Volume : 2 | Issue : 6 | June 2013 • ISSN No 2277 - 8160

Research Paper | Marine

A Cryptographic Scheme using Infinite Series and Laplace Transform

Sachin Vyavahare BITS, Pilani Off campus center Tolani Maritime Institute, Induri, Pune 410507

Bani Upmanayu BITS, Pilani Off campus center Tolani Maritime Institute, Induri, Pune 410507

ABSTRACT

Abstract: This paper presents different scheme for cryptographic purpose, by combining Infinite series and Laplace transform using ASCII code (128 bit). Encryption is done by using Infinite series and then Laplace transform, arranged in the form of an array with keys at even position. Decryption is done by inverse Laplace transform. The process of creation of public key cipher is also discussed.

KEYWORDS : cryptography, Infinite Series, Laplace Transform, ASCII code.

1. Introduction:

In the modern age of electronic communication, cryptography is the only most important tool that avoids the threat against possible attacks by hackers during transmission process of the message. Encryption is the process of translating information from its original form (called plaintext) into an encoded, incomprehensible form (called cipher text). Decryption refers to the process of taking cipher text and translating it back into plain text. Any type of data may be encrypted, including digitized images and sounds. Cryptography secures information by protecting its confidentiality. Ciphers are usually parameterized by a piece of auxiliary information, called a key. The encrypting procedure varies depending on the key, which changes the detailed operation of the algorithm. Mathematical models play a very important role in cryptography. [1, 2, 3, 4, 5, 9, 10, 11, 13, 14]

1.1 Infinite series:

We will use infinite series in encryption technique, which is of general nature. Infinite series of standard functions like exponential, sine, cosine etc. can be used for encryption purpose. [7, 12]

1.2 Laplace Transformation:

Let f (t) is a function defined for all positive values of t. Then the Laplace transform of f (t), denoted by L [f (t)] or F(s) is defined by $L[f(t)] = F(s) = \int_0^\infty e^{-st} f(t)\,dt$, provided that the integral exists. Here the parameter ' s' is a real or complex number. The above relation can also be written as $f(t) = L^{-1}[F(s)]$. In such a case, the function f (t) is said to be inverse Laplace transform of F (s). The symbol L which transforms f (t) into F (s) can be called the Laplace transform operator. The symbol L^{-1} which transforms F (s) to f (t) can be called the inverse Laplace transform operator. [7, 12]

2. Scheme: In this section we present the scheme for encryption, key generation and decryption. This is based on earlier work by G. Naga Lakshmi, Ravi Kumar B. and Chandra Sekhar A. [4] and Hiwarekar A.P. [8]

2.1 Encryption and Key Generation:

Step I: Convert the given message to its equivalent ASCII number $G_1G_2G_3...G_n$

Step II: Attach these numbers as coefficient to infinite series

$$f(t) = \sum_{n=1}^{\infty} G_n \left(\frac{n+1}{n}\right) \sin nt$$

Step III: Take Laplace transform on the both side then we have

$$F(s) = \sum_{n=1}^{\infty} \frac{Q_n}{s^2 + n^2}$$

Step IV: If $128.K_n + G_n' = Q_n$ i.e. $Q_n = G_n' \bmod 128\ (K_n)$ transform the message in the form $G_1''K_1G_2''K_2G_3''K_3...G_n''K_n$ where G_n'' is ASCII equivalent code of G_n' and K_n is key.

Step V: The sender publically sends the message and privately sends the infinite series $f(t) = \sum_{n=1}^{\infty} \left(\frac{n+1}{n}\right) \sin nt$ and the Laplace expansion.

