Non-Uniform Steps Model: New Layer to Traditional Security Encryption Algorithms (Next Generation Data Security Layer)

Nitish Varshney and Mohammed Abdul Qadeer

***Abstract*—The rapidly increasing reliance of nearly every kind of organization on systems that process electronic data has introduced new concerns, and to tackle the misuse of precious data, encryption of important data has to be done. Traditional encryption security algorithms are well known and can undergo attacks in a number of ways. In this paper we will introduce encryption and the different encryption algorithms, then we will look briefly at the new purposed algorithm based on Non-Uniform Steps Model, which can be applied as a layer over traditional encryption algorithm to enhance power of them. Further in this paper we will briefly describe the various encryption algorithms that we can utilize with Non-Uniform Steps model to enhance security and issues involved with the algorithm and their possible solution. We will try to characterize proposed algorithm to have some experimental analysis. We will then have a look at encryption models applicability and propose new algorithms as a possible solution of number of problems. We will lastly conclude the paper.**

***Index Terms*—Communication system security, data security, security, signature verification.**

I. Introduction

This is the age of internet and networking. With the advancement in technologies, security threats have also increased. No data these days is 'secure enough'. When you type your credit card number and password on an order form, you want to be sure that no one can find the information as it passes through the network. You can't be sure that no one is snooping on your information; your only hope to save such precious data from curious eyes is to encrypt data before you send it. It leads to development of many algorithms and applications based on those algorithms for data protection. Encryption is the process of transforming information utilizing an algorithm to make it unreadable to anyone except those who know how to decode it by knowing the key, as shown in Fig. 1, the man in the Fig sends the encrypted information with the help of key, if the woman in the Fig knows the decryption key, she can find useful information in it. An encryption algorithm utilizes a mathematical formula to make information unreadable. Key can be seen as password.

Manuscript received June 22, 2012; revised July 25, 2012.

The authors are with the Department of Computer Engineering, Aligarh Muslim University, Aligarh, U.P., India (e-mail: nitishvarshney@zhcet.ac.in, maqadeer@gmail.com).

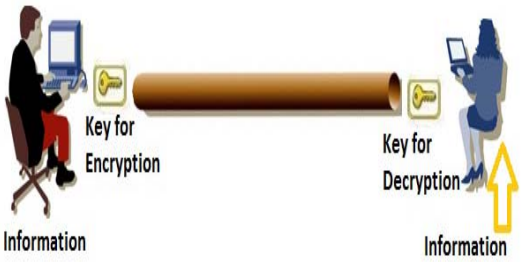

Fig. 1. A General encryption algorithm works.

A lot of encryption algorithms are developed in last decades after introduction of concept of a digital signature in 1976 but most of them are nearing the end of their useful life. Some of them are RSA [1977] [1], DES [1977] [2], BLOWFISH [1993] and AES [2001] [3]. All of them are vulnerable to brute-force attack and other attacks like side channel attacks

II. Different Encryption Algorithms in Brief

Various encryption algorithms are used now-a-days. Some of them are discussed here along with the issues related to them.

A. Data Encryption Standards (DES)

The Data Encryption Standard or DES [2] was publicly announced for use in 1977 by the National Bureau of standards for use in non classified US government files. It utilizes public key cryptography technique. DES encrypts a block of 64 bits using a 56 bit key. The algorithm – which is used as encipher as well as decipher is summarized in Fig. 2. The input block T is first transposed under an initial permutation IP, giving $T_0 = \text{IP}(T)$. After it has passed through 16 iterations of a function f, it is transposed under the inverse permutation IP^{-1} to give the final result. Its 56-bit key size is vulnerable to brute-force attack [4], [5]. It leads to emergent of much stronger method Triple-DES. Triple-DES encrypts data three times and utilizes a different key for one of the three passes. It increases the key size. Triple-DES is much more secure in comparison to DES algorithm.

B. RSA

In 1977 three scientists Rivest, Shamir and Adleman [1] publicly described an algorithm. It was the first practical signature scheme based on public-key techniques. RSA algorithm involves three steps viz. Key generation, Encryption and Decryption. Encryption is done through public key and decryption is done through utilizing a private key. RSA realizes on mathematical symmetry as to begin two large prime numbers are selected and multiplied together.

