



Performance Evaluation of New Encryption Algorithms with Emphasis on Probabilistic Encryption & Time Stamp in Network Security

Shashi Bala

Software Engineering Department,
Bits Bhiwani, India

Lect. Vipin Arora

Computer Science Department
BITS Bhiwani, India

Abstract- *The necessity of information security within an organization have undergone major changes in the past and present times. In the earlier times physical means is used to provide security to data. With the advent of computers in every field, the need for software tools for protecting files and other information stored on the computer became important. The important tool designed to protect data and thwart illegal users is computer security.*

This study represents the importance of Encryption of data for storage and transmission. The significance of encrypted data can be identified in light of the mushrooming applications and globalization of communication. The advantages of encrypting data manifest themselves in the form of security & confidentiality in real time applications. Encryption of data is of particular significance in applications like email, e commerce, e-cash where highly vulnerable communication lines is accessed for transmission of highly volatile data.

The study traces the development of various encryption models in a real time environment in all their breath taking diversity and breakthroughs. The significance of the advances and adaptabilities is measured in terms of their diversity of applications in myriad ways that we feel in our daily lives.

To identifies the methodology used in the developed work. It is classified as two algorithms. The first algorithm generates a sequence, followed by model to generate sub keys and mapping of sequence or the sub keys on plain text to generate cipher text. The second algorithm considers a key, a time stamp & a nonce value to generate sub keys which are mapped on plain text to generate cipher text.

*Training an encryption model involves variable length key, a plain text and an algorithm which applies the key on the plain text to generate cipher text. This allows for the data to be transmitted over the network in some form which cannot be read by any intruder. In the first algorithm, the model is trained for different keys and an analysis of the models is being done. The random matrix keys of the form 3*3 keys and 4*4 matrix keys are considered in the training process. In the second algorithm, the model is trained for different key values, time stamps & nonce values. By having small variations in the keys, the models are studied for their increase in performance and working. The models are also trained for their increase in security by having slight variations in the key values. The models are also studied for changes in data overhead for small variations in the key values.*

Keywords-*Encryption, Encryption Algorithms , Algorithms, Network Security.*

I. INTRODUCTION

Introduction-Because of the fallibility of its human designers and its own abstract, complex nature, software development must be accompanied by quality assurance activities. It is not unusual for developers to spend 40% of the total project time on testing. For life-critical software (e.g. flight control, reactor monitoring), testing can cost 3 to 5 times as much as all other activities combined. The destructive nature of testing requires that the developer discard preconceived notions of the correctness of his/her developed software. The necessity of information security within an organization have undergone major changes in the past and present times. In the earlier times physical means is used to provide security to data. With the advent of computers in every field, the need for software tools for protecting files and other information stored on the computer became important. The important tool designed to protect data and thwart illegal users is computer security.

With the introduction and revolution in communications, one more change that affected security is the introduction of distributed systems which requires carrying of data between terminal user and a set of computers. Network security measures are needed to protect data during their transmission. The mechanisms used to meet the requirements like authentication and confidentiality are observed to be quite complex.

Security mechanisms usually involve more than a particular algorithm or protocol for encryption & decryption purpose and as well as for generation of sub keys to be mapped to plain text to generate cipher text. It means that participants be in possession of some secret information (Key), which can be used for protecting data from unauthorized users. Thus a model has to be developed within which security services and mechanisms can be viewed.

To identify and support the security services of an organization at its effective level, the manager needs a systematic way. One approach is to consider three aspects of information security that is Security attack, Security mechanism and Security services. Security attack identifies different modes by which intruder tries to get unauthorized information and the services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

As the importance of information systems is ever growing in all most all fields, electronic information takes on many of the roles, earlier they being done on papers. Few information integrity functions that the security mechanism has to support are security and confidentiality of the data to be transmitted and authentication of users.

This general model shows that there are four basic tasks in designing a particular security service.

1. Designing an algorithm for performing encryption & decryption process.
2. Generating the secret information with the help of algorithm of step 1.
3. Identifying methods for the distribution and sharing of secret information.
4. Identifying rules to be used by both the participating parties to make it secured.