2.2 Decryption:

Step I: We receive the message in the form $G_1''K_1G_2''K_2G_3''K_3...G_n''K_n$

Step II: Convert ASCII code G_n'' to its equivalent numerical value G_n'

Step III: Using values G_n' and above keys K_n obtain the number Q_n as $128.K_n + G_n' = Q_n$

Step IV: Replace the values of Q_n in the series

$$F(s) = \sum_{n=1}^{\infty} \frac{Q_n}{s^2 + n^2}$$

Step V: Take inverse Laplace transform and rearrange the terms in the form

$$f(t) = \sum_{n=1}^{\infty} G_n \left(\frac{n+1}{n}\right) \sin nt$$

Step VI: From the above series we have $G_1G_2G_3...G_n$ Converting to its equivalent ASCII code we get required message

3. Implementation:

Consider the example

Let the given message be: Do you have 5 guns?

Encryption:

Its equivalent ASCII code is 68 111 32 121 111 117 32 104 97 118 101 32 53 32 103 117 110 115 63.

Let $G_1 = 68, G_2 = 111, G_3 = 32, ..., G_{19} = 63$ and $G_n = 0 \quad n \geq 20$

Therefore $f(t) = \sum_{n=1}^{\infty} G_n \left(\frac{n+1}{n}\right) \sin nt$ becomes

$$f(t) = 68\left(\frac{2}{1}\right)\sin t + 111\left(\frac{3}{2}\right)\sin 2t + 32\left(\frac{4}{3}\right)\sin 3t + 121\left(\frac{5}{4}\right)\sin 4t$$
$$+111\left(\frac{6}{5}\right)\sin 5t + 117\left(\frac{7}{6}\right)\sin 6t + 32\left(\frac{8}{7}\right)\sin 7t + 104\left(\frac{9}{8}\right)\sin 8t + 97\left(\frac{10}{9}\right)\sin 9t$$
$$+118\left(\frac{11}{10}\right)\sin 10t + 101\left(\frac{12}{11}\right)\sin 11t + 32\left(\frac{13}{12}\right)\sin 12t + 53\left(\frac{14}{13}\right)\sin 13t + 32\left(\frac{15}{14}\right)\sin 14t$$
$$+103\left(\frac{16}{15}\right)\sin 15t + 117\left(\frac{17}{16}\right)\sin 16t + 110\left(\frac{18}{17}\right)\sin 17t + 115\left(\frac{19}{18}\right)\sin 18t + 63\left(\frac{20}{19}\right)\sin 19t$$

Taking Laplace transform on both sides we get

$$F(s) = \frac{136}{s^2+1} + \frac{333}{s^2+4} + \frac{128}{s^2+9} + \frac{605}{s^2+16} + \frac{666}{s^2+25} + \frac{819}{s^2+36} + \frac{256}{s^2+49} + \frac{936}{s^2+64} + \frac{970}{s^2+81} + \frac{1298}{s^2+100}$$
$$+\frac{1212}{s^2+121} + \frac{416}{s^2+144} + \frac{742}{s^2+169} + \frac{480}{s^2+196} + \frac{1648}{s^2+225} + \frac{1989}{s^2+256} + \frac{1980}{s^2+289} + \frac{2185}{s^2+324} + \frac{1260}{s^2+361}$$

As 136 = 8 mod 128(1), 333 = 77 mod 128(2) , 128 = 0 mod 128(1), 605 = 93 mod 128(4) ,

666 = 26 mod 128(5), 819 = 51 mod 128(6), 256 = 0 mod 128(2), 936 = 40 mod 128(7),

970 = 74 mod 128(7), 1298 = 18 mod 128(10), 1212 = 60 mod 128(9), 416 = 32 mod 128(3),

742 = 102 mod 128(5), 480 = 96 mod 128(3), 1648 = 112 mod 128(12), 1989 = 69 mod 128(15),

1980 = 60 mod 128(15), 2185 = 9 mod 128(17) and 1260 = 108 mod 128(9).