DOI: 10.7763/IJET.2012.V4.489

The product further can be used as modulus of both public and private key. The problems of RSA are in factoring large numbers and RSA numbers. There are a number of ways to crack the code. Out of these, one carries out a relatively basic calculation again and again. In this way computer can search for similar patterns and such similar patterns can be utilized to break the code. All the methods to crack RSA like Davida's attack, Denning attack viz. rely on the multiplicative property of algorithm.

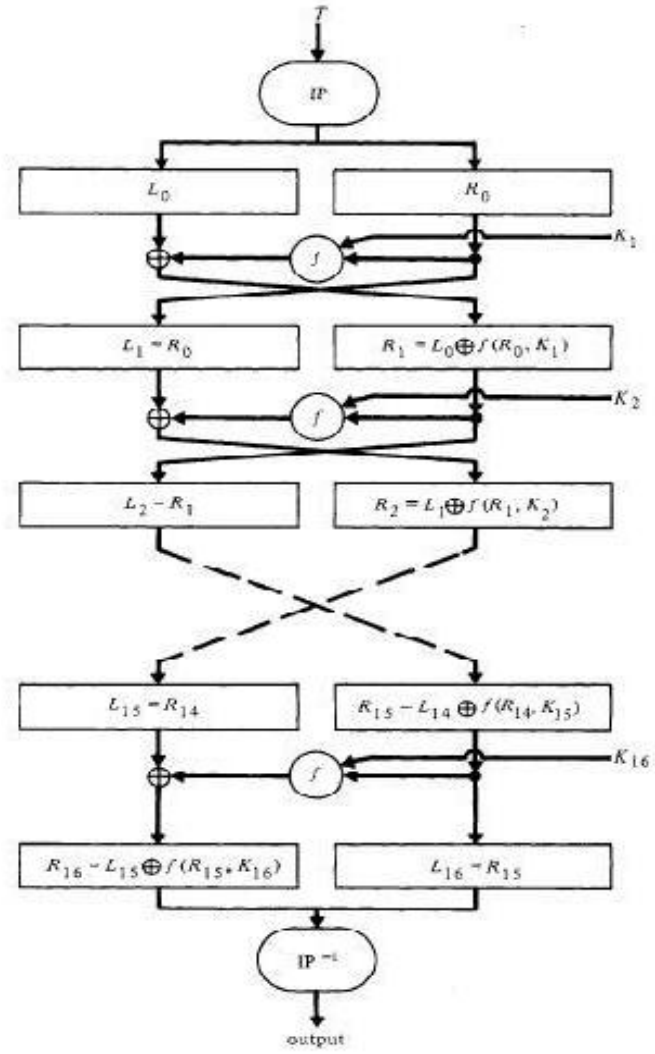

Fig. 2. DES algorithm in operation.

C. Advanced Encryption Standards (AES)

The Advanced Encryption Standards or AES [3], [6] was introduced by National Institute of standards and Technology in 2001. AES takes a block of 128 bits and key is of 128 bits. Both Encryption and decryption starts with "AddRoundKey" stage followed by nine rounds of four stages each and tenth round of three stages. Four stages in the first nine rounds are "substitute keys", "shift rows", "mix column", "AddRoundKey". Mix column stage is not utilized in tenth round. AES is vulnerable to timing attacks and also to brute-force attack with a complexity of 2^119 [7]. In an attempt Daniel J. Bernstein already successfully attacked on open AES in 2005 [8]. So it cannot be used alone for transferring precious data over networks. However it can be combined with other algorithms to enhance security.

III. Next Generation Security

There has been a lot of research which has revealed the vulnerability of these algorithms to different attacks [3]. And most of these algorithms are at the end of their useful life. It leads to think for next generation algorithms. It leads to the development of digital signature algorithms which are used to protect and give access to original data [9][10]. In this paper we are proposing a new model for encryption which is based on "Non-Uniform Steps model"- a technique based on digital signaturing. In Non-Uniform steps model the range of input information is divided in non-uniformly varying steps. Instantaneous step size is determined through some well defined mathematical function. We utilize non-uniform steps to make a model of information that is being input by the user. A database or variable length array can be utilized for storing steps initial position and final position.