A crypto system is an algorithm, plus all possible plain texts, cipher texts and keys.

II. METHODOLOGY OF THE PROPOSED WORK

The following sequence of steps identifies the methodology adopted in this work.

1. Definition of the problem.
2. Algorithms for generation of subkeys.
3. An algorithm 1 which multiplies ternary vector and a random matrix key to generate a sequence. Dividing the sequence generated in algorithm 1 into basins based on equality of values. Mapping of the sequence or basins to the plain text to generate cipher text. This mapping develops 3 models which are discussed in detail as subunits. The developed algorithm is trained to find an optimal key.
4. An algorithm 2 which considers a key, a time stamp and an Initialization vector to generate sub keys which are mapped to plain text to generate cipher text.
5. Training of the developed algorithms with different keys.
6. Adopting a suitable mechanism to identify any garbled keys while transmission from the Key distribution centre.
7. Comparative study of the developed algorithms in terms of Computing power, their Complexity in terms construction & strength, Avalanche effect & Security analysis.
8. Comparative study of the algorithms with standard models like DES & RC4.
9. Summary & Conclusion of the work.

The first algorithm uses a matrix key which on multiplication with a ternary vector and applying a sign function on the product generates a sequence. This sequence will be used to generate three different models of substitution technique. Thus the algorithm is considered to be a substitution algorithm which uses a single key to be shared by both the sender and receiver, and the cipher processes the input element continuously, producing output one element at a time. The new encryption algorithm is based on the concept of Poly alphabet cipher which is an improvement over mono alphabet..

The second algorithm considers not only key but also initialization vector and a time stamp to generate sub keys which are used for encryption process.

COMPARATIVE STUDY OF DIFFERENT DEVELOPED MODELS

Comparative Study of Different models of the proposed work.

The core of the study is the analysis and discussion of Developed encryption models. All the models are studied for their performance in terms of computational power, avalanche effect, complexity of the models in terms of their construction and strength. The models are also studied for their improved performance against crypto analysis.

Number of Computations for the developed models

Algorithm1:

Model 1: 10 Computations to convert one plain text character to one cipher text character.

Model 2: 14 Computations to convert one plain text character to one cipher text character.

Model 3: 11 Computations to convert one plain text character to one cipher text character.

Algorithm 2:

Model : 09 Computations to convert one plain text character to one cipher text character.

Computational overhead (Computing Power) for the developed models

Algorithm 1:

Model 1:

Computation overhead for a 9 character key

1st computation: 27 calculations, 2 computation: 27 calculations, 3 computation: 27*9 calculations. 4th computation: 27 calculations, 5th computation: 27 calculations, 6th computation: 27 calculations, 7 computation: 27 calculations considering a 27 character plain text, 8th computation: 27 calculations, 9th computation: 27 calculations, 10th computation 27 calculations.

Thus the total computational overhead per block of data by the first model is 486 calculations.

Model 2:

Computational overhead for a 9 character key

1st computation: 27 calculations, 2nd computation: 27 calculations, 3rd computation: 27*9 calculations, 4th computation: 27 calculations, 5th computation: 27 calculations, 6th computation: 27 calculations, 7th computation:

27*27 calculations +27*27 calculations, 8th computation: 27 calculations, 9th computation: 03 calculations depending on chosen rule, 10 computation 03 calculations, 11 computation: 27 calculations, 12th computation: 27 calculations, 13th computation: 27 calculations, 14th computation: 03 calculations depending on the chosen rule.

Thus the total computational overhead per block of data by the second model is 1953 calculations.

Model 3:

Computational overhead for a 9 character key

1st computation: 27 calculations, 2nd computation: 27 calculations, 3rd computation: 27*9 calculations, 4th computation: 27 calculations, 5th computation: 27 calculations, 6th computation: 27 calculations, 7th computation: 27*27 calculations +27*27 calculations, 8th computation: 27 calculations, 9th computation: 81 calculations, 10th computation: 81 calculations, 11th computation: 81*k calculations (where k refers to number of computations for a random pick up of values). Thus the total computational overhead per character by the fourth model is 2025 +81k calculations.

