DOI: http://dx.doi.org/10.26483/ijarcs.v8i7.4284

ISSN No. 0976-5697

Volume 8, No. 7, July – August 2017

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

AN APPROACH TO REVAMP THE DATA SECURITY USING CRYPTOGRAPHIC TECHNIQUES

Chakshu Diwan, Dr. Sunil K Singh
Chandigarh College of Engineering and Technology,
Degree Wing, Chandigarh, India

Abstract— In this rapidly changing world where the need of digital storage is multiplying, where advance requirement is securing the data, so that the data should reach to the designated user. Cryptography plays the crucial role on ensuring the information security and authenticity of modernized computer systems. Information Security is a challenging issue of data communication today that is handling different areas including secure communication channel, robust data encryption technique to maintain the database. The confidential data could be accessed by the unauthorized user for ill-natured objective. So, it is mandatory to apply effective encryption and decryption methods to reinforce data security. In this review paper, various cryptographic techniques, like Rivest-Shamir-Adleman (RSA), Diffie-Hellman Key Exchange, Elliptic curve cryptography (ECC), Quantum Key Distribution (QKD) and Hybrid Cryptography are observed. By enhancing abstract, we address the problem of determining and concluding security and also the future of encryption in a context where the database of the user must be protected.

Keywords—cryptography, information security, data communication, encryption, unauthorized, decryption

I. INTRODUCTION

Cryptography facilitates the user to transmit the secure information across any troubled network so that it cannot be used by an unauthorized party. Cryptography is the mechanism that involves encryption and decryption of text using numerous breakthroughs. Encryption means the technique of converting the plain text into an incomprehensible form called a cipher text [1]. This cryptic form cannot be easily understood by an unauthorized party and sent across the insecure media. Decryption means the technique of converting this incomprehensible form back into its authentic form, so that it can be easily understood by the designated recipient. Database protection relies on various approach and techniques, which includes access control, network security, authentication of user and data, encryption, digital signatures, and some other cryptographic methods [2]. It sounds great to develop a logical understanding of database security problems and their explanations and to turn up with a skeleton structure. Cryptography classified as Symmetric cryptography and Asymmetric cryptography techniques. Authorizing the two persons, to convey the information in a way that an intruder cannot understand the shared info of what is being transferred is the fundamental aim of cryptography. This is usually done for secrecy, and typically for private communications.

II. SECURITY SERVICES OF CRYPTOGRAPHY

There is an urge of providing security to ensure that data remains private and only accessible to authorized party and insure that no violator is able to switch the information, so it provide full precision. The essential part of cryptography is to provide the four rudimentary data security services.

A. CONFIDENTIALITY

The basic security service which is catered by cryptography is confidentiality. This assistance helps in keeping the information secured from an unauthorized party. Secrecy is the other name for confidentiality. It can be accomplished through many ways starting from securing the information through physical means to come up with the usage of mathematical mechanisms for encoding.

B. DATA INTEGRITY

Data Integrity is the security service which is concerned with identifying any variation to the information. The information might get modified by an unauthorized party. It cannot help in preventing the alteration of information, but can provide with a way for detecting whether information has been modified in an illegitimate manner. Manipulating the transmitted information is only allowed to the authorized user.

C. AUTHENTICATION

Authentication provides the identification of the prime. The data acquired by the system checks the authenticity of the sender that whether the data turned up from an authorized person or an illegitimate entity.

D. NON-REPUDIATION

Non-repudiation is a security service, type of an assurance where the sender of the information is not in a situation to decline at a later stage his or her intentions in the transporting of the information. For example, if non-repudiation service is enabled in the transaction and an order is once placed electronically, a user cannot decline the purchased order.

III. CRYPTOGRAPHY

The skill of secret writing is termed as cryptography. A secret approach of writing is cipher code; where by clear

text gets converted into the ciphertext. This process of conversion where the plaintext gets converted into ciphertext is called encryption. The technique of converting ciphertext back to the plaintext is called decryption. These two techniques namely, encryption and decryption are regulated by cryptographic keys.

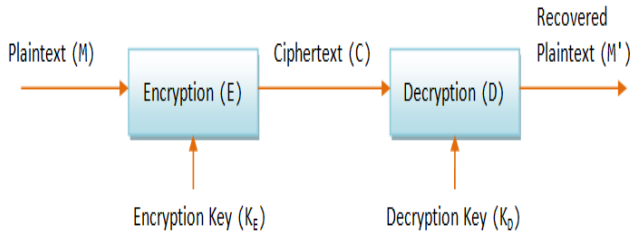

Figure 1: Cryptographic Process

Fig 1: demonstrate the cryptographic process where M stands for Plaintext, C stands for Ciphertext, E stands for Encryption & D stands for Decryption.