A. Encryption

Initial requirements are four variables previous-x (prevx, to locate step initial x-coordinate), previous-y (prevy, to locate step initial y-coordinate), current-x (curx, to locate final and current position of x-coordinate) and current-y (cury, to locate final and current position of y-coordinate) as shown in Fig. 4 which shows non-linear steps breaking of text information which is shown in Fig. 3. These steps values can be taken at every mouse movement, if information is very sensitive like in the case of signatures.

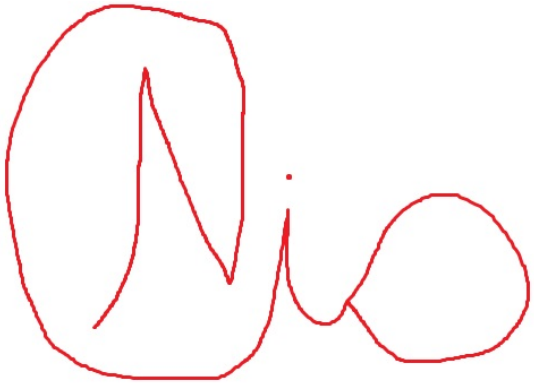

Fig. 3. Snapshot of text information.

Further, we can continue to find out new values of all variables. Now current-x and current-y would become previous-x and previous-y and a new value is stored at current-x and current-y as shown in Fig. 5. The pattern generated can be seen in Fig. 6, first two columns contain the previous x and y coordinates and last two contain the current x and y coordinates. After each fetching of text current-x and current-y can be set as origin (0, 0) and previous-x and previous-y are found in a relative manner in comparison of new origin as shown in Fig. 7. In this way steps are restricted to a maximum of integer value sixty four or one hundred and twenty seven, based on the programming language used by programmer. This restriction provides proposed algorithm a new security layer and further reduces the size of the file or variable data array used to store all variables values. As steps can now be treated as "Unicode encoding text format" not as an integer number. If one tries to decode final cipher and if

succeeded all he or she would have a Unicode encoded text whose value is less than sixty four which makes it unrecognizable to a person who would not know the algorithm. Unicode text may look alike as in Fig. 8. Maximum range comes from the Unicode encoding standards, in which recognizable characters are represented by a value greater than sixty four. Fig. 7 also depicts the fact that if steps formulation is chosen properly, step size is never more than sixty four. Further, we can continue in the same manner to find out a variable pattern having all integers which can not be identified due to asymmetry of steps.

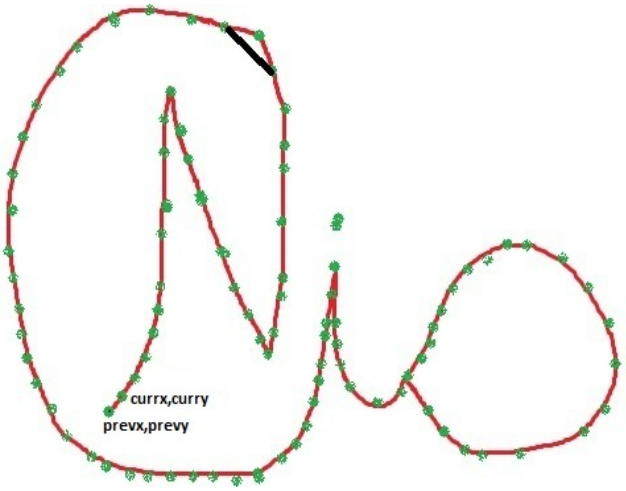

Fig. 4. Snapshot of the non-uniformly stepped cipher.

