ONE TIME PAD ENCRYPTION: A REVIEW

[1]YSR Gayatri, [2]Chandresh Parekh
[1]Scholar, [2]Assistant Professor
[1]Department of IT & Telecommunications,
[1]Raksha Shakti University, Ahmedabad, India

Abstract: With advancement in technology the cryptographic encryption systems are becoming more vulnerable and need for more secure encryptions is rising. This paper reviews one such encryption- One time pad. This paper introduces the one time pad encryption with its history, how it is implemented in general and the security it provides. Based on one time pad encryption's advantages and disadvantages, sustainable solutions are given. Solution is based on generating a truly random number.

***IndexTerms* - Cryptography, encryption, one time pads, true random number.**

I. INTRODUCTION

Cryptography is an art of writing secrets. Everyone has been captivated by the concept of a cipher that is unbreakable. A cipher called poly-alphabetic substitution was invented in 1568 AD by the famous Frenchman B. de Vigenere, in which one single letter of the plain text(PT)/message is replaced in different characters on the basis of a secret key of certain length [1]. This was considered to be unbreakable for a while. Nonetheless, this was in time broken by Charles Babbage in 1854. The exploration for a cipher that is unbreakable was continued till 1949, after that, Shannon provided us a definition for perfect secrecy of message which was mathematically sound [2]. Shannon has used information theory concepts, from which he had developed a systematic mathematical theory of systems secrecy, to be built one year before it was published. He had showed that the encryption using One-Time Pad(OTP), which was invented in 1917, was indeed unbreakable, mathematically [3][4]. The OTP is one of the most simple encryption algorithms. For PTs transformed into binary messages, OTP encryption is achieved by an exclusive-OR operation (XOR) with each bit of the message and the corresponding bit of the OTP (Secret Key). For the OTP to be unbreakable, the private key used should be as long as the message and should be used only once. Thus, the name "One time Pad" came into existence. It is used in cryptographies like DNA, quantum and classical cryptography, whenever the highest form of security is desired [4]. One can say all the modern stream ciphers today are based on OTP.

II. METHODOLOGY

Gilbert Vernam in 1917 invented the electrical One-Time Pad for encryption [5]. It is known to all as Vernam cipher today and the encryption in it is done by the XOR operation of each character in the message with some other character or symbol on a paper tape key. The usage of a pad that is completely random and is not repeating improves the security level of Vernam cipher vastly [8]. Russian agents operating in foreign countries used the OTP extensively. In 1957 a high ranking Russian agent, Rudolph Abel captured in the United States had a postage stamp sized booklet containing a One-Time Pad [9]. The OTP process of encryption and decryption is given below [1]:

1) An OTP is a random set of bits. These are used as an asymmetric key which is known only to sender and receiver who wish to communicate with each other [1].
2) This involves an XOR operation of the message M with the OTP key which yields the cipher-text C [1].
3) The process of decryption involves an XOR operation of C with the OTP key to get back the original message M [1].

III. SECURITY OF OTP

Even though a random private-key that is non-repeating used only once for encryption greatly increases the OTP's security, it was only in 1949 that the basis for this fact was provided by Shannon mathematically [3]. If a cryptanalyst has only the cipher text in his possession (OTP encryption's result) then he cannot do anything better than guessing the message, which can be any binary string of length L. In other words, for him, each and every binary string is equally likely to be the PT [6]. The ambiguity of the PT for the cryptanalyst never reduces with the interception of the cipher text [1]. Thus we can say that cipher text does not leak any information. Results of Shannon imply that for any scheme of encryption, OTP provides the best probable mathematical security [6]. In the past sixty years many cryptographic algorithms have emerged, private-key and public-key algorithms both [6], but none of them could ever offer perfect secrecy even till date. In fact, algorithms accepted by masses such as RSA, ECC, DES and AES have not even been proven to be computationally secure, based on the failure of existing attempts to break them, they are assumed to be hard to break [1]. As rapid developments in quantum computing rise, certainty of these algorithms are questioned, whereas the OTP encryption is supposed to remain immune to any future computing developments [1].

IV. ADVANTAGES AND DISADVANTAGES OF OTP

Advantages:
1) Theoretically perfect secrecy and most optimal cryptosystem
2) Practical method that can be performed even on a paper
3) One Time Pad can be used in Supercomputer

4) This is only encryption scheme that is linked with Quantum Key Distribution.
5) OTP cipher text doesn't provide any info about plain text this makes it unbreakable system
6) Truly Randomness of the Secret key makes the OTP perfectly secure.

