International Journal of Research Instinct
(Peer-reviewed Journal)

ISSN ONLINE 2348-2095
Research Article

Ensuring Data Security by using Quantum Key Distribution in Data Communication

Dr. L. Jayasimman, I.Priya,

[1].Assistant Professor, [2].Research scholar, Department of CS, Srimad Andavan Arts & Science College, (Autonomous)Trichy- 620005.

simmanjaysee@gmail.com,smartmail15@gmail.com

ABSTRACT:

Data security is solitary of the significant aspects of data announcement. The secret data being sent via electrical medium is very susceptible, which can be accessed for malicious purpose. The conservative methods of encryption can only continue the data security so modern cryptography is very greatly needed to improve the data security, so need of mounting new concept and new cryptography is stipulate of the hour. Therefore it is necessary to apply well-organized encryption technique to boost data security. This paper mainly focuses on the dissimilar kind of encryption techniques that existing. For the security of data in communication it uses Quantum key distribution as an encryption technique.

Key words: Data security, Encryption, Multiphase encryptions, multiple encryption.

I.INTRODUCTION

Cryptography is the knowledge of devising methods that allow in sequence to be sent in a secure form in such a way that the only individual able to retrieve this in sequence is the intended recipient [1]. The highly use of set of associations leads to the data switch over the network while communicating to one and another system. While communication it is very important to encrypt the communication so that intruder cannot read the message. Network safety measures

are highly based on cryptography. Cryptography is an art of thrashing information by encrypting the message using algorithms. The cryptography system is a system which carries out encryption and decryption process. The encryption process takes plain text as input and bring into being an output called cipher text using key. The decryption process carries out same as encryption but in turn around order. Cryptography algorithm mostly falls under two categories i.e. Asymmetric and Symmetric encryption techniques. In contemporary times, cryptography is measured a branch of both mathematics and computer science, and is allied closely with in sequence theory, computer safety measures, and manufacturing [2]. A simple text is encrypted by means of an algorithm called "encryption algorithm". A secret message text is decrypted by means of an algorithm called "decryption algorithm". An input is use at the time of encryption and decryption process. The safekeeping level of cryptography is strong-minded by the key space (size of key). This paper holds a number of of the encryption techniques and safety measures issues.

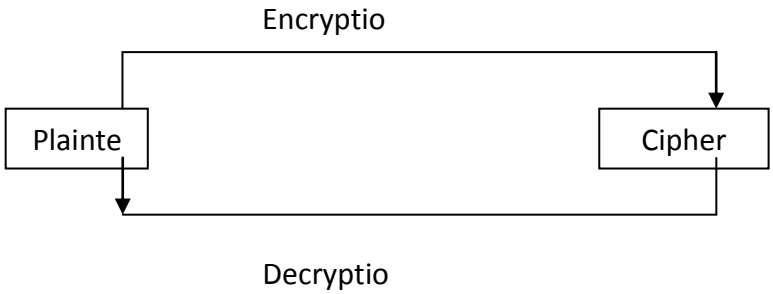

Figure 1. General Cryptography Mechanism

II.CRYPTOGRAPHY GOALS

Cryptography is used to achieve many goals some of the goals are as follows:

1. Authentication: it is a process of giving identity to someone to access particular resource using the keys.

2. Confidentiality: It is most important goal of cryptography, which ensure that nobody understand the message except the one who has the cipher key.

3. Data Integrity: It is the process of ensuring that nobody is allowed to alter the transmitted message except the party who is allowed to do so.

4. Non-Repudiation: Ensure that neither the sender nor the receiver of the message should be allowed to deny the transmission of the message.

5. Access Control: Ensure that only the authorized parties are able to access the transmitted message.

III BASIC TERMINOLOGY USED IN CRYPTOGRAPHY

1. Plain Text: The new message which is to be sent from dispatcher to the beneficiary. This plain text is put as participation at the time of encoding process. For example: if Ram wants to send a text "hello world" to Sohan then it is believe as a plain text.

2. Cipher Text: Secret message text is a text which is being sent from dispatcher to beneficiary and it is not understandable by anybody. It is output of the encryption process. For example: "*@97K&A%L#1" is a secret message is converted into basic text "hello world".

3. Encryption: It is a process of exchange a plain text into secret message by using encoding key and an algorithm known as encryption algorithm.