A. CRYPTOSYSTEMS

Cryptosystem is comprised of cryptographic algorithms, plaintext, ciphertext, and keys. It performs with the combo of keys and algorithm to encipher the plaintext and to decipher the ciphertext. A cryptosystem is one of the application of cryptographic techniques and their lead support to cater information security services [3]. Cipher system is the other name of cryptosystem. The primary objective of cryptosystem is that eventually at the end of the mechanism, the plaintext will only be understood by the sender and receiver. Essentially, there are two categories of cryptosystems which are based on the research in which encryption-decryption is performed out in the system.

1) SYMMETRIC KEY ENCRYPTION

Symmetric key encryption is a technique where the same keys are affiliate for encrypting the plaintext and decrypting the ciphertext. Symmetric cryptosystems adapt the symmetric-key algorithms technique referred to as symmetric cryptography. Secret key cryptosystems is the other name called to symmetric cryptosystems.

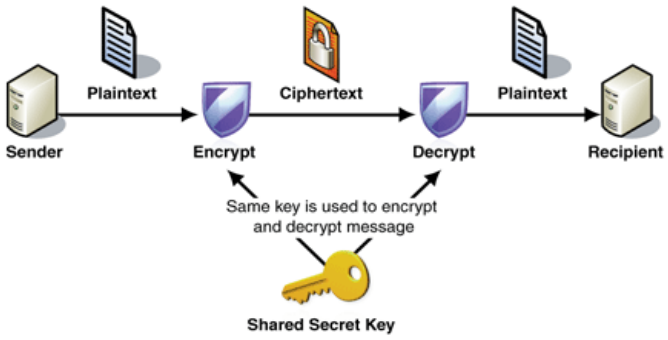

Figure 2: Symmetric Key Encryption Process

2) ASYMMETRIC KEY ENCRYPTION

Asymmetric key encryption is a technique where the different keys are affiliated for encrypting the plaintext and decrypting the ciphertext. This kind of encryption uses dissimilar keys namely, private and public key to encrypt and decrypt the information. Asymmetric-key encryption is also known as public key encryption.

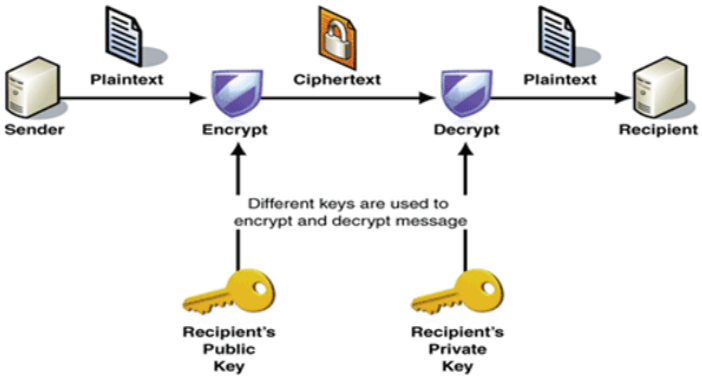

Figure 3: Asymmetric Key Encryption Process

IV. CRYPTOGRAPHIC TECHNIQUES

A. DATA ENCRYPTION STANDARD (DES)

The Data Encryption Standard is a block cipher. It helps in encrypting the data in a block which is of 64 bits and thus it produces the 64-bit. The key length available is 56 bits. At initial level, the key consists of 64 bits. DES is widely used by the financial services and the other industries worldwide to protect sensitive online applications [4].

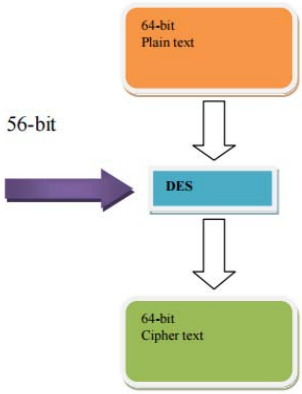

Figure 4: The conceptual working with DES

B. TRIPLE DES

Triple Data Encryption Algorithm is simply three successive encryptions with DES. It is possible to use either two or three distinct keys with 3DES. Thus, for the three-key case, one obtains the benefit of a 168-bit key space with the known strength of the DES algorithm. Performed correctly, 3DES is as unbreakable a secret-key algorithm [5]. Moreover, Triple DES systems are significantly more secure than single DES, but these are clearly a much slower process than encryption using single DES.

