A Design nad Analysis of Geo-Crypto Key Exchange Algorithm for Secure Transmission

L. Rama Parvathi, R. Logeshwari

Abstract*: *The study of different age people from different lifestyle, what all symptoms came for the disease, at what stage, what measures taken to get rid of, later changes, what were the side effects, how it decreased or increased will help in future prediction of possible chance for illness in others. A System which having the above details, suggestions from good and expert practitioners, can be used to give warnings to people about the possibility to get affected after 5 or 10 years and to take pre-cautions . Combinational outcome of Descriptive, Predictive and Prescriptive Data Analytics methods on past and present structured and unstructured Big Data can be used to predict future after effects which should be prioritized and treated. Suggestions can be given to people to take appointment with dieticians, change food habits, perform exercises, practice remedial measures etc. Right step at correct time save lives, gives happiness to families, reduces medical expenditures. The relevant information hidden in massive amount of data are made available by the AI assistants to make better clinical decisions in the functional areas of healthcare. To make such a system, a detailed study on big data, analytics methods, health care, practicing methods, electronic health records etc is required. A preventive guidance and less cost expert system which is helpful for common man and experts, for immediate solution and care can be developed in future. Deep machine learning algorithms to detect later possibility of occurrence should be developed. For this a study on Big Data and Health Care Analytics is done.

Index Terms*: *Big Data, Data Analytics, Descriptive Analytics, Predictive Analytics, Prescriptive Analytics, Volume, Velocity, Veracity.

I. INTRODUCTION

In the advancement, people in need to hide data in the composed structure and retrieve the data without loss. The key exchange mechanism is one of the important concerns, addressed by cryptographic protocol. If the sender and the receiver want to exchange the secret information1, cryptographic algorithms play a vital role in it. If they use a code or cipher sender and receiver are in need of codebooks2 and appropriate keys.

If the cipher is symmetric then both sides are in need of same secret key or if the cipher is asymmetric then both in need of each other's public key. Therefore, the secret keys are to be securely communicated to each other to transfer the secret data in secured manner. To improve the security of the system, the generated key for encoding and decoding process must be long enough to be unbreakable4. There are two types of authentication systems, first one is Knowledge based system, the user needs to remember the key which is more inconvenient to the user and the second one is Possession Based system, the secret keys are stored in smart card, where it can be missed or lost, whereas storing the lengthy keys on a system is more expensive and not much secure5. Geometric based key exchange system can mitigate the constraints of the introductory systems. When user A and B wish to exchange a plaintext message, in figure 1 6, A encrypts the message using the key K and sends to B. Here, B receives the encrypted message and decrypts it with

the same key Ks only. To perform this work, either key Ks or key generation information must be exchanged securely between the users. Hence, there is a need of sharing secure information between the users in the non-secure communication channel.

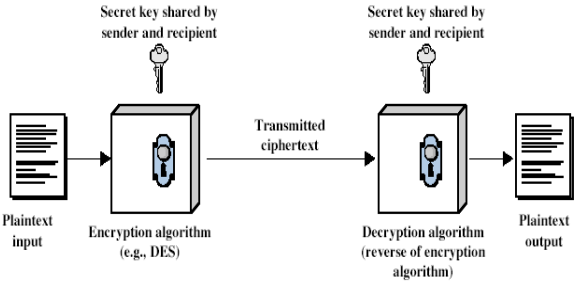

Fig 1. Symmetric cipher model [6]

II. RELATED WORK

For decennium, the labyrinthine patterns have been researched in various fields. Trochoids is one such class of these patterns. The patterns which are formed may not be a circle but it can be irregular. Broadly, trochoidal family includes hypotrochoids, epitrochoids, epicycloids and so on where trochoids are constructed by the locus at a fixed distance from a point adhere to the circle which rotate over another circle. Trochoids are the complex patterns generated by the spirograph tool. General memoir of such curves is explained.[7-8]. To trace the hypotrochoid like patterns for unicycle agents, the range measurements is proposed[9]. Similarly heading angle information is proposed[10]. A Secure Hash Algorithm (SHA-256) is one of the hash functions which generates hash length of 256-bits. A visual based image secure encryption algorithm based on Chaos System was proposed[11], where the parameters of zigzag confusion and 1-D skew tent map are calculated from the

Revised Manuscript Received on December 22, 2018.
Dr.L. Rama Parvathi, Professor, Department of Computer Science and Engineering, Saveetha Institute of Medical and Technical Sciences
R. Logeshwari, Research Scholar, Department of Computer Science and Engineering, Saveetha Institute of Medical and Technical Sciences

original image hash function using SHA-256. The perfect cryptographic hash work has some principle properties which is highlighted[12]. It is infeasible to create a message from its hash, a slight change in message stream will reflect a vast change the hash code sequence. Broadly new hash sequence seems to be un related to the original hash sequence therefore, it is absurd to explore two different message streams with same hash sequence.

