation of the algorithm [11]. Without having the proper key it is impossible to decrypt the given text.

[*] *Corresponding Author.*

1.1 Natural Transform

The new integral transform Natural transform was defined by Khan and Khan [1] as N - transform who gave the properties and application of N-transform. Belgacem [2, 3] defined inverse Natural transform and studied some properties and applications. Many authors have contributed in the study of N-transform [4, 5, 6, 7]. Natural transform can be used to solve the problems in engineering, fluid mechanics and other science faculty.

1.2 Definition of Natural Transform

The Natural transform of the function $f(t) \in \Re^2$ is given by the following integral equation [3]

$$\mathbb{N}[f(t)] = G(s,u) = \int_0^\infty e^{-st} f(ut)dt \tag{1}$$

where $Re(s) > 0$, u $\in (\tau_1, \tau_2)$ provided the function $f(t) \in \Re^2$ is defined in the set

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

The inverse Natural transform related with Bromwich contour integral[2, 3] is defined by

$$\mathbb{N}^{-1}[G(s,u)] = f(t) = \lim_{T\to\infty} \frac{1}{2\Pi i} \int_{\gamma-iT}^{\gamma+iT} e^{\frac{st}{u}} G(s,u)ds \tag{2}$$

1.3 Standard Result of Natural Transform

In this section we can see the Natural transform of some of the standard functions. [1, 3]

$$\mathbb{N}[1] = \frac{1}{s} \tag{3}$$

$$\mathbb{N}[t] = \frac{u}{s^2} \tag{4}$$

$$\mathbb{N}[t^n] = \frac{u^n}{s^{n+1}} n! \tag{5}$$

$$\mathbb{N}[e^{at}] = \frac{1}{s-au} \tag{6}$$

$$\mathbb{N}[\frac{sin(at)}{a}] = \frac{u}{s^2+s^2u^2} \tag{7}$$

$$\mathbb{N}[cos(at)] = \frac{s}{s^2+s^2u^2} \tag{8}$$

$$\mathbb{N}[\frac{t^{n-1}e^{at}}{(n-1)!}] = \frac{u^{n-1}}{(s-au)^2} \tag{9}$$

$$\mathbb{N}[f^{(n)}(t)] = \frac{s^n}{u^n}.R(s,u) - \sum_{n=0}^{\infty} \frac{s^{n-(k+1)}}{u^{n-k}}.u^{(k)}(0), \quad \text{where} f^{(n)}(t) = \frac{\mathrm{d}^n f}{\mathrm{d}t^n} \tag{10}$$

2 Main Result

2.1 Encryption Using Exponential Function

Consider the Taylor series expansion of the exponential function e^{rt} as

$$e^{rt} = 1 + \frac{rt}{1!} + \frac{(rt)^2}{2!}..... = \sum_{n=0}^{\infty} \frac{(rt)^n}{n!} \tag{11}$$

where r is constant.

$$\therefore t.e^{rt} = t + \frac{rt^2}{1!} + \frac{r^2t^3}{2!}..... = \sum_{n=0}^{\infty} \frac{r^n t^{n+1}}{n!} \tag{12}$$

Now we allocate 0 to A,1 to B and so on then Z will be 25.

consider the plain-text as "SCIENCE" which is equivalent to 18 2 8 4 13 2 4

Put$P_0 = 18, P_1 = 2, P_2 = 8, P_3 = 4, P_4 = 13, P_5 = 2, P_6 = 4, P_n = 0$ for n≥7

$$f(t) = Pt.e^{rt} = P_0t + P_1\frac{rt^2}{1!} + P_2\frac{r^2t^3}{2!} + P_3\frac{r^3t^4}{3!}..... = \sum_{n=0}^{\infty} P_n\frac{r^n t^{n+1}}{n!} \tag{13}$$

for r = 2 we have

$$f(t) = Pt.e^{2t} = P_0t + P_1\frac{2t^2}{1!} + P_2\frac{2^2t^3}{2!} + P_3\frac{2^3t^4}{3!}..... = \sum_{n=0}^{\infty} P_n\frac{2^n t^{n+1}}{n!} \tag{14}$$

$$f(t) = Pt.e^{2t} = 18t + 2\frac{2t^2}{1!} + 8\frac{2^2t^3}{2!} + 4\frac{2^3t^4}{3!} + 13\frac{2^4t^5}{4!} + 2\frac{2^5t^6}{5!} + 4\frac{2^6t^7}{6!} \tag{15}$$