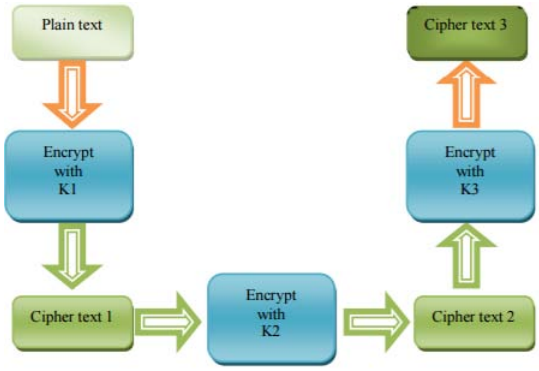

Figure 5: Encryption process Triple DES with three keys K1, K2 and K3

C. AES

Advanced Encryption Standard (AES) is the current standard for secret key encryption. AES was created to replace the old Data Encryption Standard (DES) method. The algorithm is referred to as AES-128, AES-192, or AES-256, depending on the key length. During encryption decryption process, AES system goes through 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys in order to deliver final cipher-text or to retrieve the original plain-text. It was successful because it was easy to implement and could run in a reasonable amount of time on a regular computer [6].

D. ONE-TIME-PAD

The one-time pad, also called Vernam Cipher, is implemented using a random set of non-repeating characters as the input cipher text. The Vernam Cipher is used one-time pad, which is discarded after a single use, and therefore suitable only for short messages. The Vernam Cipher was first implemented with the help of a device called Vernam machine. The one-time pad is typically implemented by using a modular addition (XOR) to combine plaintext elements with key elements [7].

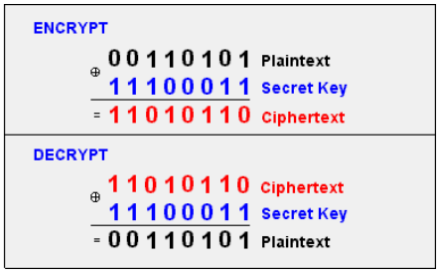

Figure 6: One-Time pad implementation using modular addition

E. RSA Encryption

RSA is designed by Ron Rivest, Adi Shamir, and Leonard Adleman in 1978. It is one of the best known public key cryptosystems for key exchange or digital signatures or encryption of blocks of data. RSA uses a variable size encryption block and a variable size key. It is an asymmetric (public key) cryptosystem based on number theory, which is a block cipher system. It uses two prime numbers to generate the public and private keys. These two different keys are used for encryption and decryption purpose. Sender encrypts the message using Receiver public key and when the message gets transmit to receiver, then receiver can decrypt it using his own private key [8,9]. RSA Encryption is the most widely used asymmetric key encryption system used for electronic commerce protocols.

F. Diffie-Hellman Key Exchange

The Diffie-Hellman Key Exchange is a cryptographic protocol that allows two parties with no prior knowledge of each other to establish a shared secret key, which typically is used in symmetric key cipher [10]. The Diffie-Hellman Key Exchange relies on exponential functions computing much faster than discrete logarithms. When used properly, the Diffie-Hellman Key Exchange protocol gives two parties the same key without transmitting it. The strength of this algorithm depends on the time it takes to compute a discrete logarithm of the public keys transmitted.

G. DSA – Digital Signature Algorithm

In many digital communications, it is desirable to exchange an encrypted message than plaintext to achieve confidentiality. There are two possibilities, sign-then-encrypt and encrypt-then-sign. However, the crypto system based on sign-then-encrypt can be exploited by receiver to spoof identity of sender and sent that data to third party. Hence, this method is not preferred. The process of encrypt-then-sign is more reliable and widely adopted. Digital signatures may also be generated for stored data and programs so that the integrity of the data and programs may be validate at any later time [11].

V. THE FUTURE OF ENCRYPTION

A. Elliptic Curve Cryptography (ECC)

Elliptic curve cryptography is a newer approach to public-key cryptography that is based on the algebraic structure of elliptic curves over finite fields. It requires smaller keys as compared to non-ECC cryptographic techniques to provide the same security. In ECC 160-bit key provides the equivalent security as compared to the traditional crypto systems like RSA with a 1024-bit key, thus which lowers the computer power. Therefore, ECC offers security at great extent for a given key size. Consequently, key with the smaller size makes it possible and more compact implementations for a given level of security, which means faster cryptographic operations, run on smaller chips or more compact software. Further, there are truly efficient, compact hardware implementations are there available for ECC exponentiation operations, that offers potential reductions in implementation footprint even beyond those because of the smaller key length. This technique is not only emerged as an appealing public key crypto-system for mobile and wireless environments but also helps in providing bandwidth savings [15]. Elliptic Curve Cryptography algorithm is also suitable for smart card application, as it is faster and occupies less

memory than RSA. Elliptic curve cryptography is difficult to understand by the attacker and therefore not easy to break.