Algorithm 2:

If we go by the algorithm, the number of computations required to generate the sequence at different grid points by different time stamps depends on the steps of time stamp, nonce considered. In the given problem for a time stamp 10 units & a Nonce of 21, the total number of computation needed to generate 20 character block of cipher text is around 500 computations.

III. APPLICATIONS

Mobile Adhoc Networks:

In applications like Mobile Adhoc Networks [39], Wireless Sensor Networks and Broad Casting Applications, New symmetric encryption techniques and probabilistic encryption techniques can well be used. It can also be used for Key encapsulating mechanism (KEM) along with Public key cryptography, which can well be used in secure electronic transactions.

A wireless sensor network:

WSN is a wireless network [19,41,42] consists of distributed devices which contains sensors to observe environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different places. The main application of this sensor networks lies with motivated by military applications. Each node is associated with sensors, with a radio transceiver, a small microcontroller, and a battery. The capacity of the sensor considered depends on energy requirements and bandwidth and computational speeds. A sensor network is supported with multi-hop routing algorithm. Since the very important application of wireless sensor network lies with military applications, security is of high importance.

Broad Casting Applications:

One more important application of encryption algorithms lies with Broadcasted data [6]. Broadcasting applications like audio and video is transmitted to the public. Television and radio programs are examples of broadcasting applications. In certain applications like military applications, policing applications, financial applications relevant to a larger variety of customers, message transmission through broad casting is very much relevant. These are certain applications where higher level of security is needed. Since the data rate is very high in broad casting applications, the computing power needed for encryption process and decryption process is also high.

Key Encapsulating Mechanism:

Some more practical applications use hybrid encryption to deal with large plaintext messages since the efficiency of the public key encryption algorithm is low and computational head is high. As a main part of hybrid encryption schemes, Key Encapsulation Mechanism [5,16] allows a sender to generate a random session key and distribute it to recipient. In some communication scenario, the session key used in new symmetric encryption model and as well probabilistic encryption models can be encapsulated to designated group through their public keys. Anyone can encapsulate a session key for a designated group and any recipient in the designated group can decapsulate the session key with his private key. Thus the mechanism is secure against adaptively chosen cipher text attacks in standard model, which provides ultimate security, confidentiality and authentication to the transmitted data.

IV. CONCLUSION

- The conclusions is, reflecting the overall security and confidentiality rates of transmitting data, confirm the improvement in the efficiency of transmitting data. The methodology used in the dissertation can be used for evaluating new encryption algorithms in terms of multiple parameters. Further, the quantitative data indicates relationship between Random key considered, sub keys (Basins) generated, computational power needed by the first algorithm and the strength and security of the algorithm. It also identifies the importance of multiple parameters like keys, time stamps and nonce values used in second algorithm in terms of its security & strength.
- In the case of Substitution encryption algorithms, the gain by using DES algorithm is its low computational power, which will be very much gained by using the developed models. The developed models are giving almost equal security at low computational overhead (Computing power). As the security of encrypting models is directly related to the key length [3], the more the key length the more will be the security of the algorithm.

But this parameter increases the computational overhead (computing power) of the encryption algorithms. The security of the developed models is relatively free from the key length which gives more flexibility regarding computing power.

- Another conclusion from the above study is freeness from public key attacks. With probabilistic encryption algorithm (Model 3), a crypto analyst can no longer encrypt random plain texts looking for correct cipher text. Since multiple cipher texts will be developed for one plain text, even if he decrypts the message to plain text, he does not know how far he had guessed the message correctly. Under this scheme, different cipher texts will be formed for one plain text. Also the cipher text will always be larger than plain text.

V. FUTURE SCOPE

The focus today and I believe for the indefinite future, will be to create new products that are far simpler and easier to use, that cost less to manage, and that provide a higher level of assurance the enterprise is in compliance with government regulations and industry standards. I see secure messaging and data-storage solutions becoming largely transparent to the end user. Nearly all the technologies needed to transparently encrypt, decrypt, sign, and verify any data object—whether it's an email, a video clip, or a voice transmission—are in place today. At the same time, however, future products based on these newer application technologies will also offer a degree of user interaction—or at least enterprise-level modification—to accommodate the varied and specific security needs of particular groups of users. So, the underlying implementations will be more sophisticated than they are today, but the user interface will be virtually transparent to most users. We will secure our messages and data and not even have to think about it. That is where I see the future of encryption—enabling us to accomplish more complicated tasks with far less effort, and more securely.