Now taking the Natural transform on both sides of above equation, we get

$$\begin{aligned}
&\mathbb{N}[f(t)] = \\
&= \mathbb{N}[Pt.e^{2t}] \\
&= \mathbb{N}[18t + 2\frac{2t^2}{1!} + 8\frac{2^2t^3}{2!} + 4\frac{2^3t^4}{3!} + 13\frac{2^4t^5}{4!} + 2\frac{2^5t^6}{5!} + 4\frac{2^6t^7}{6!}] \\
&= 18.\mathbb{N}[t] + 2.\frac{2}{1!}\mathbb{N}[t^2] + 8.\frac{2^2}{2!}\mathbb{N}[t^3] + 4.\frac{2^3}{3!}\mathbb{N}[t^4] + 13.\frac{2^4}{4!}\mathbb{N}[t^5] + 2.\frac{2^5}{5!}\mathbb{N}[t^6] + 4.\frac{2^6}{6!}\mathbb{N}[t^7] \\
&= 18.\frac{u}{s^2} + 2.\frac{2}{1!}\frac{u^2}{s^3}2! + 8.\frac{2^2}{2!}\frac{u^3}{s^4}3! + 4.\frac{2^3}{3!}\frac{u^4}{s^5}4! + 13.\frac{2^4}{4!}\frac{u^5}{s^6}5! + 2.\frac{2^5}{5!}\frac{u^6}{s^7}6! + 4.\frac{2^6}{6!}\frac{u^7}{s^8}7! \\
&= 18.\frac{u}{s^2} + 8.\frac{u^2}{s^3} + 96.\frac{u^3}{s^4} + 128.\frac{u^4}{s^5} + 1040.\frac{u^5}{s^6} + 384.\frac{u^6}{s^7} + 1792.\frac{u^7}{s^8}
\end{aligned}$$

Now the key (K_i) for the cipher text is calculated by following method

$18 \equiv 18(mod26)$,$8 \equiv 8(mod26)$,$96 \equiv 18(mod26)$,$128 \equiv 24(mod26)$,

$1040 \equiv 0(mod26)$,$384 \equiv 20(mod26)$,$1792 \equiv 24(mod26)$.

Which gives the key as 0 0 3 4 40 14 68.

Let $P_i^{'} = r_i = q_i - 26K_i$ for i = 0,1,2,3,4,5,6

$\therefore P_0^{'} = 18, P_1^{'} = 8, P_2^{'} = 18, P_3^{'} = 24, P_4^{'} = 0, P_5^{'} = 20, P_6^{'} = 24, P_n^{'} = 0$ for $n \geq 7$

Hence the given plain-text "SCIENCE" get converted into "SISYAUY".

2.2 For Decryption

Now receiver receives the message as "SISYAUY" which is equivalent to 18 8 24 0 20 24

$Since P_0^{'} = 18, P_1^{'} = 8, P_2^{'} = 18, P_3^{'} = 24, P_4^{'} = 0, P_5^{'} = 20, P_6^{'} = 24, P_n^{'} = 0 \quad forn \geq 7$

and we have the key as 0 0 3 4 40 14 68 so we can calculate $q_i = 26K_i + P_i^{'}$ for i = 0,1,2...

$$P\frac{u}{(s-2u)^2} = 18.\frac{u}{s^2} + 8.\frac{u^2}{s^3} + 96.\frac{u^3}{s^4} + 128.\frac{u^4}{s^5} + 1040.\frac{u^5}{s^6} + 384.\frac{u^6}{s^7} + 1792.\frac{u^7}{s^8} \quad (16)$$

