Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 9, September 2014, pg.482 – 488

RESEARCH ARTICLE

A Study on Cryptography Aspects and Approaches

Shivani[1], Mamta Sachdeva[2]

Student, MTech (CSE)
South Point Institute of Technology & Management, Sonepat, Haryana
nirun788@gmail.com

Associate Professor, Department of Computer Science
South Point Institute of Technology & Management, Sonepat, Haryana
get_mamta@rediffmail.com

Abstract— Cryptography is one of the effective tool to provide the secure information transmission over the public channel. To perform the effective and secure information transmission, it is required to identify the requirement and the relative approaches to obtain the security features during transmission. In this work, a study based work is defined on cryptography process. The paper has defined the requirement of information security and its association with cryptography process. The paper also discussed the different cryptography approaches along with adapted procedures.

Keywords- Symmetric Key, Authentification, Encryption, Integrity

I. INTRODUCTION

To provide the effective communication over the public network, there is the requirement of some secure means to provide reliable communication. To provide the information security over open channel, confidentiality and data integrity are the basic requirement to save data from unauthorized access. There are number of associated approaches to provide this secure communication. These approaches include cryptography and steganography methods. Cryptography is about to encode the information data from one form to other so that it will not get recognized by unauthorized person. Steganography is the approach that actually hides the information behind other media type such as image, video audio etc. This paper is focused on the cryptography process and the relative approaches study. To understand the necessity of cryptography approaches, there pillars of secure communication are discussed here. These three pillars are privacy, integrity and the authentication. In this section, these three pillars are explained in detail.

A) Privacy

The privacy is about to provide the information communication in such way, only the sender and receiver can understand the conversation. If some intruder wants to eavesdrops the communication, he must be unable to sense it. Cryptography is able to provide such secure communication. Cryptography is a key based approach in which only the person having the authenticated key can extract the actual information from the encoded data. This authorization level can also be defined under different kind of key specification. These key specifications include the private key, public key and group key based concepts. The private key is the simplest form of cryptography in which single key is used for encoding and decoding process. In case of public key cryptography, different keys are used for encryption and decryption. In case of group key, two or more persons can encode or decode the information. In case of shared information communication, group key concept is used.

B) Integrity

Integrity is another required property of secure communication between two or more parties. Integrity actually defines the verification process performed by the receiver side to check whether the information is sent by the particular sender or not. If the sender is verified, it is also identified that there is no malicious message communicated by the sender. Integrity is about the verification that no third party or the unauthenticated party is involved in the communication. In the cryptography process, to achieve the integrity, the sender identity mark is also included with information message.

C) Authentication

A secure communication should ensure that the parties involved in the communication are who they claim to be. In other words, we should be protected from malicious users who try to *impersonate* one of the parties in the secure conversation. Again, this is relatively easy to do with some network sniffing tools. However, modern encryption algorithms also protect against this kind of attacks.

Cryptography process actually combines all the three types of information security. The encryption process converts the information text to some unreadable format that can be extracted back to the original form only by using the respective decryption algorithm. This decoding process is generally the reverse process of encoded form. There are number of different kind of cryptography approaches. These cryptography approaches are shown in figure 1.