Let

$G_1' = 8, G_2' = 77, G_3' = 0, G_4' = 93, G_5' = 26, G_6' = 51, G_7' = 0, G_8' = 40, G_9' = 74, G_{10}' = 18, G_{11}' = 60, G_{12}' = 32$
$G_{13}' = 102, G_{14}' = 96, G_{15}' = 112, G_{16}' = 69, G_{17}' = 60, G_{18}' = 9, G_{19}' = 108$ and $G_n' = 0$ for $n \geq 20$.

with keys

$K_1 = 1, K_2 = 2, K_3 = 1, K_4 = 4, K_5 = 5, K_6 = 6, K_7 = 2, K_8 = 7, K_9 = 7, K_{10} = 10, K_{11} = 9, K_{12} = 3,$
$K_{13} = 5, K_{14} = 3, K_{15} = 12, K_{16} = 15, K_{17} = 15, K_{18} = 17, K_{19} = 9$ and $K_n = 0$ for $n \geq 20$.

We convert message in the form $G_1'' K_1 G_2'' K_2 G_3'' K_3 \ldots G_n'' K_n$ where G_n'' is ASCII equivalent code of G_n' and K_n is key. Hence the message encrypted to

BS1M2NUL1]4SUB536NUL2(7J7DC210<9 3f5'3p12E15<15TAB17I9

Decryption:
We have encrypted message as

BS1M2NUL1]4SUB536NUL2(7J7DC210<9 3f5'3p12E15<15TAB17I9

Let

$G_1'' = BS, G_2'' = M, G_3'' = NUL, G_4'' =], G_5'' = SUB, G_6'' = 3, G_7'' = NUL, G_8'' = (, G_9'' = J, G_{10}'' = DC2, G_{11}'' =<, G_{12}'' =$,
$G_{13}'' = f, G_{14}'' =', G_{15}'' = p, G_{16}'' = E, G_{17}'' =<, G_{18}'' = TAB, G_{19}'' = I$ and $G_n'' = 0$ for $n \geq 20$.

with given keys

$K_1 = 1, K_2 = 2, K_3 = 1, K_4 = 4, K_5 = 5, K_6 = 6, K_7 = 2, K_8 = 7, K_9 = 7, K_{10} = 10, K_{11} = 9, K_{12} = 3,$
$K_{13} = 5, K_{14} = 3, K_{15} = 12, K_{16} = 15, K_{17} = 15, K_{18} = 17, K_{19} = 9$ and $K_n = 0$ for $n \geq 20$.

Let we convert ASCII code G_n'' to its equivalent numerical value G_n' as

$G_1' = 8, G_2' = 77, G_3' = 0, G_4' = 93, G_5' = 26, G_6' = 51, G_7' = 0, G_8' = 40, G_9' = 74, G_{10}' = 18, G_{11}' = 60, G_{12}' = 32,$
$G_{13}' = 102, G_{14}' = 96, G_{15}' = 112, G_{16}' = 69, G_{17}' = 60, G_{18}' = 9, G_{19}' = 108$ and $G_n' = 0$ for $n \geq 20$.

Now as $128 . K_n + G_n' = Q_n$

$Q_1 = 136, Q_2 = 333, Q_3 = 128, Q_4 = 605, Q_5 = 666, Q_6 = 819, Q_7 = 256, Q_8 = 936, Q_9 = 970, Q_{10} = 1298, Q_{11} = 1212,$
$Q_{12} = 416, Q_{13} = 742, Q_{14} = 480, Q_{15} = 1648, Q_{16} = 1989, Q_{17} = 1980, Q_{18} = 2185, Q_{19} = 1260$ and $Q_n = 0$ for $n \geq 20$.

Replacing these values of Q_n in the series $F(s) = \sum_{n=1}^{\infty} \frac{Q_n}{s^2 + n^2}$

$$F(s) = \frac{136}{s^2+1} + \frac{333}{s^2+4} + \frac{128}{s^2+9} + \frac{605}{s^2+16} + \frac{666}{s^2+25} + \frac{819}{s^2+36} + \frac{256}{s^2+49} + \frac{936}{s^2+64} + \frac{970}{s^2+81} + \frac{1298}{s^2+100}$$
$$+ \frac{1212}{s^2+121} + \frac{416}{s^2+144} + \frac{742}{s^2+169} + \frac{480}{s^2+196} + \frac{1648}{s^2+225} + \frac{1989}{s^2+256} + \frac{1980}{s^2+289} + \frac{2185}{s^2+324} + \frac{1260}{s^2+361}$$