Submit your manuscript electronically for review.

III. PROPOSED SYSTEM

The proposed work initially generates the geometric pattern spirograph (Fig 2a, Fig 2b), where Spirograph is technically known as hypotrochoids. This is by a fixed point on an inner circle rolling inside a fixed outer circle. Fig 2c, shows two circles, outer and inner circle where outer circle OC0 of radius R0 is fixed and a small inner circle IC1 of radius R1 where R1 < R0.

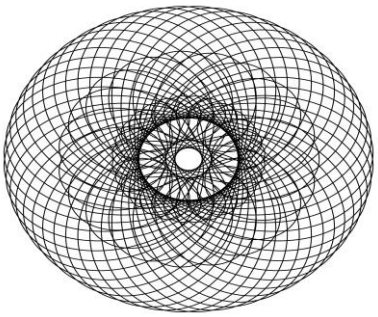

Fig 2. a) outer circle =350, inner circle=250, pen position=25

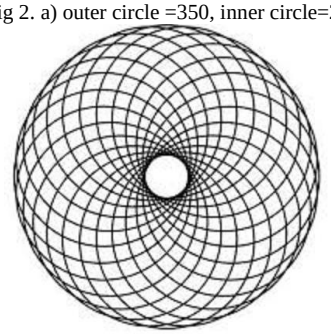

Fig 2 b) outer circle =220, inner circle=145

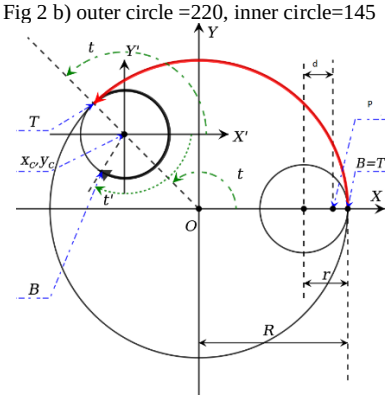

Fig 2. C) Spirograph Mathematical Model

Now assume a point P lying somewhere inside the inner circle IC1 is located at distance d < R1 from IC1's center. Select a point P correlates to the pen hole of the inner circle. Assume that the initial position of the point P is in X-axis whereas it is a tangent of IC1 and OC0. Then the points T and B should be marked in outer and inner circle. The starting position of the point B coincides with the outer circle point T where the point B will traverse on inner circle IC1. The distance traversed by point B and T on inner IC1 and outer OC0 is same. The relative system coordinates (X′,Y′) are defined with respect to the origin at the center of IC1 and the axis which is parallel to original X and Y coordinates. The parameters t and t' are defined to be the angle of T and B which rotated in OC0 and in relative system of coordinates. Therefore, the obit travelled by T and B is same along their corresponding circles. This can be given as,

$$tR0 = (t - t')R1 \quad (1)$$

Let (x1, y1) be the coordinates of the center of inner circle IC1.

$$t' = -\frac{(R0-R1)}{R1}t \quad (2)$$

Where R0 – R1 represents the radius of the center of inner circle IC1 which undergoes circular motion thus,

$$x1 = (R0 - R1)\cos t \quad (3)$$
$$y1 = (R0 - R1)\sin t \quad (4)$$

As stated above, t' is the angle of rotation in the relative system where, a point P obeys the law of circular motion therefore, its coordinates in the new relative system (X', Y') must obey,

$$x' = d\cos t' \quad (5)$$
$$y' = d\sin t' \quad (6)$$

In order to calculate the point P in the actual system of coordinates,

$$x = x1 + x' = (R0 - R1)\cos t + d\cos t' \quad (7)$$
$$y = y1 + y' = (R0 - R1)\sin t + d\sin t' \quad (8)$$

To define the above equations in single term t, use the relation between t and t' from obtained equations, and use the fact that function is odd. Therefore, the spirograph generation equation finally takes the below form,

$$x(t) = R0[(1-k)\cos t + lk\cos\frac{1-k}{k}t] \quad (9)$$
$$y(t) = R0[(1-k)\sin t - lk\sin\frac{1-k}{k}t] \quad (10)$$