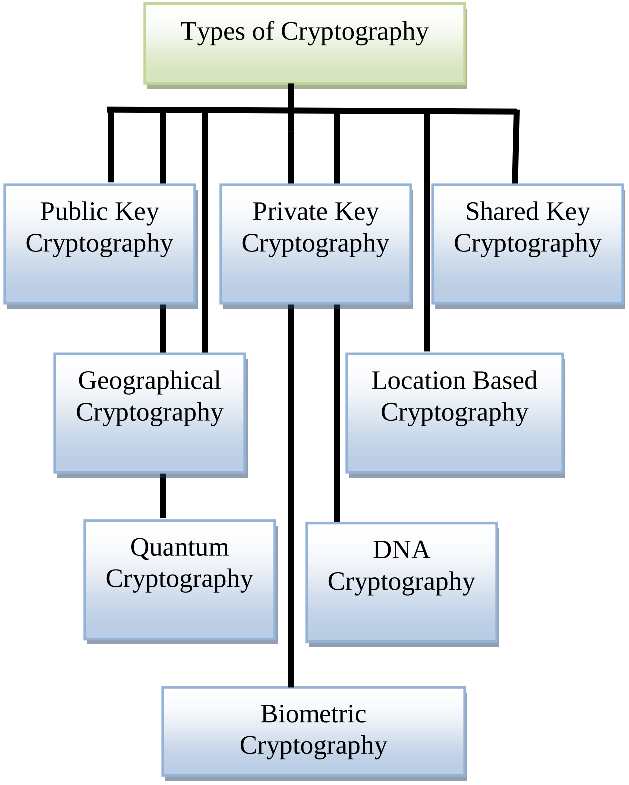


Figure 1 : Types of Cryptography

In this paper, a study on different cryptography approaches is defined. In section I, the study on different features of cryptography algorithms is defined. The section has explored the cryptography process along with encryption methods. In section II, the work defined by earlier researchers is discussed. In section III, the study on different cryptography algorithms is defined. In section IV, the conclusion and results associated with work are explored.

II. RELATED WORK

Parisa Kaghazgaran[3] presented a work to provide the information security in case of involvement of more than one party in encryption process. Author defined the variant of comparison problem under different input. Author presented the work in real time situations where the cryptography is required. Author presented the cryptography at protocol level and provides the comparative analysis on existing and modified secure protocol approach for data encoding. Author enabled the secure transmission over the network. Ohood S. Althobaiti[1], discuss the relationship between cryptography and mathematics in the context of Elliptic Curve (EC). Author presents the idea of biometric signature - a new method to combine biometrics with public key infrastructure (PKI), the security can be increased using the ECC in biometric signature creation, because the private and public keys are produced without saving and sending any secret information anywhere. Another work on visual information cryptography using the DH scheme was proposed by Chao-Wen[5] in year 2008. Author presented an improved mechanism based diffie helman approach for visual cryptography approach. Author used a shared key mechanism using visual cryptography. Author used the half tone shadow images to show the work implementation. Author implemented the work using shared key and symmetric key approaches to achieve high level security.

Another work on block cipher cryptography and white box cryptography to secure the data was performed by Jaesung Yoo in year 2012. In this paper, Author implemented an improved AES for image encryption by using the dynamic key updation approach. Author adopted composite mode using White-Box AES and Standard AES. Presented scheme shows almost same performance with Standard AES and provides dynamic key approach effect. Moreover, it has a CPA-secure property and can be constructed for CCA-secure scheme with Message Authentication Code [6]. Trisha Chatterjee presented a work on the cryptographic algorithms for symmetric key cryptography. Author provided more secure approaches by modifying the existing symmetric key cryptography approaches. The modification is here done at cipher text generation. Author provided the new algorithm to provide the text based encoding at the frequency level analysis. Author enabled the ASCII character encoding to perform the cryptography and to convert the information one form to other. This cryptography approach is based on random key generation [4].Wasim A Al-Hamdani defined a work on Elliptic Curve Cryptography to protect the data. Author defined a public key based approach under the algebraic structure. This was performed on a smaller group can be used to obtain the same level of security as RSA based. In this article a simple presentation on cryptography with focus on elliptic curve algorithm, examine its security, benefits and its functions with privacy issues [7]. A work on identity based cryptography was performed on symmetric cipher cryptography by Joonsang Baek. In this paper, as contributions to this line of research, Author construct hybrid identity-based encryption schemes which produce compact cipher texts while providing both efficiency and strong security without resorting to the strong length preserving symmetric cipher. In this paper, author defined a comparative analysis under different communication attacks to reveal the communication information and to extract the user data under different assumptions. Author provided the symmetric key encryption under improved form [8]. In Year 2012, Seny Kamara defined a work on Symmetric encryption using dynamic searchable technique. The presented approach allows a client to encrypt the data in such way the search can over the data can be performed over it. Author has defined SSE based scheme to satisfy the search condition. The work presented by the author actually extends the inverted index approach in different non-trivial ways and also introduce new technique to design the SSE. Author implemented the presented scheme and conducts the performance evaluation. The presented approach is highly efficient and ready for the deployment [2].