Disadvantages:

1) It requires a truly random One Time Pad which is not a small problem considering it has to be implemented practically.
2) The secure creation of a secure pad (which must be as long as the message) and its exchange between users is the most important problem of OTP.
3) OTP requires the unlimited number of random key because it allows one secret key to be used for single time.
4) The security of OTP scheme is only as secure as the security of OTP key.

V. Results and Discussions

The mentioned method addresses the concern of a truly random number and its security. Truly random number should be as long as the PT message and should not be repeated for further encryptions in OTP. These two qualities ensure the security of the message [1].

If the length of PT and the key is same then the intruder needs to perform the attack for each and every bit. This is advantageous because any bit can be the true bit and hence any result he gets can be the correct one. Hence, the security is ensured by keeping key's and message length same [1].

The random number chosen should not be repeated over time or if possible should never be repeated. Intruder can analyze the pattern over which the random number gets repeated and can make a smart guess over time to crack the message. This leaves certain messages vulnerable to attack. If the number is never repeated then the attacker is forever in loop of finding the random number [1].

This truly random one time pad can be achieved by embedding in it atmospheric noise [11], system oscillations [12], date & time and many others, let us call these providers of a true random number. These can be chosen based on the level of security required in a system. One can insert this provider at certain positions in the random number generated where it is not detectable as such by the intruder. Suppose some random number is of length ten then at alternate positions the providers can be embedded, whereas remaining digits in can be generated using any random number generator. Using these addresses both issues of true random number generator as they make sure the random number never gets repeated and the attached random number can be as long as the message without any risk.

Let us consider an easy example. The message is of length thirty; this implies that the key should also be of length 30. Now suppose random number is 727651980535682345892341648970. This number can be repeated anywhere in future as it doesn't contain anything that makes it a true random number. Hence to make it truly random we insert date & time at alternate position which yields 307204762051189809050335126898. Now not only it of same length as the message it also is truly random.

One can use any random number provider based on their needs. We must ensure that it is truly random before using it anywhere in cryptography. After generation of key a major concern in OTP encryption is its distribution which should also be considered and shared securely.

VI. Conclusion

The OTP encryption system has been reviewed. Its disadvantages were recognized and based on these disadvantages a solution to generate truly random number was identified. It is seen that by using a truly random number in OTP, the encryption system becomes very much difficult to break though key distribution remains a concern.

References

[1] Jayashree Katti, Santoshi Pote and B. K. Lande, "Two Level Encryption based on One Time Pad and Koblitz Method of Encoding" in International Journal of Computer Applications (0975 – 8887) Volume 122 – No.15, July 2015
[2] Shannon CE. Communication theory of secrecysystems. Bell Syst Tech J 1949;28:656–715
[3] Shannon CE. A mathematicaltheory of communication. Bell Syst Tech J 1948; 27:379–423
[4] Nithin Nagaraj, "Short communicationOne-Time Pad as a nonlinear dynamical system" Amrita Vishwa Vidyapeetham, Amritapuri Campus, India, Elsevier, http://dx.doi.org/10.1016/j.cnsns.2012.03.020
[5] Menezes A, van Oorschot PC, Vanstone S. Handbook of applied cryptography. Boca Raton, FL: CRC Press; 1996
[6] Nithin Nagaraj and Vivek Vaidya "Re-visiting the One-Time Pad", International Journal of Network Security, Vol.6, No.1, PP.94–102, Jan. 2008
[7] Ms Sunita and Ms Ritu Malik, "Hyper Encryption as an Advancement of one Time Pad an Unbreakable Cryptosystem" in International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X Volume 4, Issue 1, January 2014
[8] Shukla, R. and Prakash, H.O., "Sampurna Suraksha: Unconditionally Secure and Authenticated One Time Pad Cryptosystem", IEEE Conference: International Conference on Machine Intelligence and Research Advancement, 2013, Pages: 174 - 178, DOI: 10.1109/ICMIRA.2013.40
[9] Borowski, M., Lesniewicz, M.,"Modern usage of old one-time pad", IEEE Conference :Communications and Information Systems 2012,Pages: 1 – 5, ISBN: 978-1-4673-1422-0.
[10] https://blog.cloudflare.com/why-randomness-matters/ accessed on 30 April 2018
[11] https://searchsecurity.techtarget.com/definition/one-time-pad accessed on 30 April 2018
[12] M. Bucci, L. Germani and R. Luzzi, "A high-speed oscillator-based truly random number source for cryptographic applications on a smart card IC" in IEEE Transactions on Computers (Volume: 52, Issue: 4, April 2003)