4. Decryption: It is a process of converting a cipher text into a basic text by using decryption key and an algorithm known as decoding algorithm.

5. Keys: A Key is a numeric or alpha numeric text or may be a particular symbol. The Key is used at the time of encoding takes place on the Plain Text and at the time of decoding takes place on the Cipher Text. The assortment of key in Cryptography is very significant since the safety of encoding algorithm depends directly on it [3].

IV Classification of Cryptography

Cryptography can be divided into two major category based on the use of key.

1. **Symmetric Encryption (Private Key Encryption):** In this type of encryption same key is used at the time of encryption and decryption. The key distribution has to be made before the transmission of the information starts. The key plays a very important role in this type of encryption.

Example: DES, 3DES, BLOWFISH, AES etc.

2. Asymmetric Encryption (Public Key Encryption): In this type of encryption different key is being used for encryption and decryption process. Two different key is generated at once and one key is distributed to other side before the transmission starts.

Example: RSA algorithm.

V BRIEF DESCRIPTION OF MOST COMMONLY USED ALGORITHM

1. **Advance encryption algorithm (AES):** AES algorithm is one of the most widely used encryption algorithm. AES is a block cipher .It has variable key length of 128, 192, or 256 bits; default 256. It encrypts data blocks of 128 bits in 10, 12 and 14 round depending on the key size. AES encryption is fast and flexible; it can be implemented on various platforms especially in small devices [4].

Four different stages are used, one of permutation and three of substitution:

• Substitute bytes: Uses an S-box to perform a byte-by-byte substitution of the block

• Shift Rows: A simple permutation

• Mix Columns: A substitution that makes use of arithmetic over GF(28)

• Add Round Key: A simple bitwise XOR of the current block with a portion of the expanded key.

2. **Data encryption standard (DES):** The initial key consists of 64 bits. However, before the DES process even start, every eight bit of the key is discarded to produce a 56-bit key. DES Encryption is based on the two fundamentals attributes of cryptography: substitution and transportation. DES consists of 16 steps, each of which is considered as round. Each round performs the steps of substitution and transportation as: In the first step, the 64-bit plain text block is handed over to an Initial Permutation (IP) function. The Initial Permutation is performed on plain text. Next, the IP produces two halves of permutated block; say Left Plain Text(LPT) and Right Plain Text(RPT)[4][5]. Then, each LPT and RPT goes through 16 rounds for encryption process. In the end, LPT and RPT are rejoined and a Final Permutation is performed on the combined block and result of this process produce 64-bit cipher.

3. **Triple Data encryption standard (3DES):** 3DES was developed in 1998 and derived for DES. It applies DES encryption 3 times to perform encryption and decryption process is just reverse of encryption process. It uses key length 56*3=168 bits. 3DES encryption can be

performed using either 2 key or 1 key. 3DES encryption follows encrypt-decrypt-encrypt (EDE) sequence.

If 3DES encryption uses two key K1 and K2 respectively then

C = E (K1, D (K2, E (K1, P)))

P = D (K1, E (K2, D (K1, C)))

If 3DES encryption uses one key K1 then

C = E (K1, D (K1, E (K1, P)))

P = D (K1, E (K1, D (K1, C)))

3DES with two key is relatively most popular alternative to DES and has been adopted by for use in the key management standards ANS X9.17 and ISO 8732 [4].

4. Multiphase encryption: Multiphase encryption is a modern encryption technique. Multiphase encryption comprises number of such phases which are strongly protected due to multiple encryption in each phase [2].In multiphase encryption the number of phases can be extent to n number of phase depending upon the type of data and required security.

Example:

Plain text (P): = HELLOWORLD

Algorithm (C): = ((P+1) +3) +2…… (N times)

Cipher Text:

IFMMPXPSME (After first cycle)

LIPPSASVPH (After second cycle)

NKRRUCUXRJ (After third cycle)

…….

…….

Encrypted N Times.

VII LITERATURE SURVEY

Mohammed Abutaha [6] mentioned that the main drawback of symmetric key cryptography is that all social gathering concerned have to swap over the key used to encrypt the data previous to they can decrypt it. This requirement to securely deal out and supervise large numbers of keys means most cryptographic armed forces also make use of other types of

encryption algorithms. Sheltered MIME (S/MIME). For example uses an asymmetric algorithm - public/private key algorithm - for non-repudiation and a symmetric algorithm for well-organized seclusion and data protection. RSA is much slower than symmetric encryption, what characteristically happens is that data is encrypted with a symmetric algorithm and then the moderately short symmetric key is encrypted using RSA.