Ralf Kusters[9] performed a work," Computational Soundness for Key Exchange Protocols with Symmetric Encryption". In this paper, Author show the first general computational soundness result for key exchange protocols with symmetric encryption, along the lines of a paper by Canetti and Herzog on protocols with public-key encryption. In this paper, Author presented an improved mechanism for key sharing over the network. Author defined a new improved protocol to enable the public key cryptography and to provide the secure key sharing over the network. Ueli Maurer[12] performed a work," On the Soundness of Authenticate-then-Encrypt- Formalizing the Malleability of Symmetric Encryption". Author highlight two reasons for investigating nevertheless AtE as a general paradigm: First, this calls for a definition of confidentiality; what separates a confidential from a secure channel is its (potential) malleability. Author proposes the first systematic analysis of malleability for symmetric encryption, which, in particular, allows us to state a generic condition on encryption schemes to be sufficient for AtE. Second, AtE is used in practice, for example in TLS. Author shows that the schemes used in TLS (stream ciphers and CBC encryption) satisfy the condition.

III. CRYPTOGRAPHY APPROACHES

In case of electronic data communication the requirement of such cryptographic approach is more critical. Different kind of secure communication or digital transaction increased the need of cryptography approaches. Such as credit card payments, e transactions require more concern of user to use the secure communication. Today emails and SMS are also communicated in secure way. Many of the service provide also available web information security in secure means and present the information under the trust level. A trustful communication medium is more reliable to provide the effective communication over the network. This kind of secure communication is not only required for public networks but while performing the offline data transmission, the cryptography approaches are more beneficial. These approaches also secure the information from social hacking or the attack done by some known person.

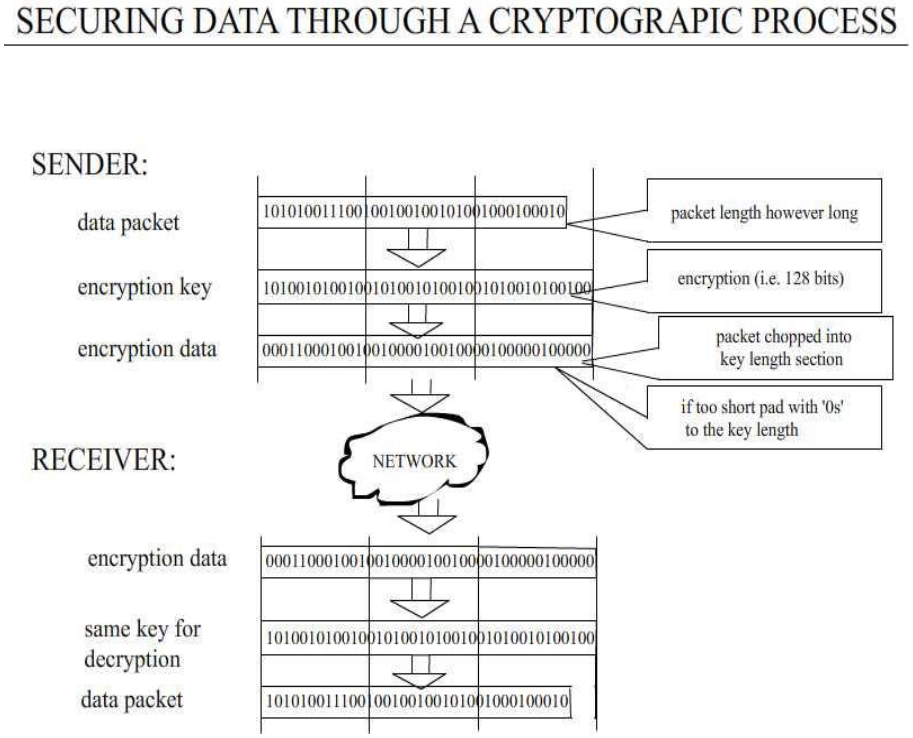


Figure 2: Cryptography Process

Here to secure the information, the cryptography mechanism basically requires two main components called cryptographic algorithm and the secure key. Cryptographic algorithm is the approach applied to encode the information and the key is the actual password information used by the sender to encode the information. A cryptography algorithm accepts the raw textual information and the sender key as input and performs the encoding