B. Decryption

In the decryption phase one just has to trace the values stored in variable data array or at a memory location or in a file starting from first information stored. Authentication is required here to prevent illegal access of information. To provide authentication other traditional encryption security standards can be utilized. Tracing is the most important part of proposed algorithm in which step-size comes into picture. If step-size is quite large there is a large probability of errors to occur and decrypted data may produce faulty results in very precious situations like encryption of signature. Error situation is depicted in Fig. 4 through black line. It leads to requirement of small step-sizes.

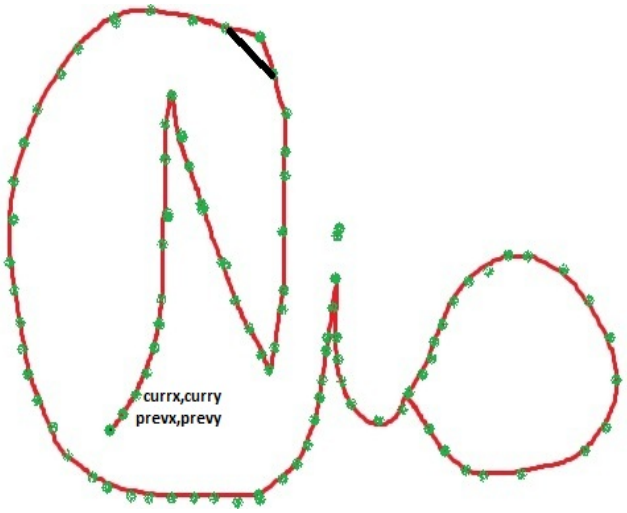

Fig. 5. A Snapshot of the next step in algorithm.

48	377	48	383
48	383	48	388
48	388	48	393
48	393	48	400
48	400	48	405
48	405	48	412
48	412	48	417
48	417	48	424
48	424	48	427
48	427	48	432
48	432	49	438

Fig. 6. A Snapshot of the pattern generated.

48	377	0	6
0	0	0	5
0	0	0	5
0	0	0	7
0	0	0	5
0	0	0	7
0	0	0	5
0	0	0	7
0	0	0	3
0	0	0	5
0	0	1	3

Fig. 7. A Snapshot of the relative pattern.

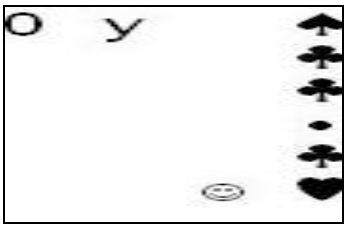

Fig. 8. A Snapshot of Unicode text.

IV. Experimental Results

The encryption method explained so far have been implemented with JAVA language and have been applied to more than 500 images. In this chapter, we characterize the proposed methods with the average values for the whole applied images.

Encryption method proposed by us is characterized on different basis like CPU time, memory required and information content in an offline signature reduction. When whole applied image set summarized average pixels in an image comes out to be 119497 pixels. However, when on same set number of steps required is averaged it comes out to be 797 (0.7% of a signature image). It summarizes the fact in real, less than 1% of the offline signature image is the information part all the other pixels are not of any use. It strengthens the fact about requirement of new algorithm. Also on an average a signature image requires 17560 bytes if saved in JPEG format however output text file created by algorithm takes only 1594 bytes on an average. It means memory or bandwidth requirement is reduced by 91%, a lot

of memory is saved.

In Fig. 9, we provide a snapshot of basic input signature scenario processed by us. Time required for tracing the output text file taken as cipher comes out to be about 36ms.

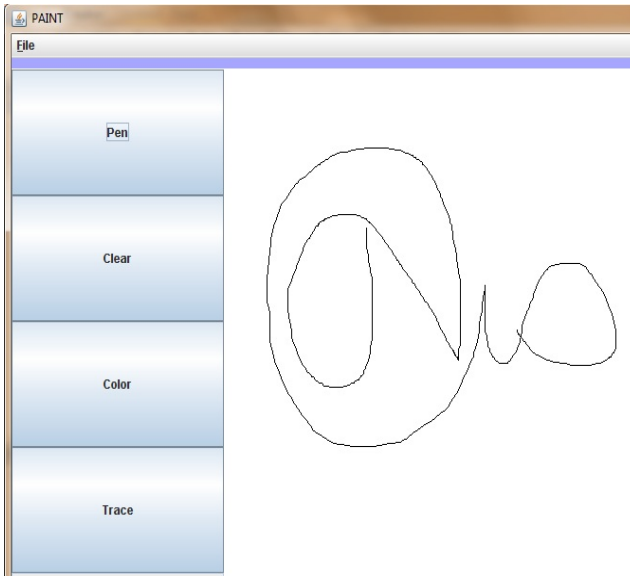

Fig. 9. Basic input scenario.