Yogesh Kumar [7] has done the contrast between DES and AES and establish that DES is faster and AES is Slower, key allocation is difficult in DES and key distribution is easy, complexity of DES is O (Log N) and difficulty of RSA is O (N3), safety measures in DES is reasonable and Security in RSA Height, natural world of DES is closed and Nature of RSA is Open, Secure services in DES is done self-assuredly and protected service in RSA is done Confidentially with honesty and no refutation.

Simar Preet Singh and Raman Maini [8] has done evaluation between algorithms and found that AES shows poor presentation results compared to other algorithms, since it have need of more dispensation power. They also found that 3DES necessitate always more time than DES for the reason that of its triple phase encryption feature.

Shashi Mehrotra Seth and her coworker Rajan Mishra(2011) jointly has complete a Comparative Analysis Of Encryption Algorithms. The investigational results demonstrate the assessment of three algorithm AES, DES and RSA using same passage file for five experiments, productivity byte for AES and DES is same for dissimilar sizes of files. The authors become aware of the RSA has very smaller output byte compared to AES and DES algorithm. Time consumed by RSA algorithm is much advanced compare to the time taken by AES and DES algorithm.

Shashi Mehrotra Seth, 2Rajan Mishra [9] accomplished that reminiscence usage while encryption time differentiation is extremely slight in case of AES algorithm and DES algorithm. RSA munch through longest encryption time and reminiscence usage is also very far above the ground but output byte is least in case of RSA algorithm.

Diaa Salama Abd Elminaam1, Hatem Mohamed Abdual Kader2 [10] have accomplished that RC6 requires less time than all algorithms apart from Blowfish. The AES has an benefit over

other 3DES, DES and RC2 in terms of time consumption and throughput. 3DES has low presentation in terms of power expenditure and throughput when measure up with DES.

Himanshu Gupta and Vinod Kumar Sharma [2] talk about that the source code for multiphase encryption will increase the popularity of Applied Cryptography for the augmentation of data safety measures. At the initial stage, the accomplishment of multiphase encryption may be complex but it will improve the safety measures of data announcement extremely.

Himanshu Gupta and Vinod Kumar Sharma [2] also point out that Multiphase encryption may reduce the predicament of key administration in the existing knowledge of Personal Identity Verification (PIV) due to use of dissimilar encryption algorithms with fixed size keys as an alternative of large numeral of variable length keys.

Himanshu Gupta and Vinod Kumar Sharma [2] completed that Multi-phase Data Encryption illustrates the improved complexity of data encryption due to numerous operations of single phase encryption performance in cryptography and the benefit of numerous encryptions is that it provides better safety measures because even if some constituent ciphers are broken down or some of the top secret keys are documented, the confidentiality of unique data can still be maintain by the several encryptions.

VII. PROPOSED APPROACH:

Quantum Cryptography

The investigate paper meeting point on quantum cryptography, and how this manufacturing helps the system security. The quantum cryptography organization joins a variety of QKD (Quantum Key Distribution) strategies to well-established web innovation to build a protected system. The security of quantum cryptography depends on the sacred laws of quantum technicalities, and the incomprehensibility of faultless cloning of non-orthogonal states put it to somebody the security of this gathering. The quantum cryptography depends on two very important components of quantum mechanics-the Heisenberg Uncertainty standard and the rule of Photon Polarization. The safety measures of quantum cryptography rely on upon the organization of quantum mechanics, and that can modify the system security. The advances in mechanism handling force and the risk of constraint throughout today's cryptography

frameworks will stay behind a main thrust in the carry on with innovative work of quantum cryptography.