The present work deals with plain text being represented by numerical and characters of English alphabet. The work can be improved so that it can support the characters of not only English but also of other languages as well. The work can also be improved to support not only text but also other forms of message transmission like audio, video and images.

REFERENCES

- [1] Amjay Kumar, Ajay Kumar: Development of New Cryptographic Construct using Palmprint Based Fuzzyvault, EURASIP Journal on Adv. In Signal Processing, Vol 21, pp 234-238, 2009
- [2] Baocang Wang, Qianhong Wu, Yupu Hu: A Knapsack Based Probabilistic Encryption Scheme, On Line March 2007, www.citeseer.ist.psu.edu.
- [3] Bluekrypt 2009: Cryptographic Key length Recommendations, <http://www.keylength.com>
- [4] Blum L., Blum M., Shub M.: A simple unpredictable pseudo random number generator, SIAM J. compute, 1986, 15, (2), pp 364-383.
- [5] Brics: Universally comparable notions of key exchange and secure channels, Lecture Notes in Computer Science, Springer, Berlin, March 2004.
- [6] Sage.math.Washington.edu/home/jetchev/Public.html/docs/jetchev-talk.ppt- Broadcast encryption schemes.
- [7] Brassard G.: Modern Cryptology, a tutorial lecture Notes on computer science, (325), (spring-verlas).
- [8] Bruce Schneier: Applied cryptography (John Wiley & sons (ASIA) Pvt. Ltd.
- [9] Carlone Fontaine & Fabien Galand: A Survey of Homomorphic Encryption for non specialists, EURASIP Journal, Vol 07, Article 10.
- [10] Donovan G.Govan, Nathen Lewis: Using Trust for Key Distribution & Route Selection in Wireless Sensor Networks, International Conference on Network Operations & Management, IEEE Symposium 2008, PP 787-790.
- [11] Dorothy E. Denning et al.: Time Stamps in Key Distribution Protocol, Communication of ACM, Vol 24, Issue 8, Aug 1981, pp 533-536.
- [12] E.C.Park, I.F.Blake: Reducing communication overhead of Key Distribution Schemes for Wireless Sensor Networks: Computer Communications & Networks, ICCCN 2007, pp 1345-1350.
- [13] Georg J.Fuchsbaauer: An Introduction to Probabilistic Encryption, 'Osjecki
- [14] Matematicki List 6(2006), pp37-44.
- [15] Guo D, Cheng L.M., Cheng L.L.: A New Symmetric Probabilistic Encryption Scheme Based on Chaotic Attractors of Neural Networks, Applied Intelligence, Vol 10, No.1, Jan 99, pp 71-84.
- [16] Hamid Mirvazri, Kashmiran Jumari Mahamod Ismail, Zurina Mohd. Hanapi: Message based Random Variable Length Key Encryption Algorithm, Journal of Computer Science, pp 573-578, 2009.
- [17] Hianyi Hu, Gufen Znu, Guanning Xu: Secret Scheme for Online Banking based on Secret key Encryption, Second International Workshop on Knowledge Discovery & Data Mining, Jan 23-25 2009.
- [18] Henry Baker and Fred Piper: Cipher systems(North wood books, London 1982).
- [19] William Stallings: Cryptography and network security (Pearson Education, ASIA 1998)
- [20] Kaiping Xue: Study of improved key Distribution Mechanisms based on two length structure for wireless sensor networks, International conference on adv. Information Technology, 2008.
- [21] Krishna A.V.N.: A new algorithm in network security, International Conference Proc. Of CISTM-05, 24-26 July 2005, Gurgoan, India.
- [22] Krishna A.V.N., Vishnu Vardhan.B.: Utility and Analysis of some Encryption algorithms in E learning environment, International Convention Proc. Of CALIBER 2006, 02-04 Feb. 2006, Gulbarga, India.
- [23] Krishna A.V.N., S.N.N.Pandit: A new Algorithm in Network Security for data