A) Symmetric Cryptography

This kind of cryptography approach is also called private key cryptography. As the name suggested in this cryptography approach only single key is involved to enable the encoding and decoding process. It means same key is used to perform data encryption and to retrieve the data back from cipher text [10]. At the earlier stage, this kind of cryptography not looks stronger as the complete security depends on single key. But there are number of cryptography algorithms comes under symmetric key cryptography that increases the data integrity by using the larger key size and number of encoding level in the algorithmic approach [9]. This is the most traditional type of cryptography, in which the key information is common for both sender and receiver. In such system, the sharing mechanism of key requires some effective approach. Single key is here defined to perform data encoding and decoding. This single key is able to provide the reliable communication over the network [2][4][8][9].

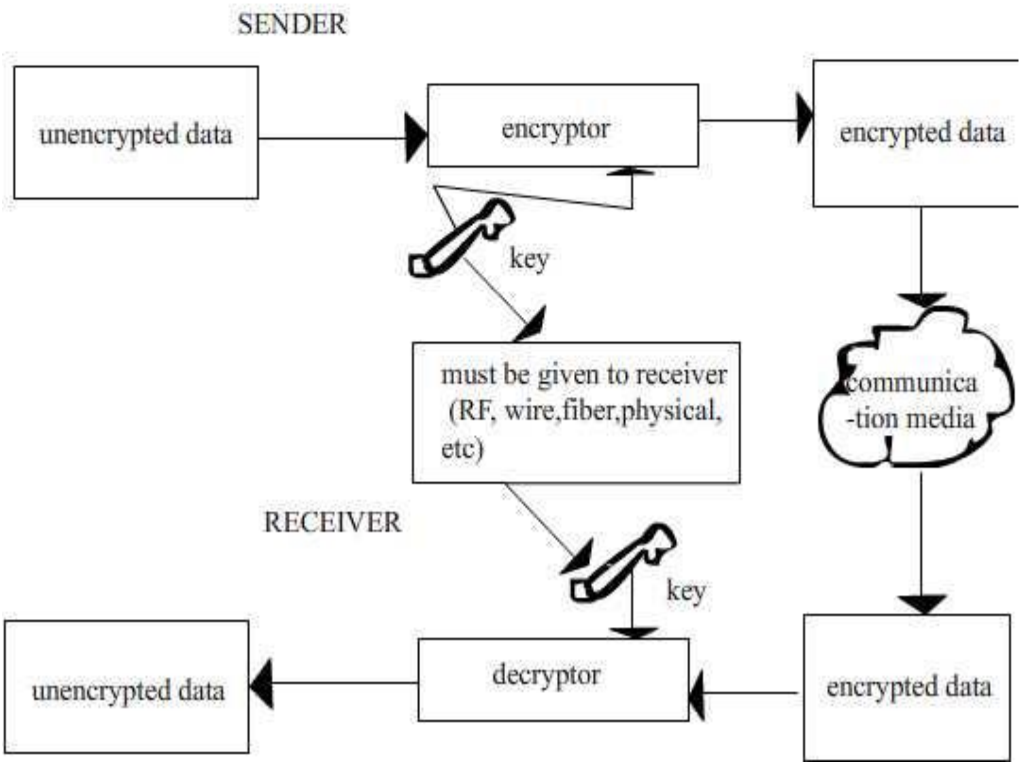
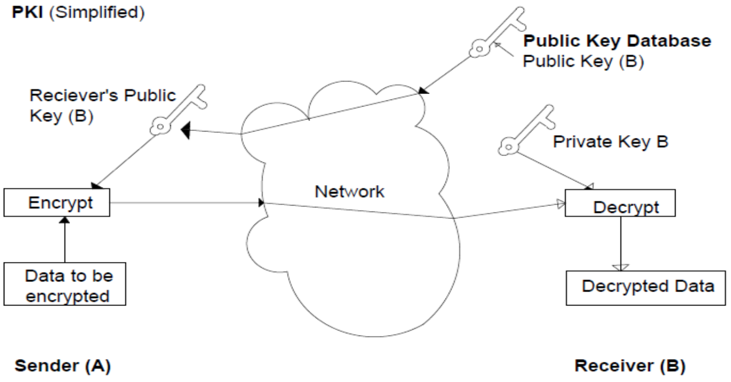