For convenience we represented (R0-R1) in terms of the radius R of outer circle. The parameter $0 \le l \le 1$ represents the distance of the point P is placed from the mid of IC1. Also $0 \le k \le 1$ represents size of the inner circle is with respect to outer circle. A shearing transformation is applied to alter the shape of the spirograph pattern object. In shearing process, we either change the image object horizontally and vertically. Shearing can be done based on the 2 transforms X-shear, Y-shear. The X-shear and Y shear values are selected between (0, inner circle radius). X-shear conserves the Y coordinates and transformation made to X coordinates which tilts the vertical lines to left or right. Y-shear conserves the X coordinates and transformation made to the Y coordinates which tilts the horizontal lines to move up or down. Then we apply the random permutation on the tilted bit streams based on the user key, which is referred as permutation key acts as seed value to generate the random numbers equal to the bit stream size. Based on the random numbers, each bit in the string is swapped. Finally, will result with permuted bit string of original bit string. The permuted bit string is hashed with SHA-256 to generate the 256-bit key which act as a private key. This way, private keys of both sender and receiver is generated (PRK_s, PRK_r). Further, we apply Diffie Hellman key exchange algorithm[3], to compute the keys on both sides. The work model (Figure 3) as follows:

Diffie Hellman algorithm requires the large prime number P and its smallest primitive root α. Where P and α can be a fixed value for number of sessions.

Step 1: Take a prime number of P and primitive root α.

Step 2: For user A, using PRK_s compute PUK_s as

$$PUK_s = \alpha^{PRKs} \, mod \, P \qquad (11)$$

Step 3: For user B, using PRK_r compute PUK_r as

$$PUK_r = \alpha^{PRKr} \, mod \, P \qquad (12)$$

Therefore, (PRK_s, PUK_s), (PRK_r, PUK_r) are the key pairs of the user A and B respectively.

Step 4: Share PUKs and PUK_r among the user A & B.

Step 5: Compute secret key K_s by the User A as

$$K_s = (PUK_r)^{PRKs} mod \, P \qquad (13)$$

Step 6: Compute secret key K_r by the user B as

$$K_r = (PUK_s)^{PRKr} mod \, P \qquad (14)$$

Step 7: This secret key is termed as Transitional Key, where this key is hashed using SHA256 to achieve 256-bit key

This 256-bit key is used for encoding and decoding process by the sender and the receiver.

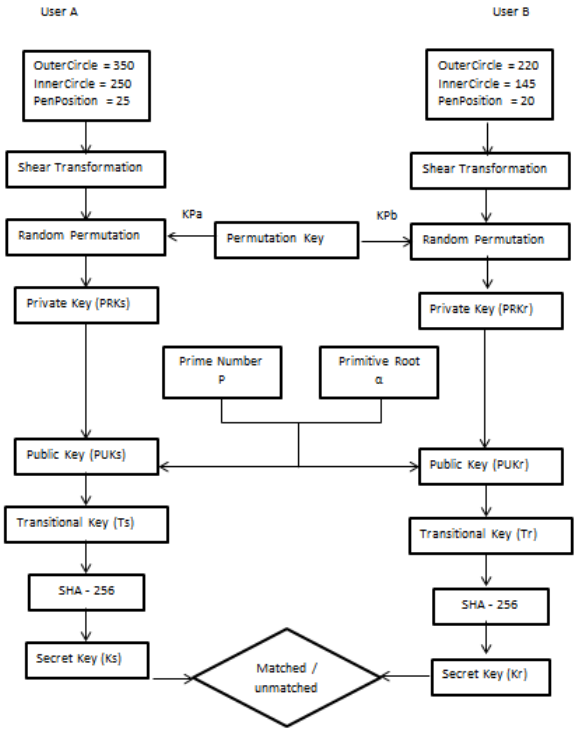

Fig 3. Working Model of Geo-Crypto Key Exchange Protocol

IV. EXPERIMENTAL OUTCOME AND ANALYSIS

The proposed groundwork to perform communication in a secured way is evaluated based on key randomness. The experiment is carried out in MATLAB 2015a. Hardware configuration was: Pentium(R) Dual core 3.0G, 8 GB RAM for 10 sets of geometric patterns where 10 secret keys are generated. The following results obtained from the set 1.