V. Features

A. Advantages and Possible Extensions

Non-Uniform Steps adoption makes proposed algorithm asymmetrical and less vulnerable to most of the attacks. The most important advantage of the algorithm is that a number of security layers can also be employed over it. It makes it much more secure by enhancing decryption complexity and deploying much secure password protection. Most trusted encryption algorithm standard that can be implemented with proposed model is Advanced Encryption Standard (AES), which can impart enhanced security complexity of order 2^119. Combining a traditional security algorithm makes it unreadable as shown in Fig. 10. Other important fact is that, if a person is able to decode it, he would get a string of integers nothing else. But the issue is that if output text file is encrypted using maximum throughput algorithm blowfish, decrypting the cipher in ECB mode on a P-4 2.4 GHz machine takes about 250ms. It means about 282 ms are required to trace the signature at decryption end, while other encryption schemes like level 4, wavelet domain image encryption by sub band selection and data bit selection only requires 201.43ms.

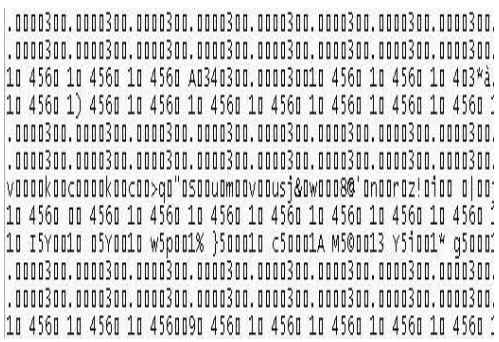

Fig. 10. A piece of encoded message.

Algorithm can be deployed on hardware's too. In the hardware implementation one can utilize variable size array which can take a minimum of thousands information. Directional infra-red (IR) sensors are supposed to give better results.

B. Issues and Their Solution

Proposed algorithm requires a lot of memory for implementation on different scenarios as even a small text requires kilobytes of data for storing. Memory is precious in hardware's and we cannot use kilobytes of data for small information. Algorithm memory requirements can be minimized by minimizing number of variables. As we know that in proposed algorithm

$$(\text{current-}x/y)_i = (\text{previous-}x/y)_{i+1} \text{ for each } i.$$

We can use only one variable out of current and previous. Starting positions can be stored in a variable and then we can just look for current and save it in memory. In this way storage requirement is reduced by a factor of two. Still memory requirements are too high, hence memory requirements is still an issue except in the case of signatures. As actual information content is only 1% of the image and output of algorithm has file size about 9% of the input information, about 8% high.

C. Uses

New introduced algorithm can be deployed in any scenario if some of the basic requirements are fulfilled like presence of memory for saving information and high speed computational device to perform quick manipulation over text. As proposed algorithm provide better security but at cost of storage memory, algorithm can be utilized to encrypt short messages like short message services (sms) and cryptographic message syntax (CMS). Passwords, credit card numbers and other essential information can also be stored in a non-uniformly stored stepped cipher and can be placed anywhere and it is safe as it passes through network. The algorithm is supposed to be efficient in encrypting packet-sized data. (An ATM packet has a 48- byte data field.) Digital signatures problem can also be resolved through it, as in place of coded message sequence of non-uniformly stepped encoded cipher is provided.

