Volume 3, Issue 8, August 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Data Encryption and Decryption using Deterministic Random Key for Transmission: A Review

Er. Vidiksha[1]
[1]*GIMT, KURUKSHETRA*
India

Er. Shekher Saini[2]
[2]*ASSTT. PROFESSOR, GIMT, Kurukshetra*
India

Abstract: Cryptography is an art of scrambling the data in order to provide security and confidentiality. Cryptography is being used in order for the securely transmission of the data. Now a day's it is impossible to provide security as the hacker or the attackers can easily get the data as they are easily able to know key and if key get key they will be able to decrypt your whole important data. This document survey many research papers about cryptography and various means to make cryptography more robust and propose a way in order to make your encryption more reliable and secure by adding randomness to the key, by adding the randomness to the key in order to keep the important data more secure. The key that I will try to generate will be going to generate randomly for every connection. The proposed work act as an alternative to key distribution as the key is not being distributed but is being generated on both the ends deterministically.

Keywords: Encryption, Decryption, Cryptography, Key.

I. INTRODUCTION

In today's world security is an imperative part of our life. With the advancement in the communication, security is the only thing that is needed by everyone in order to keep their communication secure. There are many methods that have been proposed many researchers that provide security during communication using random number generators, using secure key, using large length key which is very difficult to break. This paper is divided in to various sections which are as follows In Section 1 we present the introduction about the cryptography from its dawn, In Section 2 we survey already existing papers on cryptography, In Section 3 we will propose our algorithm for generating the random key for the communication and finally In Section 4 we will conclude.

Plain text [8]: Message in original form is known as plaintext.

Encryption or Enciphering [8]: The process of converting plain text in to cipher text is known as Encryption and Enciphering.

Cipher text [8]: Message in encrypted form or coded form is known as cipher text.

Decryption or Deciphering [8]: The process of converting cipher text into plain text is known as Decryption or Deciphering.

Cryptography [8]: Art and science of scrambling data is known as cryptography.

Cryptography is the art and science of using cryptographic techniques means using and practicing the cryptographic techniques and designing a secure cryptosystem. Cryptanalysis refers to the art and science of breaking that cryptographic technique. Cryptography and cryptology are being used interchangeably but the cryptography is the study of the cryptographic techniques but the cryptology is the combined study of both the cryptography and cryptanalysis. Types of cryptography

- Symmetric-key cryptography
- Asymmetric-key cryptography

Symmetric-key cryptography is also known as the secret key cryptography or private key cryptography. In this cryptography both the sender and the receiver knows the secret key used for the encryption of the data. In this both sender and the receiver both shares the same key. Asymmetric-key cryptography is also known as the public key cryptography. In this the pair of keys are used one is to encrypt the data at the sender side and other is to decrypt the data at the receiver side. In this the data at the sender side is encrypted using the public key and encrypted data at the receiver side is decrypted using the private key.

Nowadays as the communication is increasing and our lots of sensitive information is being sent over the network or internet so there is a need of information security and safety.

II. RELATED STUDY

We have made an extensive research regarding the generation of the random key for the encryption of data.

M.G. Madiseh et. al. [1] used the information of the source in order to generate the random key, the author has generated the key rather than keeping an eye on the key distribution. The author has used the characteristics of the random source and then generated the key. In my proposed approach I will try to use some easy way to generate the key rather than going for the information of the random source. G Ramesh et. al. [3] has proposed the new encryption algorithm in which a key is generated randomly and used for the encryption but the algorithm proposed by him is very complex, includes lots of computation and difficult to implement. N Khanna et. al. [2] algorithm that uses the symmetric key cryptography in which the key must be known on the both sides and using that key certain parameters are calculated which then be used to construct the matrix and then the encryption is done but as the key must be known at the both sides so that may lead to problems that if the third party get to know about the key so the data won't be secure any more. Hatem Hamad and Souhir Elkourd [4] used the method for key generation in mobile network. In their paper they have used the location coordinates and the dtd for their key generation but the problem with that was that the phone has to be GPS enabled and if there the device is moving fast so there are chances of error in the generation of the key.

