RESEARCH ARTICLE OPEN ACCESS

A Brief Survey of Cryptography Techniques

Dr. Kusum Lata Bharti [1], Dr. Varun Tiwari [2]
Associate Professor
Comm-IT Career Academy, (Aff. GGSIP University)
India

ABSTRACT
In the current era, assessment of networking and wireless network has come in information and communication expertise there are several things that give facility to deal with these technologies using internet. In internet communication security is main phase and the method of cryptography acts an important task to grant the security to the networks. To improve security and efficiency most communication system (email system) approve Public Key Infrastructure as the method to execute security, but PKI based systems endure from expensive certificate management and troubles in scalability. The object of this method to understanding of email security and its necessities to the common computer users. There are number of cryptographic techniques are elaborate for achieving secure communication. The proposed email system is secure against normal security model.

Keywords: Encryption, Decryption, Cryptography, DES,3DES, AES, two fish, Blowfish, RSA, Hacking, Security, Digital Signature

I. INTRODUCTION

The idea of encryption and its algorithm by which we can encode our information in secret code and not to be legible by unauthorized person. There are different encryption techniques for encourage the information protection. The progress of encryption is moving prospect of infinite form of possibilities. As it is not possible to end hacking, we are able to safe our data even it is hacked using encryption techniques and protecting the information security. In this document on cryptographic techniques based on several algorithm and which is appropriate for several applications where security is the main concern.That encoded algorithm is used to save our information and securing our data from hacker. DES, AES and or more technique used for the encryption in cryptography.

II. REVIEW

Cryptography concerns with

2.1Use of Cryptography

- **Privacy –** The transmitted text must be such that only the intended receiver should be able to read it.
- **Non-Repudiation-**Receiver should be able to confirm that the text it has received has come from a specific sender.
- **Access Control-**It means a system allowance or repeals the right to access some data, or achieve some action.
- **Integrity-**An incoming data at the receiver accurately, as it was sent. They should not be changed. The digital signature can provide message integrity.
- **Authentication-**The receiver needs to be sure regarding the sender's identity. Digital signature is used for providing the message authentication.

2.2 Cryptography algorithms are of following types-

Secret Key Cryptography,

Public key Cryptography

- **Secret key Algorithm :** It is also called symmetric key algorithm or private key. Single key for encryption and decryption. Famous secret key cryptographic algorithms include the Data Encryption Standard (DES), triple-strength DES (3 DES), Rivest Cipher 2 (RC2), Rivest Cipher 2 (RC4).

- **Public Key Cryptography:** It is also called asymmetric cryptography algorithm. Public key for encryption and private key for decryption.
- **Hash Functions:** They use no key and are also called one-way encryption. It mainly used to ensure that a file has remained unchanged.

2.3 CRYPTOGRAPHY

- **Plaintext**-The original message is called plaintext.
- **Encryption Algorithm**-it is the process to convert plaintext into cipher text.
- **Cipher text** –It is the encrypted form of the plaintext. It is depending on the key.
- **Decryption Algorithm**-It is the process to convert cipher text into plaintext.
- **Key**-The exact substitutions and transformations performed by the algorithm depend on the key.

Certificateless Public Key Cryptography

It is introduced by Sattam S. Al-Riyami and Kenneth G. Paterson; they have considered generation of private keys by a Key Generation Center (KGC). If the KGC gets compromised it will break security, so why should a KGC generate private keys.

III. RELATED WORKS

3.1 DES-It is a symmetric cipher, meaning one secret key is used for both encryption and decryption. It provides the foundation and structure for other symmetric ciphers. The DES handles a 64-bit block size and uses a 56-bit key during execution.DES makes use of the concepts developed for the Feistal Cipher. It alternates between substitutions and permutations conforming to the principles of confusion and diffusion of Claude Shannon.

3.2 TRIPLE DES (3DES) - Tuchman proposed a triple encryption technique. As a defense against man-in-the-middle attack of double DES, we can consider triple DES with three different keys. This requires a key length of 3x56=168 bits. The function follows encrypt-decrypt-encrypt sequence. The encrypted output of the first stage is decrypted using another key. This only scrambles the message further, making it difficult to decipher. The third stage again encrypts the encrypt-decrypt data, adding more security.

3.3 The Advanced Encryption Standard (AES) is the algorithm trusted as the standard by the U.S. Government and numerous organizations. It is extremely efficient in 128-bit form; AES also uses keys of 192 and 256 bits for heavy duty encryption purposes. AES is basically considered unreceptive to all hit or attack, with the exception of brute force, which attempts to decipher messages using all possible combinations in the 128, 192, or 256-bit cipher.

