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
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 8, August 2016, pg.55 – 59

A SURVEY PAPER ON CRYPTOGRAPHY TECHNIQUES

A. Joseph Amalraj[1], Dr. J. John Raybin Jose[2]

[1]Research Scholar, Computer Science, Bishop Heber College, Tiruchirapalli, Tamil Nadu, India
[2]Head, Department of Information Technology, Bishop Heber College, Tiruchirapalli, Tamil Nadu, India
[1] softwarejoseph@gmail.com , [2] johnraybinjose@gmail.com

ABSTRACT— In the modern era evaluation of networking and wireless networks has come in information and communication technology, there are so many things that gives facility to deal with these technology using internet. In internet email security is main aspect and the process of cryptography plays an important role to provide the security to the networks. To improve security and efficiency, most email system adopt Public Key Infrastructure (PKI) as the mechanism to implement security, but public key infrastructure based systems suffer from expensive certificate management and problems in scalability. The main objective of this approach is awareness of email security and its requirements to the common computer users. A number of cryptographic techniques are developed for achieving secure communication. The proposed mailing system is secure against standard security model.

Keywords— Encryption, Decryption, Computer Security, Cryptography, DES, AES, Blowfish, RSA, CL-PKC, Securing Data, Hacking.

I. INTRODUCTION

Today's our entire globe is depending on internet and its application for their every part of life. Here comes the requirement of securing our data by ways of Cryptography. Cryptography plays a major role in a science of secret writing. It is the art of protecting information by transforming and technology application. The main reason for using email is probably the convenience and speed with which it can be transmitted, irrespective of geographical distance. Now a day's our entire globe is depending on internet and its application to protecting national security. Cryptography is used to ensure that the contents of a message are very confidentiality transmitted and would not be altered.

Cryptography provides number of security goals to ensure of privacy of data, on-alteration of data and so on. The idea of encryption and encryption algorithm by which we can encode our data in secret code and not to be able readable by hackers or

unauthorized person even it is hacked. The main reason for not using encryption in email communications is that current email encryption solutions and hard key management.

Different encryption techniques for promoting the information security. The evolution of encryption is moving towards a future of endless form of possibilities. As it is impossible to stop hacking, we can secure our sensitive data even it is hacked using encryption techniques and which protecting the information security. In this paper we present a survey paper on cryptographic techniques based on some algorithm and which is suitable for many applications where security is main concern.

II. LITERATURE REVIEW

Some of the concepts are used in Cryptography are mentioned here [1]:

2.1 Purpose of Cryptography

- *Authentication*: Authentication mechanisms help to establish proof of identities. This process ensures that the origin of the message is correctly identified.
- *Confidentiality*: The principle of confidentiality specifies that only the sender and the intended recipient should be able to process the contents of a message.
- *Availability*: The principle of availability states that resources should be available to authorized parties all the times.
- *Integrity*: The integrity mechanism ensures that the contents of the message remain the same when it reaches the intended recipient as sent by the sender.
- *Access Control*: Access Control specifies and controls who can access the process.

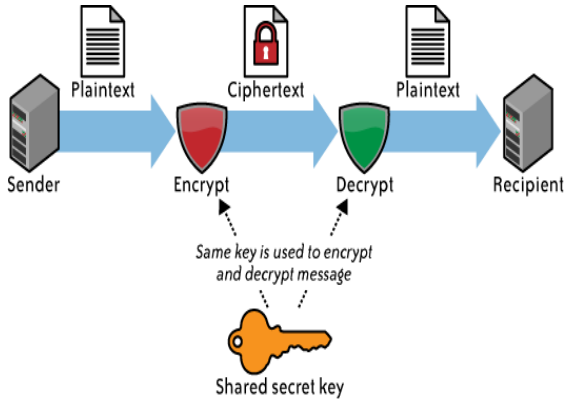

Fig.2. Secret Key Cryptography

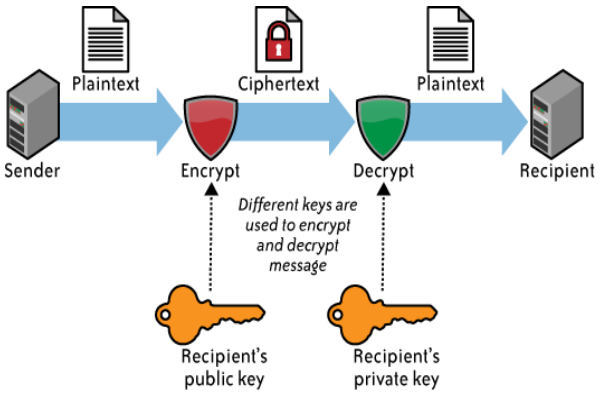

Fig.3. Public Key Cryptography

2.2 Types of Cryptography

- *Secret Key Cryptography*: When the same key is used for both encryption and decryption, DES, Triple DES, AES, RC5 and etc., may be the examples of such encryption, then that mechanism is known as secret key cryptography.
- *Public Key Cryptography*: When two different keys are used, that is one key for encryption and another key for decryption, RSA, Elliptic Curve and etc., may be the examples of such encryption, then that mechanism is known as public key cryptography.