Table I: Input data to generate Geometric pattern

	Outer Circle radius	Inner Circle radius	Pen Position	Shearing Factor
User A	350	250	25	10
User B	220	145	20	12

Table II: Private Key Generation

	User A	User B
Input pattern size	2596	1804
Seed Value	17	21
	After applying SHA-256	
Private Key	215639398169882319921128459198782 77	663604376762932176694692887993655 80
Prime Number P	3142992502864370765738392805586321 2389	
Primitive Root	2	
Public Key	272581060932284088163511807105112 35	427423575658792512334042910786964 07
	Public keys shared among users, compute secret Key on both sides	
Secret Key	530370133549785293956866911687349375	

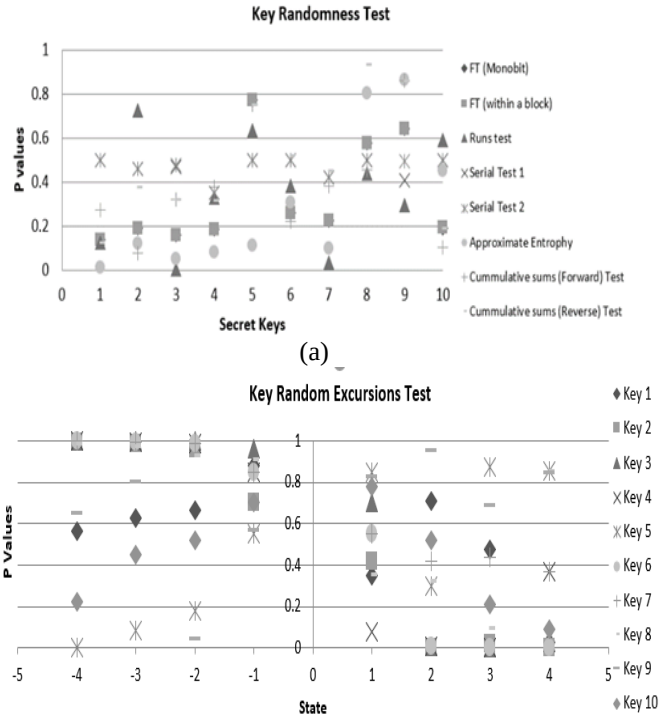

Fig 4 a,b - The Results of The NIST Randomness Tests For 10 Secret Keys

From Table I, we analyses that the user A and B assumes the outer and inner radius of the circle and the pen position where inner circle radius is less than outer circle and pen position value is given within an inner circle. Once the spirograph is generated apply shearing factor to reshape the image. Then the permutation step is carried out based on seed value. The result bit string (Table II) is applied with SHA256 to generate 256-bit private key of user A and User B. further the longest prime number, the primitive root and the private key is used to compute the public key. This public key is shared among the users in the secure channel. Then on both sides' using the each other's public key and their own private key computes the Secret key K which will be same for both users. Sample data is given in Table 1 and Table 2.

Key Randomness Test:

At various aspects of randomness in a long sequence of bits, the statistical tests developed by NIST. The NIST documented 15 statistical tests [13]. We attempted to correlate and classify the binary sequences to a random

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

sequence which satisfies the probabilistic property.

Mono-bit Frequency Test:

Purpose: the distribution of zeroes and ones in the entire bit sequence.

If P value is less than 0.01 then the continuity is not random

FT within a block:

Purpose: the distribution of Ones within a M-bit Block

If P value is less than 0.01 then indicates a large discrepancy from the balanced distribution of ones and zeros in any of the blocks.

Runs Test:

Purpose: the total number of runs is tested in the bit sequence where the test is an uninterrupted sequence of indistinguishable bits.

If P value is less than 0.01 then the continuity is not random

Approximate Entropy Test:

Purpose: Comparing the frequency of projecting blocks of two successive/adjacent lengths (n and n+1) across the expected result for a indiscriminate sequence.

If P value is less than 0.01 then the continuity is not random small values would involve strong regularity. Large values would imply irregularity.

Cumulative Sums:

Purpose: this test is to check whether cumulative sum of the partial sequence is too huge or too small for the random sequence.

If P value is less than 0.01 then the continuity is not random

If mode =0, then it declares, there are either too many zeroes or ones at early stages.

If mode = 1, then it declares, there are either too many zeroes or ones at late stages.

The small values declare that ones and zeros are associated too evenly.

Random Excursion Test:

Purpose: The focus of this check is that the variety of cycles having precisely K visits during additive total stochastic process.

This test is actually a series of eight test in eight states. -4, -3, -2, -1 and +1, +2, +3, +4.

If P value is less than 0.01 then the continuity is not random

Serial Test:

Purpose: To test for the uniformity in two dimensions or higher.

Use chi-square test to search out the deviation of the particular counts from the expected counts.