B. Quantum Key Distribution (QKD)

Quantum cryptography provides a cryptographic result which is long-lasting as it renders prime secrecy that is applied to quantum public key distribution. It is a technology wherein two parties can communicate securely with the sights of quantum physics. In classical cryptography, information is encoded with the help pf bits whereas quantum cryptography i.e. quantum computer uses quantum particles or photons and photon's polarization which is their quantized properties to encode the information. This is represented in qubits which is the unit for quantum cryptography [13]. The transmissions are secure as it is depended on the inalienable quantum mechanics laws. QKD could very well be the future of unbreakable encryption.

C. Hybrid Cryptography

A method of encryption that combines two or more encryption strategies and includes a combination of symmetric and asymmetric encryption to take advantage of the strengths of each type of encryption is known as Hybrid Encryption. A hybrid cryptosystem is a protocol using multiple ciphers of different types together, each to its best advantage. One common approach is to generate a random secret key for a symmetric cipher, and then encrypt this key via an asymmetric cipher using the recipient's public key. The message itself is then encrypted using the symmetric cipher and the secret key. Both the encrypted secret key and the encrypted message are then sent to the recipient [14]. The recipient decrypts the secret key first, using his/her own private key, and then uses that key to decrypt the message. DES and RSA hybrid cryptographic algorithm is relatively more reliable and secure.

VI. CONCLUSION AND FUTURE DIRECTIONS

In this paper, evaluation of basic information about cryptographic techniques are observed. For data and information security, different cryptographic techniques are used. This paper outlines the cryptographic belief of key encryption for sending confidential data and key decryption for receiving it. These techniques will be helpful in such applications where privacy, authentication and integrity, all are supreme demands.

VII. ACKNOWLEDGMENT

I would like to thank my mentor Dr. Sunil Kumar Singh, HOD of Computer Science Department for his full support and motivation. I sincerely thank to all my teachers who have guided and provided expertise in this paper. I also wish to express my gratitude to all people who rendered their help to fulfill my task.

VIII. REFERENCES

[1]. SuyashVerma, RajnishChoubey, Roopalisoni “An Efficient Developed New Symmetric Key Cryptography Algorithm for Information Security” International Journal of Emerging Technology and Advanced Engineering Volume 2, Issue 7, July 2012.

[2]. S. Castano, M. Fugini, G. Martella, and P. Samarati, Database Security, Addison-Wesley, 1995.

[3]. Dr. L. Arockiam, S. Monikandan, “AROcrypt: A Confidentiality Technique for Securing Enterprise’s Data in Cloud”, International Journal of Engineering and Technology, ISSN: 0975-4024, Volume 7, Issue 1, February-March 2015, pp. 245-253.

[4]. Wuling Ren, "A Hybrid Encryption Algorithm Based on DES and RSA in Bluetooth Communication”, Second International Conference on Modeling", Simulation and Visualization Methods (WMSVM), 2010.

[5]. Grabbe J, Data Encryption Standard: The Triple DES algorithm illustrated Laissez faire city time, Volume: 2, No. 28, and 2003.

[6]. Chih-Pin Su, Tsung-Fu Lin, Chih-Tsun Huang, and Cheng-Wen Wu, National Tsing Hua University,” A high throughput low cost AES processor” IEEE Communications Magazine 0163-68 04/03 2003.

[7]. Nithin Nagaraj, “Short communication One-Time Pad as a nonlinear dynamical system” Amrita Vishwa Vidyapeetham, Amritapuri Campus, India, Elsevier

[8]. Aman Kumar, Dr. Sudesh Jakhar and Mr. Sunil Makkar, "Comparative Analysis between DES and RSA Algorithm’s", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7, pp. 386-391, July 2012.

[9]. Xin Zhou and Xiaofei Tang, "Research and Implementation of RSA Algorithm for Encryption and Decryption", the 6th International Forum on Strategic Technology, pp. 1118 – 1121, 2011.

[10]. Simon Blake Wilson et al., “Key agreement protocols and their security analysis,” 9-sep- 1997.

[11]. Erfaneh Noorouzil et al, “A New Digital Signature Algorithm”, International Conference on Machine Learning and Computing, IPCSIT vol.3, 2011.

[12]. Robert Zuccherato, “Elliptic Curve Cryptography Support in Entrust,” Entrust ltd. in Canada, Dated: 9-may-2000.

[13]. Othman O. Khalifa, “Communication Cryptography”, IEEE transaction on Cryptography, 2004, pp. 1-15.

[14]. Meenakshi Shankar and Akshaya.P, Hybrid Cryptographic Technique Using RSA Algorithm and Scheduling Concepts, International Journal of Network Security & Its Applications (IJNSA) Vol.6, No.6, November 2014.

[15]. SK Singh, A Kumar, S Gupta, R Madan, Architectural performance of WiMAX over WiFi with reliable QoS over wireless communication, International Journal of Advanced Networking and Applications (IJANA), Volume: 03, Issue: 01, pp1017-1024, 2011.