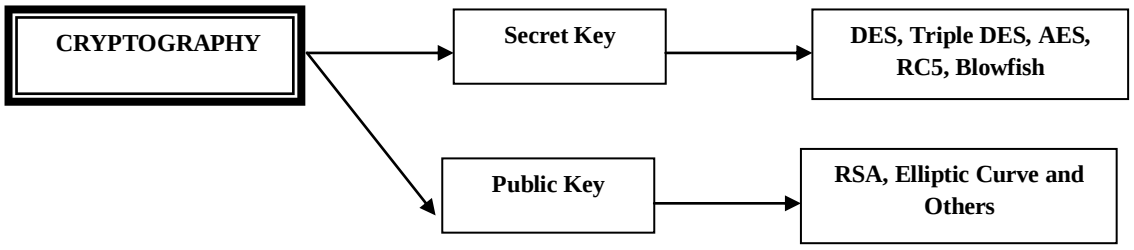

Fig.1. Classification of Cryptography

2.3 Cryptography

- *Plain Text*: Any communication in the language that we use in the human language, takes the form of plain text. It is understood by the sender and the recipient and also by anyone who gets an access to that message.

- *Cipher Text*: Cipher means a code or a secret message. When a plain text is codified using any suitable scheme the resulting message is called as cipher text.
- *Key*: An important aspect of performing encryption and decryption is the key. It is the key used for encryption and decryption that makes the process of cryptography secure.

2.3 Certificateless Public Key Cryptography

The concept of Certificate-less Public Key Cryptography (CL-PKC) is introduced by Al-Riyami and Paterson [18] in 2003, to overcome the key escrow problem of Identity Based Cryptography. In CL-PKC, a trusted third party, called the Key Generation Center (KGC), supplies a user with partial private key. While compared to identity based public key cryptography (IDPKC), the trust assumptions regarding the trusted third party in this scheme are significantly reduced. Using this scheme, the replacement of a public key of a user in the system by the KGC is equivalent to certificate by PKI system.

III. RELATED WORKS

3.1 DES

- ✓ DES is a block cipher that uses shared secret key for encryption and decryption. DES algorithm as described by Davis R [3] takes a fixed length of string in plaintext bits and transforms it through a series of operations into cipher text bit sting of the same length and its each block is 64 bits.
- ✓ There are 16 identical stages of processing, termed rounds. There is also an initial and final permutation which named as IP and FP

3.2 3DES

- ✓ 3DES is an enhancement of DES and it is 64 bit block size with 192 bits key size. In this standard the encryption of method is similar to the one in the original DES and increase the encryption level and the average safe time.
- ✓ In 3DES is slower than other block cipher methods. It uses either two or three 56 bit keys in the sequence order of Encrypt-Decrypt-Encrypt.
- ✓ TDES algorithm with three keys require 2^{168} chances of combinations and with two keys requires 2^{112} combinations; and the disadvantage of this algorithm is too time consuming problem.

3.3 AES

- ✓ In AES [6] is the almost identical of block cipher Rijndael cipher developed by two Belgian cryptographers, Joan and Vincent Rijmen. The algorithm explains about by AES is a secret-key algorithm which means of the same key is used for both encrypting and decrypting the data.
- ✓ AES on the other hand which encrypts all 128 bits in one iteration. This is one reason why it has a comparably small number of rounds. AES encryption is fast and flexible. It can be implemented on various platforms especially in small devices

3.4 Blowfish

- ✓ Blowfish [5] is one of the most common public domain encryption algorithm provided by Bruce Schneier one of the worlds leading cryptologists, and the president of Counterpane Systems and a consulting firm specializing in cryptography and computer security
- ✓ Blowfish encrypts 64-bits block cipher with variety length key and its contains two parts.

  - ❖ *Data Encryption*: Its involves the iteration of a simple function of 16 times. Each round contains a key dependent permutation and data dependent substitution.
  - ❖ *Subkey Generation*: Its involves converts the key upto 448 bits long to 4168 bits.