Observation:

From figure 3a, it is observed that the key 3 fails in runs test because of P value = 0.006 and Key 1 fails in approximate entropy test where P value is 0.013. From fig 3b, it is observed that Key 2 fails at state 2 and 4 where P values are (9.38E-05, 1.25E-05), Key 3 fails at state 3 where P value is (1.50E-06), Key 6 fails at state 2,3,4 where P values are (0.005177, 0.001146, 1.14E-05) in Random Excursion Test.

V. CONCLUSION

The analysis of necessities of the security and experiments for the exchange of secret key between two users has been done. The proposed geo-crypto key exchange algorithm successfully enabled two users to securely agree on a secret key with less computational cost. Also, the proposed algorithm outperforms against various attacks such as replay attack , attack on a host, network attack, etc., where we achieved 93.5% of randomness in generated key sequence, therefore this key exchange approach provides an effective solution for session based secure key exchange communication setup for transmitting the images, videos, audios, text data etc., The Diffie-Hellman key exchange algorithm though provides secure way to exchange the secret keys but, it doesn't verifies the user's identity which gives way for man-in-the-middle attack. Our future work is to deal with the man-in-the-middle attack and to create Multi-Secret Image shares using geometric pattern based key exchange techniques in order to increase the level of security.

REFERENCES

1. G. O. Young, "Synthetic structure of industrial plastics (Book style with paper title and editor)," in Plastics, 2nd ed. vol. 3, J. Peters, Ed. New York: McGraw-Hill, 1964, pp. 15–64.
2. W.-K. Chen, Linear Networks and Systems (Book style).Belmont, CA: Wadsworth, 1993, pp. 123–135.
3. H. Poor, An Introduction to Signal Detection and Estimation. New York: Springer-Verlag, 1985, ch. 4.
4. B. Smith, "An approach to graphs of linear forms (Unpublished work style)," unpublished.
5. E. H. Miller, "A note on reflector arrays (Periodical style—Accepted for publication)," IEEE Trans. Antennas Propagat., to be published.
6. J. Wang, "Fundamentals of erbium-doped fiber amplifiers arrays (Periodical style—Submitted for publication)," IEEE J. Quantum Electron., submitted for publication.
7. C. J. Kaufman, Rocky Mountain Research Lab., Boulder, CO, private communication, May 1995.
8. Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interfaces(Translation Journals style)," IEEE Transl. J. Magn.Jpn., vol. 2, Aug. 1987, pp. 740–741 [Dig. 9th Annu. Conf. Magnetics Japan, 1982, p. 301].
9. M. Young, The Techincal Writers Handbook. Mill Valley, CA: University Science, 1989.
10. (Basic Book/Monograph Online Sources) J. K. Author. (year, month, day). Title (edition) [Type of medium]. Volume(issue). Available: http://www.(URL)
11. J. Jones. (1991, May 10). Networks (2nd ed.) [Online]. Available: http://www.atm.com
12. (Journal Online Sources style) K. Author. (year, month). Title. Journal [Type of medium]. Volume(issue), paging if given. Available: http://www.(URL)
13. R. J. Vidmar. (1992, August). On the use of atmospheric plasmas as electromagnetic reflectors. IEEE Trans. Plasma Sci. [Online]. 21(3). pp. 876—880. Available: http://www.halcyon.com/pub/journals/21ps03-vidmar
14. Rajesh, M., and J. M. Gnanasekar. "Path Observation Based Physical Routing Protocol for Wireless Ad Hoc Networks." Wireless Personal Communications 97.1 (2017): 1267-1289.
15. Rajesh, M., and J. M. Gnanasekar. "Sector Routing Protocol (SRP) in Ad-hoc Networks." Control Network and Complex Systems 5.7 (2015): 1-4.
16. Rajesh, M. "A Review on Excellence Analysis of Relationship Spur Advance in Wireless Ad Hoc Networks." International Journal of Pure and Applied Mathematics 118.9 (2018): 407-412.
17. Rajesh, M., et al. "SENSITIVE DATA SECURITY IN CLOUD COMPUTING AID OF DIFFERENT ENCRYPTION TECHNIQUES." Journal of Advanced Research in Dynamical and Control Systems 18.
18. Rajesh, M. "A signature based information security system for vitality proficient information accumulation in wireless sensor systems." International Journal of Pure and Applied Mathematics 118.9 (2018): 367-387.
19. Rajesh, M., K. Balasubramaniaswamy, and S. Aravindh. "MEBCK from Web using NLP Techniques." Computer Engineering and Intelligent Systems 6.8: 24-26.