- [24] transmission, Acharya Nagarjuna International Journal of Mathematics and Information
- [25] Technology, Vol: 1, No. 2, 2004 pp97-108
- [26] Krishna A.V.N, S.N.N.Pandit, A.Vinaya Babu: A generalized scheme for data encryption technique using a randomized matrix key, Journal of Discrete Mathematical Sciences & Cryptography, Vol 10, No. 1, Feb 2007, pp73-81
- [27] Krishna A.V.N., A.Vinaya Babu: Web and Network Communication security Algorithms, Journal on Software Engineering, Vol 1, No.1, July 06, pp12-14
- [28] Krishna A.V.N, A.Vinaya Babu: Pipeline Data Compression & Encryption Techniques in e-learning environment, Journal of Theoretical and Applied Information Technology, Vol 3, No.1, Jan 2007, pp37-43.
- [29] Krishna A.V.N, A.Vinaya Babu: A Modified Hill Cipher Algorithm for Encryption of Data in Data Transmission, Georgian Electronic Scientific Journal: Computer Science and Telecommunications 2007 !N0. 3(14) pp 78-83.
- [30] 27.Lester S. Hill, Cryptography in an Algebraic Alphabet, The American Mathematical Monthly 36, June-July 1929, pp306–312.
- [31] 28.Lester S. Hill, Concerning Certain Linear Transformation Apparatus of Cryptography, The American Mathematical Monthly 38, 1931, pp135–1 54.
- [32] Maybec.J.S. (1981), Sign Solvability, Proceedings of first symposium on computer assisted analysis and model simplification, Academic Press, NY.
- [33] M.Steiner, M.Waidner: Tutorial on Secure Electronic Commerce, 1999.
- [34] Pandit S.N.N (1963): Some quantitative combinatorial search problems. (Ph.D. Thesis).
- [35] 32.Pandit S.N.N (1961): A New matrix Calculus, J Soc., Ind. And Appl. Math. Pp632-637.
- [36] Pci Yihting: A Temporal order Resolution algorithm in the multi server time stamp service frame work, International Conference on Advanced Information Networking & Applications, AINA 2005, Vol 2m 28-30 March, pp 445-448.
- [37] Phillip Rogaway : Nonce Based Symmetric Encryption, www.cs.ucdavis.edu/rogeway.
- [38] R.S.Thore & D.B.Talange: Security of internet to pager E-mail messages (Internet for India-1997IEEE Hyderabad section) pp.89-94.
- [39] Raja Ramanna Numerical methods 78-85(1990).
- [40] R.H.Rahnan, N,Nowshen: A New Symmetric Key Distribution Protocol Using Centralized Approach, Asian Journal of Information Technology, 2007 6(8) pp 911-915.
- [41] Suhas V. Patenkar Numerical Heat Transfer and Fluid Flow 11-75(1991).
- [42] 39 Terry Ritter: Substitution Cipher with Pseudo-Random Shuffling, Cryptologia archive,
- [43] Volume XIV, issue 4, Oct 99, www.portal.acm.org
- [44] wikipedia.org/wiki/Mobile-adhoc-network
- [45] wikipedia.org/wiki/sensor_network
- [46] Wireless sensor networks: Edited by C.S.Raghavendra, Krishna M. Sivalingam, Taieb Znati.
- [47] [http://www.cs.cmu.edu/afs/cs/project/edrc-ballista/www/Ballista COTS Software Robustness Testing Harness homepage](http://www.cs.cmu.edu/afs/cs/project/edrc-ballista/www/Ballista_COTS_Software_Robustness_Testing_Harness_homepage).
- [48] Victor R. Basili, Richard W. Selby, Jr. "Comparing the Effectiveness of Software Testing Strategies", Technical Report, Department of Computer Science, University of Maryland, College Park, 1985.
- [49] Boris Beizer, Software Testing Techniques. Second edition. 1990