3.5 RSA

- ✓ RSA is a public key algorithm invented by Rivest, Shamir, Adleman [7]. RSA involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages.
- ✓ Messages encrypted with the public key can only be decrypted using the private key. These keys for the RSA algorithm are generated in many ways.

3.6 Comparison of Cryptography Algorithms

E. Thambiraja, G. Ramesh, Dr. R. Umarani [8] have done survey on most common encryption techniques. Monika Agrawal and Pradeep Mishra [9] in have also done a comparative survey on Secret Key Encryption Techniques. Gurujeevan Singh, Ashwani Kumar Singla, K.S.Sandha [4] in have provided comparison of various cryptography technique algorithms.

Algorithm	Created by	Key Size (in bits)	Block Size (in bits)
DES	IBM in year 1975	56	64
3DES	IBM in year 1978	112 (or) 168	64
AES	Joan Daemen and Vincent Rijmen in year 1998	256	128
Blowfish	Bruce Schneier in year 1993	32 (or) 448	64

Table 1. Cryptography Algorithms – A Comparision

IV. CONCLUSION

This paper gives a detailed study of Cryptography Techniques like AES, DES, 3DES, Blowfish, RSA, CL-PKC. Among those algorithms and concepts the security for the data has become highly important since the selling and buying of products over the open network occur very frequently. In this paper it has been surveyed about the existing works on the encryption techniques. This paper presents the performance evaluation of selected symmetric algorithms. The selected algorithms are AES, 3DES, Blowfish and DES. Firstly it was concluded that Blowfish has the better performing than other algorithms. In future we can use encryption techniques in such a way that it can consume less time and power of furthermore and high speed and minimum energy consumption.

REFERENCES:

[1] Atul Kahate "Cryptography and Network Security", Tata McGraw-Hill Companies, 2008
[2] D. Boneh and M. Franklin, "Identity-based encryption form the weil pairing", in Advance in Cryptology (CRYPTO'01), LNCS 2139, Springer Verlag, 37, 213-229, 2011
[3] Davis.R, "The Data Encryption Standard in Perspective", Proceeding of Communication Society magazine, IEEE, Vol 16, Nov 1978.
[4] Gurjeevan Singh, Ashwani Kumar Singla, K.S. Sandha "Performance Evaluation of Symmetric Cryptographic Algorithms", International Journal of Electronics and Communication Technology Vol 2 Issue 3, Sep 2011.
[5] Pratap Chandra Mandal "Superiority of Blowfish Algorithm", International Journal of Advanced Research in Computers Science and Software Engineering Vol 2 Issue 9, Sep 2012.
[6] Daemen.J and Rijmen, The Advanced Encryption Standard, Dr. Dobb's Journal, March 2001.
[7] R.L.Rivest, A.Shamir, L.Adleman, "A Method for obtaining Digital Signatures and Public-Key Cryptosystem", Communication of the ACM, Vol 21, Feb 1978.
[8] E.Thmbiraja, G.Ramesh, Dr.R.Umarani, "A survey on various most common encryption techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Vol 2, Issue 7, July 2012.
[9] Monika Agrawal, Pradeep Mishra", A Comparative Survey on Symmetric Key Encryption Techniques", International Journal on Computer Science and Engineering (IJCSE), Vol.4 May 2012.
[10] D. Crocker, T. Hansen, and M. Kucherawy, Domain keys Identified Mail (DKIM) Signatures, Technical Report 6376, Sep 2011.
[11] D. Eastlake, Domain Name System Security Extensions, Technical Report RFC 2535, Mar 1990.
[12] B.A. Forouzan, Cryptography and Network Security, India: Tata McGraw Hill Publishing Company Limited, 2007.
[13] Fortinet, Forti Mail Identity Based Encryption, Jan.2014 (http://www.fortinet.com)
[14] M. Franklin and D. Boneh, "Identity based encryption from the weil pairing", Journal of Computing, 32,586-615, 2003.
[15] E. Gerck, Secure Email Technologies X.509/PKI, PGP, IBE and Zmail. A Usability and Security Comparision, ICFAI University Press, 55, 171-196, 2007.
[16] C. Gu and Y. Zhu, "New efficient searchable encryption schemes from bilinear pairings", International Journal of Network Security, 10, 25-31, 2010.
[17] M. Hassouna, N. Mohamed, B. Barry, and E. Bashier, "An end-to-end secure mail system based on certifticateless cryptography in the standard security model", International Journal of Computer Science Issues, 10, 264-272, 2013.
[18] A. R. Sattam and P. Kenneth, "Certificateless public key cryptography a full version", in Asiacrypt'03, LNCS 2894, Springer, 20, 452-473, 2003.