III. PROPOSED WORK

As many authors has proposed their idea of key generation and key distribution [1,3,4,7]. So we are going to propose an idea in which we are going to used the port numbers which are being used for the communication purposes in wired network. The communication between the client and the sender side starts with the request sent from the client to the server and then the server serves the client on that request, this is what we all know. But in order to understand what actually happens, we will have to go at the low level i.e. at the transport layer. At transport layer the communication happens to be in the form of the sockets. Where the client socket communicates with the server socket. The socket is basically the combination of the IP address and the port no. of the application. The client knows the port no. of the server and sends the request to the server, and the server on accepting the request gets the port no. of the client. As both the sever and the client knows each other port number so that information I am going to use for the generation of the key and after that generation the hashing will be applied on that key that is generated and that will be used for the encryption of data. The same algorithm works for both sender and receiver for generating the key for encryption and decryption. If the connection is for the first time then the sender will generate the key using the port no. of the client and by having the hash of that key a unique number will be generated and that unique number will be used as encryption key for encrypting the data. At receiver side i.e server side the server receives the encrypted data and then using the same algorithm the server or the receiver generates the same key and decrypt the data. The main advantage here is that the key is not being distributed here but the key is being generated on both sides using the same algorithm successfully. The key that is being generated at both the sides is simple and can be easily generated using the port numbers. The main reason for saying the key as deterministic is that, the key is easily determined easily by both sender and receiver. And the other point is that the key has randomness in it and the is being generated on both sides successfully without the overhead of key distribution.

IV. Conclusion

As with the advancement in the communication technologies there is a need of security and there are many authors that have proposed many ways of providing security but most of them provide the secure way of key distribution. As there is other problem that the key that is being distributed if get to know by the third party then that will lead to the leak of the information. So I am trying in my proposed work to provide the best way of key generation that will provide the security without any overhead of key distribution by adding randomness to the key.

Refrences

[1] M.G. Madiesh, M.L. Mcguire, S.W. Neville,” Secret Key Generation within Peer-to-Peer Network Overlays”, P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2012 Seventh International Conference, PP 156-163, IEEE 2012.

[2] N Khanna, J Nath , J James, S Chakraborty, A Chakrabarti, A Nath, ” New Symmetric key Cryptographic algorithm using combined bit manipulation and MSA encryption algorithm: NJJSAA symmetric key algorithm”, 2011 International Conference on Communication Systems and Network Technologies, pp 125-130, IEEE 2011.

[3] G Ramesh, R Umarani, “UMARAM: A novel fast encryption algorithm for data security in local area network”, pp 758 – 768, IEEE 2010.

[4] Hatem Hamad and Souhir Elkourd,” Data encryption using the dynamic location and speed of mobile node” Journal Media and Communication Studies, Vol. 2(3), pp. 067-075, JMCS 2010.

[5] I Zarei Moghadam, A.S. Rostami, M.R. Tanhatalab,” Designing a random number generator with novel parallel LFSR substructure for key stream ciphers ”, Computer Design and Applications (ICCDA), International Conference, V5-598 - V5-601, IEEE 2010.

[6] T Yao, K Fukui, J Nakashima, T Nakai, “Initial common secret key sharing using random plaintexts for short-range wireless communications ”, vol. 55, pp. 2025 – 2033, IEEE 2009.

[7] Dutta, Chayan,” A New Encryption-Decryption Scheme that Solves Key Management Problem in Remote Sensing Satellite”, Emerging Trends in Engineering and Technology, ICETET '08, pp. 1261 – 1266, IEEE 2008.

[8] William Stallings (2004), "Network Security Essentials (Applications and Standards)", Pearson Education.