Taking inverse Laplace and rearranging the terms we have

$$f(t) = 68\left(\frac{2}{1}\right)\sin t + 111\left(\frac{3}{2}\right)\sin 2t + 32\left(\frac{4}{3}\right)\sin 3t + 121\left(\frac{5}{4}\right)\sin 4t$$
$$+111\left(\frac{6}{5}\right)\sin 5t + 117\left(\frac{7}{6}\right)\sin 6t + 32\left(\frac{8}{7}\right)\sin 7t + 104\left(\frac{9}{8}\right)\sin 8t + 97\left(\frac{10}{9}\right)\sin 9t$$
$$+118\left(\frac{11}{10}\right)\sin 10t + 101\left(\frac{12}{11}\right)\sin 11t + 32\left(\frac{13}{12}\right)\sin 12t + 53\left(\frac{14}{13}\right)\sin 13t + 32\left(\frac{15}{14}\right)\sin 14t$$
$$+103\left(\frac{16}{15}\right)\sin 15t + 117\left(\frac{17}{16}\right)\sin 16t + 110\left(\frac{18}{17}\right)\sin 17t + 115\left(\frac{19}{18}\right)\sin 18t + 63\left(\frac{20}{19}\right)\sin 19t$$

Therefore we have

$G_1 = 68, G_2 = 111, G_3 = 32, \ldots, G_{19} = 63$ and $G_n = 0 \quad n \geq 20$ which is ASCII code equivalent to the given message Do you have 5 guns?

4. Results: Encryption technique uses infinite series, which is of general nature. Moreover, here we used ASCII code with 128 characters, which can be replaced by any other character set depending upon the requirement.

5. Conclusion: In this proposed work, the proposed cryptographic scheme involves a number of mathematical tools, which makes it very complicated for an intruder to trace the message.

REFERENCES

[1] A.P. Stakhov-"The golden matrices and a new kind of cryptography", Chaos , Soltions and Fractals 32(2007) pp1138 – 1146. | [2] A.P. Stakhov-' The Golden section in the measurment theory". Compute Math Appl; 17(1989): pp613 - 638 | [3] Barr T.H. – Invitation to Cryptography, Prentice Hall, 2002. | [4] Blakley G.R. –Twenty years of Cryptography in the open literature, Security and Privacy May 1999, Proceedings of the IEEE Symposium, 9-12. | [5] Dhanorkar G.A. and Hiwarekar A.P. – A generalized Hill cipher using matrix transformation, International J. of Math. Sci. & Engg. Appls. Vol. 5, No. IV, July, 2011, 19-23. | [6] G. Naga Lakshmi, Ravi Kumar B. and Chandra Sekhar A. – A cryptographic scheme of Laplace transforms, International Journal of Mathematical Archive-2(12), 2011, 2515-2519 | [7] Grewal B.S. – Higher Engineering Mathematics, Khanna Pub. Delhi, 2005. | [8] Hiwarekar A.P. - A new method of cryptography using Laplace transform, International Journal of Mathematical Archive-3(3), 2012, 1193-1197. | [9] Lerma M. A. – Modular Arithmetic, http//www.math.northwestern.edu/mlerma/proble m solving /results/ modular arith.pdf. | [10] Petersen K. – Notes on Number Theory and Cryptography, http://www.math.unc.edu/ Faculty petersen/Coding/cr2. pdf. | [11] Overbey J. - Traves W. and Wojdylo J. – On the Key space of the Hill Cipher, Cryptologia, 29(1), January 2005, 59-72. | [12] Ramana B.V. – Higher Engineering Mathematics, Tata McGraw-Hills, 2007. | [13] Saeednia- S. – How to Make the Hill Cipher Secure, Cryptologia, 24(4), October 2000, 353-360. | [14] Stallings W. – Cryptography and network security, 4th edition, Prentice Hall, 2005.