Quantum cryptography or quantum key distribution (QKD) applies primary laws of quantum physics to assurance secure announcement. The security of quantum cryptography was proven in the last decade. Many security examinations are based on the assumption that QKD system components are idealized. In practice, inevitable device imperfections may compromise security unless these deficiencies are well investigated. A highly attenuated laser pulsate which gives a weak coherent state is widely used in QKD experiments. A weak coherent state has multi-photon mechanism, which opens up a safety measures loophole to the complicated eavesdropper. With a small adjustment of the hardware, it will prove that the decoy state method can close this loophole and considerably improve the QKD performance. It also proposes a few sensible decoy state protocols, study statistical fluctuations and perform investigational manifestation. Moreover, it will apply the methods from embarrassment distillation protocols based on two-way classical announcement to improve the decoy state QKD performance. Furthermore, we study the decoy state methods for other single photon sources, such as activate parametric down-conversion (PDC) source.

Note that this work, decoy state protocol, has attracted a lot of technical and media interest. The decoy state QKD be converted into a standard technique for prepare-and-measure QKD schemes. Aside from single-photon-based QKD schemes, there is an additional type of scheme based on entwined photon sources. A PDC source is usually used as an entangled photon source. It proposes a model and post-processing scheme for the entanglement-based QKD with a PDC foundation. Although the model is planned to study the entanglement-based QKD, it gives emphasis to that our generic model may also be useful for other non-QKD experiments involving a PDC source. By reproduce a real PDC experiment, it shows that the entanglement-based QKD can accomplish longer maximal secure disinterest than the single-photon-based QKD schemes.

QKD setup

As by pointed out previous, due to the lack of a just right single photon source for BB84, a weak coherent state source is widely used. We call this setup a consistent state QKD implementation. Similarly, perfect single photon detectors are commonly replaced by threshold

detectors. Channel Alice Bob Attn LD PC RNG RNG PC D0 D1 PBS. LD: laser diode; Attn: optical attenuator; RNG: random number generator; PC: polarization controller; PBS: polarization beam splitter; DB0, DB1: single photon detectors.

VIII CONCLUSION

Data safekeeping is one of the significance aspects of communication. Security of data can be attaining using the art of cryptography. There are many algorithms available for cryptography but the selection of one of the most excellent algorithm is also very significant. The algorithm for encryption can be selected based on the type of data being communicated and type of channel through which data is being corresponded. In this paper, it has been investigation that the presented moving parts on the encryption techniques. Those encryption techniques are investigated well to improve the data safekeeping. As the day passes modern encryption is needed to encourage the data security. The study of multiphase encryption method enhances the data security but multiphase method must also be reviewed for safekeeping purpose.

IX REFERENCES

[1] Y.Wang and M. Hu, ―Timing - evaluation of the known cryptographic algorithms, in proc. International Conference on Computational Intelligence and Security, Beijing, China Dec 2009.

[2] International Journal of Computer Theory and Engineering, Vol. 5, No. 4, August 2013 Multiphase Encryption: A New Concept in Modern Cryptography by Himanshu Gupta and Vinod Kumar Sharma.

[3] International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 7, July 2012 A Survey on Various Most Common Encryption Techniques by E.Thambiraja, G. Ramesh and Dr. R. Umarani.

[4] W.Stallings, "Cryptography and Network Security 4th Ed," Prentice Hall, 2005.

[5] Coppersmith, D. "The Data Encryption Standard (DES) and Its Strength against Attacks."IBM Journal of Research and Development, May 1994, pp. 243 -250.

[6] Mohammed Abutaha, Mousa Farajallah, Radwan Tahboub & Mohammad Odeh Survey Paper: Cryptography Is The Science Of Information Security International Journal of Computer Science and Security (IJCSS), Volume (5): Issue (3): 2011 298

[7] IJCSMS International Journal of Computer Science and Management Studies, Vol. 11, Issue 03, Oct 2011 Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures by Yogesh Kumar1, Rajiv Munjal2, Harsh Sharma3

[8] Simar Preet Singh, and Raman Maini "COMPARISON OF DATA ENCRYPTION ALGORITHMS" International Journal of Computer Science and Communication Vol. 2, No. 1, January-June 2011, pp. 125-127

[9] Shashi Mehrotra Seth, 2Rajan Mishra," Comparative Analysis of Encryption Algorithms for Data Communication", IJCST Vol. 2, Issue 2, June 2011 pp.192-192.

[10] Diaa Salama Abd Elminaam1, Hatem Mohamed Abdual Kader2, and Mohiy Mohamed Hadhoud2," Evaluating The Performance of Symmetric Encryption Algorithms", International Journal of Network Security, Vol.10, No.3, PP.213-219, May 2010.