Scope International Journal of Science, Humanities, Management and Technology. ISSN : 2455-068X
Vol.2 Issue 3 (2016) 17 - 21. Submitted 10/08/2016. Published 21/08/2016

A SURVEY ON DIFFERENT CRYPTOGRAPHIC TECHNIQUES

A.N.Nandha Kumar[1], S. Nireshkumar[2], P. Ranjitha[3]
[1]Professor, [2]Assistant Professor, [3]Assistant Professor
Department of Computer Science and Engineering
Dhanalakshmi Srinivasan College of Engineering and Technology, Tamil Nadu, India

ABSTRACT

In the present day era evaluation of networking and wireless networks has come in data and communication technology, there are so many things that offers facility to deal with these science using internet. In web email protection is fundamental issue and the method of cryptography plays an necessary function to furnish the safety to the networks. To enhance safety and efficiency, most email system undertake Public Key Infrastructure (PKI) as the mechanism to implement security, however public key infrastructure based systems suffer from pricey certificate management and issues in scalability. The main goal of this strategy is recognition of electronic mail security and its requirements to the frequent computer users. A wide variety of cryptographic strategies are developed for achieving impervious communication. The proposed mailing device is impervious towards standard safety model.
Keywords - Computer Security, Cryptography, DES, AES, Blowfish, Encryption, Decryption, RSA, CL-PKC, Securing Data, Hacking.

I. INTRODUCTION

Today's our whole globe is depending on net and its software for their each and every phase of life. Here comes the requirement of securing our facts via approaches of Cryptography. Cryptography plays a main function in a science of secret writing. It is the artwork of protecting data with the aid of remodeling and technology application. The principal motive for the usage of e-mail is possibly the convenience and velocity with which it can be transmitted, irrespective of geographical distance. Now a day's our entire globe is relying on net and its utility to defending countrywide security. Cryptography is used to make sure that the contents of a message are very confidentiality transmitted and would not be altered. Cryptography provides wide variety of safety dreams to make sure of privateness of data, on-alteration of data and so on. The concept of encryption and encryption algorithm through which we can encode our data in secret code and now not to be able readable by using hackers or unauthorized character even it is hacked. The principal reason for now not using encryption in electronic mail communications is that modern-day email encryption options and challenging key management. Different encryption strategies for promoting the facts security. The evolution of encryption is shifting toward a future of countless structure of possibilities. As it is impossible to end hacking, we can tightly closed our touchy records even it is hacked using encryption methods and which protecting the data security. In this paper we current a survey paper on cryptographic strategies based on some algorithm and which is suitable for many purposes the place safety is principal concern.

II. LITERATURE REVIEW

Some of the standards are used in Cryptography are noted here [1]:

2.1 Purpose of Cryptography

- Authentication: Authentication method facilitates to create proof of identities. This system ensures that the beginning of the message is efficiently identified.
- Confidentiality: The principle of confidentiality specifies that solely the sender and the intended recipient should be in a position to technique the contents of a message.
- Availability: The principle of availability states that sources have to be on hand to authorized parties all the times
- Integrity: The integrity mechanism ensures that the contents of the message stay the equal when it reaches the intended recipient as despatched by means of the sender.
- Access Control: Access Control specifies and controls who can get admission to the process.