Now taking inverse Natural transform on both sides

$$\mathbb{N}^{-1}[P\tfrac{u}{(s-2u)^2}] = \mathbb{N}^{-1}[18.\tfrac{u}{s^2} + 8.\tfrac{u^2}{s^3} + 96.\tfrac{u^3}{s^4} + 128.\tfrac{u^4}{s^5} + 1040.\tfrac{u^5}{s^6} + 384.\tfrac{u^6}{s^7} + 1792.\tfrac{u^7}{s^8}]$$

$$\begin{aligned} f(t) &= Pte^{2t} \\ &= 18\mathbb{N}^{-1}[\frac{u}{s^2}] + 8\mathbb{N}^{-1}[\frac{u^2}{s^3}] + 96\mathbb{N}^{-1}[\frac{u^3}{s^4}] + 128\mathbb{N}^{-1}[\frac{u^4}{s^5}] + 1040\mathbb{N}^{-1}[\frac{u^5}{s^6}] \\ &+ 384\mathbb{N}^{-1}[\frac{u^6}{s^7}] + 1792\mathbb{N}^{-1}[\frac{u^7}{s^8}] \\ &= 18t + 2\frac{2t^2}{1!} + 8\frac{2^2t^3}{2!} + 4\frac{2^3t^4}{3!} + 13\frac{2^4t^5}{4!} + 2\frac{2^5t^6}{5!} + 4\frac{2^6t^7}{6!} \end{aligned}$$

Here $P_0 = 18, P_1 = 2, P_2 = 8, P_3 = 4, P_4 = 13, P_5 = 2, P_6 = 4, P_n = 0 \quad$ for $n \geq 7$

This gives the message "SISYAUY" get converted into the original message "SCIENCE".

2.2.1 More Illustrative Examples

1 The original message "SCIENCE" get converted into "SMIQNEC" with the proper key as

0 0 8 202 112 785 for r = 3

2 The original message "SCIENCE" get converted into "SGUKAQC" with the proper key as

0 1 14 39 640 472 4411 for r = 4

3 The original message "SCIENCE" get converted into "SEYQAMC" with the proper key as

0 2 180 1688 96040 248226 8108731 for r = 14

3 Encryption Using Hyperbolic Function

Consider the Taylor series expansion of hyperbolic sine function sinh(rt) as

$$sinh(rt) = \frac{rt}{1!} + \frac{r^3t^3}{3!} + \frac{r^5t^5}{5!}..... = \sum_{n=0}^{\infty} \frac{(rt)^{2n+1}}{(2n+1)!} \tag{17}$$

where r is constant.

$$\therefore t.sinh(rt) = \frac{rt^2}{1!} + \frac{r^3t^4}{3!} + \frac{r^5t^6}{5!}..... = \sum_{n=0}^{\infty} \frac{r^{2n+1}t^{2n+2}}{(2n+1)!} \tag{18}$$

Now we allocate 0 to A,1 to B and so on then Z will be 25.

consider the plain-text as "STUDENT" which is equivalent to 18 19 20 3 4 13 19

Put$P_0 = 18, P_1 = 19, P_2 = 20, P_3 = 3, P_4 = 4, P_5 = 13, P_6 = 19, P_n = 0$ for n≥7

$$f(t) = Pt.sinh(rt) = P_0\frac{rt^2}{1!} + P_1\frac{r^3t^4}{3!} + P_2\frac{r^5t^6}{5!} + ... = \sum_{n=0}^{\infty} P_n\frac{r^{2n+1}t^{2n+2}}{(2n+1)!} \tag{19}$$

for r = 2 we have

$$f(t) = Pt.sinh(2t) = P_0\frac{2t^2}{1!} + P_1\frac{2^3t^4}{3!} + P_2\frac{2^5t^6}{5!} + ... = \sum_{n=0}^{\infty} P_n\frac{2^{2n+1}t^{2n+2}}{(2n+1)!} \tag{20}$$

$$f(t) = Pt.sinh(2t) = 18\frac{2t^2}{1!} + 19\frac{2^3t^4}{3!} + 20\frac{2^5t^6}{5!} + 3\frac{2^7t^8}{7!} + 4\frac{2^9t^{10}}{9!} + 13\frac{2^{11}t^{12}}{11!} + 19\frac{2^{13}t^{14}}{13!} \tag{21}$$