Figure 3 : Symmetric Key Cryptography

As figure shows, the sender is having the raw information to transfer over the network. This raw information can be available in different media types. These media types can be textual information, image, videos etc. To perform the cryptography, the approach requires some algorithm called encryptor and the key. This key is symmetric key shared between the senders as the receiver [6]. The security of this kind of algorithm depends on three main vectors called cryptography algorithm, key size and way to share the key [2]. There are number of symmetric key cryptography algorithms such as DES (Digital Encryption Standard), Triple DES, AES (Advanced Encryption Standard) etc. This algorithm provides the high level information security.

B) Public Key Cryptography

This cryptography approach is also called asymmetric cryptography approach. According to this approach, encryption and decryption is performed by two different



Usable mainly for relatively low data rates because asymmetric cryptography is math intensive which slows down the pipe

Figure 4 : Public Key Cryptography

keys. As the encryption process begins, instead of generating single key, two keys are generated called Public key and Private Key [1]. The generator A keeps the private key with him and distributes the public key to all users that can send information to it. Now, as some user B want to send information to the user A. In such case, user B will use the public key of User A to perform the encoding process. Here the cryptography will be performed using public key of receiver. Now after the encoded process, the cipher information is transferred to the receiver A [4]. As receiver receives this information, the decoding process is performed using private key of User A. This decoding process is able to get the information back in its original form

IV. CONCLUSION

One of the major aspect of information security is represented by cryptographic approaches. In this paper, the exploration to the available cryptographic approaches is defined. The paper has explored main cryptographic approaches called public key and private key cryptography.

REFERENCES

[1] Ohood S. Althobaiti, *An Enhanced Elliptic Curve Cryptography for Biometric*, 7th International Conference on Computing and Convergence Technology (ICCCT), pp 1048–1055, 2012.

[2] Seny Kamara, *Dynamic Searchable Symmetric Encryption*, CCS'12, October 16–18, 2012, Raleigh, North Carolina, USA. ACM 978-1-4503-1651-4/12/10 (pp 965-976).

[3] Parisa Kaghazgaran, *Secure Two Party Comparison over Encrypted Data*, World Congress on Information and Communication Technologies, pp 1127-1130, 2011.

[4] Trisha Chatterjee, *Symmetric key Cryptosystem using combined Cryptographic algorithms - Generalized modified Vernam Cipher method, MSA method and NJJSAA method: TTJSA algorithm*, Information and Communication Technologies (WICT), pp 1179, 2011.

[5] Chao-Wen Chan, *A Visual Information Encryption Scheme Based on Visual Cryptography and D-H Key Agreement Scheme*, IJCSNS International Journal of Computer Science and Network Security, Vol.8 Issue.4, pp 128-132, April 2008.

[6] Jaesung Yoo, *A Method for Secure and Efficient Block Cipher using White-Box Cryptography*, Proceedings of the 6th International Conference on Ubiquitous Information Management and Communication, 2012.

[7] Wasim A Al-Hamdani, *Elliptic Curve for Data protection*, Proceedings of the 2011 Information Security Curriculum Development Conference, pp 1-14, 2011.

[8] Joonsang Baek, *Compact Identity-Based Encryption without Strong Symmetric Cipher*, Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, pp 61-70, 2011.

[9] Ralf Kusters, *Computational Soundness for Key Exchange Protocols with Symmetric Encryption*, Proceedings of the 16th ACM conference on Computer and communications security, pp 91-100, 2009.

[10] Craig Gentry, *Fully Homomorphic Encryption Using Ideal Lattices*,, Proceedings of the 41st annual ACM symposium on Theory of computing, pp 169-178, 2009.

[11] Giuseppe Ateniese, *Provably-Secure Time-Bound Hierarchical Key Assignment Schemes*, International Association for Cryptologic Research, pp 288-297, 2006.

[12] Ueli Maurer, *On the Soundness of Authenticate-then-Encrypt- Formalizing the Malleability of Symmetric Encryption*, Proceedings of the 17th ACM conference on Computer and communications security, pp 505-515, Oct 2010.