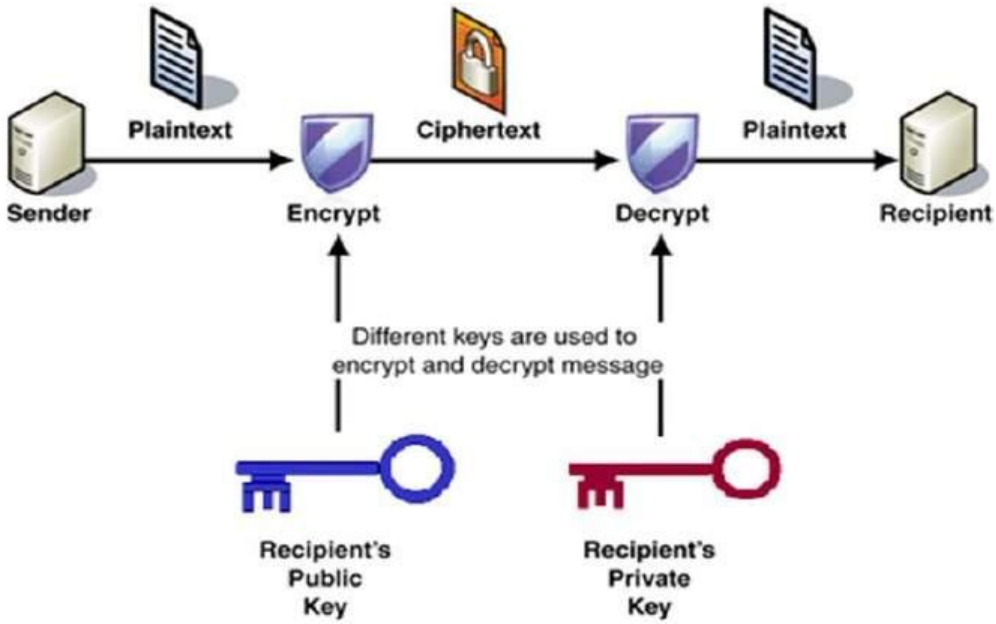


Fig.1. Public Key Cryptography

2.2 Types of Cryptography two Secret Key Cryptography:

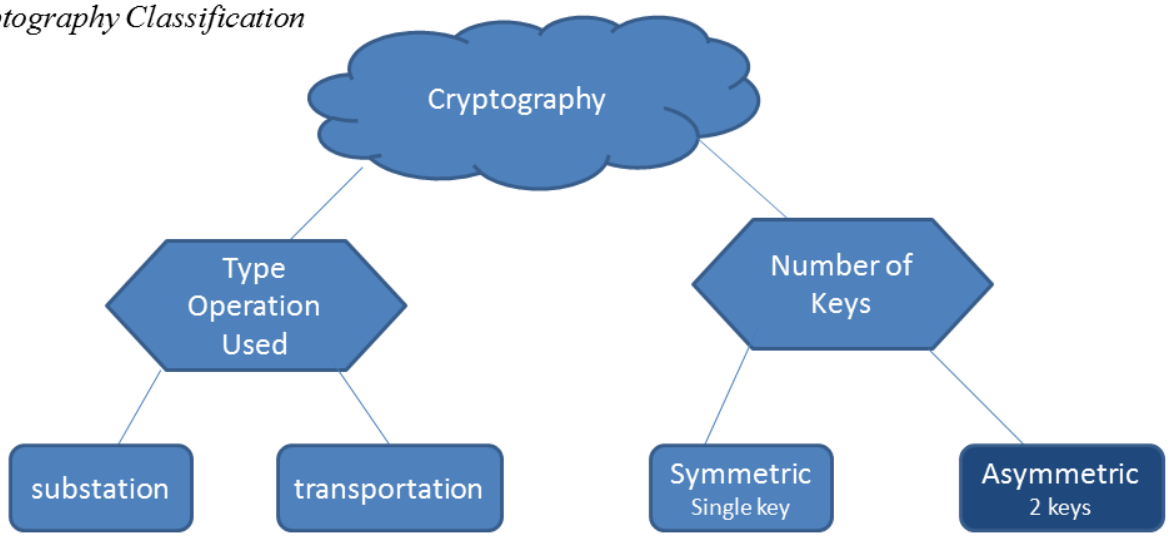
When the equal key is used for each encryption and decryption, DES, Triple DES, AES, RC5 and etc., may be the examples of such encryption, then that mechanism is recognized as secret key cryptography. Public Key Cryptography: When two unique keys are used, that is one key for encryption and some other key for decryption, RSA, Elliptic Curve and etc., might also be the examples of such encryption, then that mechanism is known as public key cryptography

2.3 Cryptography Plain Text:

Any communication in the language that we use in the human language, takes the form of simple text. It is understood by way of the sender and the recipient and additionally with the aid of

anyone who gets an get admission to that message. Cipher Text: Cipher skill a code or a secret message. When a simple text is codified using any appropriate scheme the ensuing message is referred to as cipher text. two Key: An essential issue of performing encryption and decryption is the key. It is the key used for encryption and decryption that makes the technique of cryptography secure.

Cryptography Classification



2.3 Certificateless Public Key Cryptography

The concept of Certificate-less Public Key Cryptography (CL-PKC) is brought via Al-Riyami and Paterson [18] in 2003, to overcome the key escrow problem of Identity Based Cryptography. In CL-PKC, a depended on 1/3 party, referred to as the Key Generation Center (KGC), elements a user with partial personal key. While in contrast to identification primarily based public key cryptography (IDPKC), the have faith assumptions regarding the trusted 1/3 celebration in this scheme are extensively reduced. Using this scheme, the alternative of a public key of a user in the device with the aid of the KGC is equal to certificate via PKI system.

III. RELATED WORKS

3.1 DES

DES is a mass cipher that utilizes common secret key for encryption and decryption. DES algorithm as described by using Davis R [3] takes a constant size of string in plaintext bits and transforms it via a series of operations into cipher text bit sting of the same size and its each block is sixty four bits. There are 16 identical degrees of processing, termed rounds. There is additionally an preliminary and closing permutation which named as IP and FP 3.2 3DES two 3DES is an enhancement of DES and it is sixty four bit block measurement with 192 bits key size. In this general the encryption of technique is comparable to the one in the unique DES and enlarge the encryption stage and the average protected time. In 3DES is slower than different block cipher methods. TDES algorithm with three keys require 2168 chances of mixtures and

with two keys requires 2112 combinations; and the disadvantage of this algorithm is too time consuming problem.

3.3 AES

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

3.4 Blowfish

Blowfish [5] is one of the most common public domain encryption algorithm provided by Bruce Schneier one of the world's main cryptologists, and the president of Counterpane Systems and a consulting association specializing in cryptography and computer safety two Blowfish encrypts 64-bits block cipher with variety size key and its carries two parts.

Data Encryption:

It entails the new release of a simple function of sixteen times. Each spherical includes a key dependent permutation and data established substitution. Subkey Generation: Its entails converts the key upto 448 bits lengthy to 4168 bits.

3.5 RSA

RSA is a public key algorithm invented by means of Rivest, Shamir, Adleman [7]. RSA involves a public key and a personal key. The public key can be acknowledged to all people and is used for encrypting messages. Messages encrypted with the public key can only be decrypted the usage of the personal key

IV. CONCLUSION

This paper offers a designated study of Cryptography Techniques like AES, DES, 3DES, Blowfish, RSA, CL-PKC. Among those algorithms and principles the security for the statistics has grow to be noticeably important given that the selling and shopping for of products over the open community manifest very frequently. In this paper it has been surveyed about the current works on the encryption techniques. This paper presents the overall performance evaluation of selected symmetric algorithms. The selected algorithms are AES, 3DES, Blowfish and DES. Firstly it was fulfilled that Blowfish has the improved performing than other algorithms. In outlook we can use encryption techniques that it can consume less time and power of furthermore and high speed and minimum energy consumption.

V. 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.