Now taking the Natural transform on both sides of above equation ,we get

$$\begin{aligned}
\mathbb{N}[f(t)] &= \mathbb{N}[Pt.sinh(2t)] \\
&= P\frac{(2s)(2u^2)}{(s^2-2^2u^2)^2} \\
&= \mathbb{N}[18\frac{2t^2}{1!}+19\frac{2^3t^4}{3!}+20\frac{2^5t^6}{5!}+3\frac{2^7t^8}{7!} \\
&+4\frac{2^9t^{10}}{9!}+13\frac{2^{11}t^{12}}{11!}+19\frac{2^{13}t^{14}}{13!}] \\
&= 18\frac{2}{1!}\mathbb{N}[t^2]+19\frac{2^3t^4}{3!}\mathbb{N}[t^4]+20\frac{2^5}{5!}\mathbb{N}[t^6]+3\frac{2^7}{7!}\mathbb{N}[t^8]+4\frac{2^9}{9!}\mathbb{N}[t^{10}] \\
&+13\frac{2^{11}}{11!}\mathbb{N}[t^{12}]+19\frac{2^{13}}{13!\mathbb{N}[t^{14}]} \\
&= 72.\frac{u^2}{s^3}+608.\frac{u^4}{s^5}+3840.\frac{u^6}{s^7}+3072.\frac{u^8}{s^9}+.20480\frac{u^{10}}{s^{11}}+319488.\frac{u^{12}}{s^{13}} \\
&+2179072.\frac{u^{14}}{s^{15}}
\end{aligned}$$

Now the key(K_i) for the cipher text is calculated by following method

$72 \equiv 20(mod26), 608 \equiv 10(mod26), 3840 \equiv 18(mod26), 3072 \equiv 4(mod26)$

$20480 \equiv 18(mod26), 319488 \equiv 0(mod26), 2179072 \equiv 12(mod26).$

Which gives the key as 2 23 147 118 787 12288 83810.

Let $P_i^{'} = r_i = q_i - 26K_i$ for i = 0,1,2,3,4,5,6

$\therefore P_0^{'} = 20, P_1^{'} = 10, P_2^{'} = 18, P_3^{'} = 4, P_4^{'} = 18, P_5^{'} = 0, P_6^{'} = 12, P_n^{'} = 0$ for $n \geq 7$

Hence the given plain-text " STUDENT " get converted into " UKSESAM ".

3.1 For Decryption

Now receiver receives the message as " UKSESAM " which is equivalent to 20 10 18 4 18 0 12

Since $P_0^{'} = 20, P_1^{'} = 10, P_2^{'} = 18, P_3^{'} = 4, P_4^{'} = 18, P_5^{'} = 0, P_6^{'} = 12, P_n^{'} = 0$ for $n \geq 7$ and we have the key as 2 23 147 118 787 12288 83810 so we can calculate $q_i = 26K_i + P_i^{'}$ for i = 0,1,2...

$$\begin{aligned}
P\frac{(2s)(2u^2)}{(s^2-2^2u^2)^2} &= 72.\frac{u^2}{s^3}+608.\frac{u^4}{s^5}+3840.\frac{u^6}{s^7}+3072.\frac{u^8}{s^9}+.20480\frac{u^{10}}{s^{11}}+319488.\frac{u^{12}}{s^{13}} \\
&+2179072.\frac{u^{14}}{s^{15}}
\end{aligned}$$

Now taking inverse Natural transform on both sides

$$\mathbb{N}^{-1}[P\frac{(2s)(2u^2)}{(s^2-2^2u^2)^2}] = \mathbb{N}^{-1}[72.\frac{u^2}{s^3} + 608.\frac{u^4}{s^5} + 3840.\frac{u^6}{s^7} + 3072.\frac{u^8}{s^9} + 20480\frac{u^{10}}{s^{11}} + 319488.\frac{u^{12}}{s^{13}} + 2179072.\frac{u^{14}}{s^{15}}]$$

$$\begin{aligned} f(t) &= Pt.sinh(2t) \\ &= 72.\mathbb{N}^{-1}[\frac{u^2}{s^3}] + 60.\mathbb{N}^{-1}[\frac{u^4}{s^5}] + 3840.\mathbb{N}^{-1}[\frac{u^6}{s^7}] + 3072.\mathbb{N}^{-1}[\frac{u^8}{s^9}] + 20480.\mathbb{N}^{-1}[\frac{u^{10}}{s^{11}}] \\ &+ 319488.\mathbb{N}^{-1}[\frac{u^{12}}{s^{13}}] + 2179072.\mathbb{N}^{-1}[\frac{u^{14}}{s^{15}}] \\ &= 18\frac{2t^2}{1!} + 19\frac{2^3t^4}{3!} + 20\frac{2^5t^6}{5!} + 3\frac{2^7t^8}{7!} + 4\frac{2^9t^{10}}{9!} + 13\frac{2^{11}t^{12}}{11!} + 19\frac{2^{13}t^{14}}{13!} \end{aligned}$$

Here $P_0 = 18, P_1 = 19, P_2 = 20, P_3 = 3, P_4 = 4, P_5 = 13, P_6 = 19, P_n = 0 \quad forn \geq 7$

This gives the cipher text " UKSESAM " get converted into the original message " STUDENT ".