3.4 Twofish-Computer security skilled Bruce Schneier is the mastermind behind Blowfish and its descendant Twofish. Keys used in this algorithm may be up to 256 bits in length and as a symmetric technique, only one key is needed.Twofish is regard as one of the fastest of its kind, and ideal for use in both hardware and software environments. Like Blowfish, Twofish is freely available to anyone who wants to use it. As a result, it bundled in encryption programs such as PhotoEncrypt, GPG, and the popular open source software TrueCrypt.

3.5 Blowfish-Blowfish is another algorithm designed to replace DES. This symmetric cipher splits messages into blocks of 64 bits and encrypts them individually. Blowfish is known for both its terrific speed and overall efficiency as many claim that it has never been defeated. in the meantime, vendors have taken full advantage of its free availability in the public domain. Blowfish can be found in software categories ranging from e-commerce platforms for securing payments to password management tools, where it used to protect passwords. It's definitely one of the more flexible encryption methods available.

3.6 RSA- RSA is a public-key encryption algorithm and the standard for encrypting data sent over the internet. It also happens to be one of the methods used in our PGP and GPG programs. Unlike Triple DES, RSA is considered an asymmetric algorithm due to its use of a pair of keys. Public key for encryption and private key for decryption. The result of RSA encryption is a huge batch of mumbo jumbo that takes attackers quite a bit of time and processing power to break.

3.7 Comparisons of Cryptography techniques algorithms:

Table 1

Algorithm	Developed in	Key Size(in bits)
DES	1977	56
3DES	1978	168
AES	2001	128,192 and 256
Twofish	1998	Upto 256 bits
Blowfish	1993	448

IV. CONCLUSION

In this paper a comparative study among DES, 3DES, AES, Twofish, Blowfish and RSA. For Security of data algorithms are important. In this paper it has been review about the presented works on the encryption method. This paper presents the performance assessment of chosen symmetric algorithms. The selected algorithms are DES, 3DES, AES, Twofish, Blowfish and RSA. It was concluded that Blowfish has the enhanced performing than other algorithms. In future we can use encryption method in such a way that it can use a lesser amount of time and power.

REFERENCES

[1] 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.

[2] A. R. Sattam and P. Kenneth, "Certificateless public key cryptography a full version", in Asiacrypt'03, LNCS 2894, Springer, 20, 452-473, 2003.

[3] 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.

[4] C. Gu and Y. Zhu, "New efficient searchable encryption schemes from bilinear pairings", International Journal of Network Security, 10, 25-31, 2010.

[5] E. Gerck, Secure Email Technologies X.509/PKI, PGP, IBE and Zmail. A Usability and Security Comparision, ICFAI University Press, 55, 171-196, 2007.

[6] M. Franklin and D. Boneh, "Identity based encryption from the weil pairing", Journal of Computing, 32,586-615, 2003.

[7] Fortinet, Forti Mail Identity Based Encryption, Jan.2014 (http://www.fortinet.com).

[8] B.A. Forouzan, Cryptography and Network Security, India: Tata McGraw Hill Publishing Company Limited, 2007.

[9] D. Eastlake, Domain Name System Security Extensions, Technical Report RFC 2535, Mar 1990.

[10] D. Crocker, T. Hansen, and M. Kucherawy, Domain keys Identified Mail (DKIM) Signatures, Technical Report 6376, Sep 2011.

[11] Monika Agrawal, Pradeep Mishra", A Comparative Survey on Symmetric Key Encryption Techniques", International Journal on Computer Science and Engineering (IJCSE), Vol.4 May 2012.

[12] 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.

[13] 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.

[14] Daemen.J and Rijmen, The Advanced Encryption Standard, Dr. Dobb's Journal, March 2001.

[15] Pratap Chandra Mandal "Superiority of Blowfish Algorithm", International Journal of Advanced Research in Computers Science.

[16] Atul Kahate "Cryptography and Network Security", Tata McGraw-Hill Companies, 2008.

[17] D. Boneh and M. Franklin, "Identity-based encryption forms the weil pairing", in Advance in Cryptology (CRYPTO'01), LNCS [2] D. Boneh and M. Franklin, "Identity-based encryption form the weil pairing", in Advance in Cryptology (CRYPTO'01), LNCS [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 2139, Springer Verlag, 37, 213-229, 2011

[18] Davis.R, "The Data Encryption Standard in Perspective", Proceeding of Communication Society magazine, IEEE, Vol 16, [3] Davis.R, "The Data Encryption Standard in Perspective", Proceeding of Communication Society magazine, IEEE, Vol 16, [3] Davis.R, "The Data Encryption Standard in Perspective", Proceeding of Communication Society magazine, IEEE, Vol 16, Nov 1978.