VI. Conclusion

In this paper we first introduced different traditional security standards and the need of a new layer to make them much more secure. The feasibility of the new algorithm is thus justified. Further, we provided a new security algorithm for encryption, which is simple and asymmetrical in nature. The combination of traditional encryption security algorithm with non-uniform relatively encoded steps makes the decryption extremely difficult without knowing the secret key. It provides a proper solution for problems like password storage, signature and precious data transfer through network. One can also makes use of online handwriting signatures instead of handwritten signature images for registration. The only concern that can be there and which can hinder the implementation of proposed algorithm is the CPU time requirement to manipulate signature which is slightly more

than the existing algorithm. We are planning to have cryptanalysis to determine performance of this algorithm. Also, we are trying to extend this algorithm to include hardware which can trace a message written through it.

REFERENCES

[1] R. Y. Y. Cao and C. Fu, "An efficient implementation of RSA digital signature algorithm," *Intelligent Computation Technology and Automation (ICICTA)*, 2008

[2] R. M. Davis, "The data encryption standard in perspective," *Communications Magazine, IEEE* vol. 16, no. 6, pp. 5 - 9, Nov. 1978.

[3] W. Stallings, *Cryptography and Network Security*, 2nd ed, Prentice Hall, Inc. 2000.

[4] M. J. Weiner, "Efficient DES key search," *Advances in Cryptology--CRYPTO '93 Proceedings*, Springer-Verlag.

[5] R. Kaplan. Breaking DES code. [Online]. Available: http://www.mycrypto.net/encryption/des_crack.html.

[6] Y. Xiao, B. Sun, H.-H. Chen, S. Guizani, and R. Wang, "Performance analysis of advanced encryption standard (AES)," G*LOBECOM '06 Proceedings, IEEE*.

[7] C. Parikh and P. Patel, "Performance evaluation of AES algorithm on various development platforms," in *Proc. IEEE International Symposium* on *Consumer Electronics*, vol. 20-23, pp. 1 – 6, June 2007.

[8] X. Zhao, T. Wang, D. Mi, Y. Y. Zheng, and Z. Y. Lun, "Robust first two rounds access driven cache timing attack on AES," in *Proc. Computer Science and Software Engineering, 2008 International Conference* on vol. 3, no. 12-14, pp. 785 - 788, Dec. 2008.

[9] O. Matoba, T. Nomura, E. P. Cabre, M. S. Millan, and B. Javidi, "Optical techniques for information security," in *Proceedings of the IEEE*, vol. 97, no. 6, pp. 1128 - 1148, June 2009.

[10] *Encryption Policy*, adopted by the IEEE-USA, Board of Directors, The Institute of Electrical and Electronics Engineers, Inc. - United States of America. vol. 20, June 2008.

Nitish Varshney did his Bachelor of Technology in Computer Engineering, (Class of 2011) from Zakir Hussain College of Engg. & Technology, Aligarh Muslim University, Aligarh, U.P., India. His fields of interest include data security, networks, web development etc. He is part of the team who co-initiated and cofounded "X-Coders club" to enhance programming skills of students of A.M.U.

Mohammed A. Qadeer is an Asst. Professor with the Department of Computer Engineering, Aligarh Muslim University, India. Earlier, he was working with Cisco Systems Inc. as a Network Consulting Engineer with the Advanced Services division in the APAC region. He received his B.Sc. Engineering (Computer Engineering) from Aligarh Muslim University in1996. He has an experience of 15~ years in the area of computer networks and systems. He served as a Technical Co-Chair for IEEE WOCN 2012, 2011, 2010, Technical Co-Chair IEEE AH-ICI 2012, 2011, International Steering Committee for ICACT2012, 2011, 2010 and as TPC member for CCNC 2011, 2010, INMIC 2009, AH-ICI 2009, WIA 2009 and MMA2009. He has been session chair and TPC reviewer for many IEEE/ ACM conferences and is a reviewer for IET Communications Journal as well. He is on the editorial board of International Journal of Digital Multimedia Broadcasting. Established global and nationwide setups of Internet Service Providers (ISP), Internet Exchange Points (IXP), Internet Data Centre (IDC) and Content Delivery Networks (CDN) both from a Networks and Systems perspective. His areas of research are computer networks, wireless networks, mobile computing, next generation networks, IMS, LTE, WiMAX, 4G, WiBro etc.