3.2 Generalization

for encryption of given plain-text in terms of P ,we consider the function

$f(t) = Pt^j sinh(rt) \qquad forr, j \in \mathbb{N}$

Taking Natural transform and following the procedure we can have the given messageP_i can

be converted into $P_i^{'}$ with the private key as $K_i = \frac{q_i - P_i^{'}}{26}$ for i = 0,1,2 ...

where $q_i = P_i r^{2i+1}(2i+1)(2i+3)...(2i+j)$
For dycryption for recived message (cipher text) in terms of P_i we have

$P.u^j.(-\frac{\partial}{\partial s})^j(\frac{ru}{s^2-r^2u^2}) = \sum_{n=0}^{\infty} \frac{q_n u^{2n+1+j}}{s^{2n+2+j}}$

Taking the inverse Natural transform,we can convert the given cipher text $P_i^{'}$ into the original message P_i as

$$P_i = \frac{26K_i + P_i^{'}}{r^{2i+1}(2i+1)(2i+3)...(2i+j)}$$

for i = 0,1,2 ...

4 Conclusion

Now a day's e-crimes such as internet banking fraud, data hacking etc. are commonly seen in the society. This paper gives a new cartographic application using Natural transform which helps to prevent such e-crimes in the society.It is too difficult for hackers or unauthorized person to find the private key by the brute farce attack or any other attack.

References

[1] Z.H.Khan and W.A.Khan.N-transform properties and applications. NUST Jour of Engg Sciences. , 1(1) pp 127–133,2008.

[2] Silambarasan, R. and Belgacem, F. B. M, *Applications of the Natural transform to Maxwell's Equations*, PIERS Suzhou, China,, Sept 12-16, pp 899–902, 2011..

[3] Belgacem, F. B. M and Silambarasan R., *Theory of the Natural transform*, Mathematics in Engg Sci and Aerospace (MESA) journal, Vol. 3, No. 1, pp 99–124,2012..

[4] Silambarasan, R. and Belgacem, F. B. M., *Advances in the Natural transform*, 9th International Conference on Mathematical Problems in Engineering, Aerospace and Sciences AIP Conf. Proc. , 1493, 106–110, 2012.

[5] Loonker Deshna and Banerji P.K., *Natural transform for distribution and Boehmian spaces*, Math.Engg.Sci.Aerospace ,4(1), pp 69–76,2013.

[6] Loonker Deshna and Banerji P.K., *application of Natural transform to differential equations* , J.Inadian Acad Math.,35(1), pp 151–158,2013.

[7] Loonker Deshna and Banerji P.K., *Natural transform and solution of integral equations for distribution spaces* , Amer. J. Math. Sci.,8,2013.

[8] Hiwarekar AP.,*Application of Laplace Transform for Cryptography*,International Journal of engg. sci.Resch.,5(4), 129–135,2015..

[9] Dhanorkar GA, Hiwarekar AP., *A generalized Hill cipher using matrix transformation.*,International J. of Math. Sci. Engg. Appls, 5(IV), 19–23,2011.

[10] Hiwarekar AP., *A new method of cryptography using Laplace transform.*, International Journal of Mathematical Archive., 3(3), 1193–1197.2012.

[11] Hiwarekar AP., *New Mathematical Modeling for Cryptography*, Journal of Information Assurance and Security, MIR Lab USA,9,027–033,2014.

[12] Stallings W, *Cryptography and network security, 4th edition, Prentice Hall, 2005.*

[13] Barr TH, *Invitation to Cryptography, Prentice Hall, 2002.*

[14] Buchmann JA., *Introduction to Cryptography,Fourth Edn., Indian Reprint, Springer, 2009.*