ISSN No. 0976-5697

Volume 8, No. 4, May 2017 (Special Issue)

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Data Encryption Using Different Techniques: A Review

Er. ManpreetKaur
Assistant Professor, Department of CSA
Sant Baba Bhag Singh University, Jalandhar
Manpreet5986@gmail.com

Er. Jasjeet Kaur
Assistant Professor, Department of CSE
Sant Baba Bhag Singh University, Jalandhar
jparmar21nice@gmail.com

Abstract --**In present times, the high growth in the networking technology leads a practice of interchanging of the digital data very frequently. The data in both the private and public sectors are increased which requires Availability Authentication, Confidentiality, Integrity. The security of this confidential data from unauthorized access can be done by many encryption techniques. This paper will survey some of the most popular and interesting algorithms of encryption that are currently used. This paper focuses mainly on already existed different kinds of encryption techniques.**

Keywords: - ***Encryption Algorithm Cryptography; DES; AES; Encryption; Decryption.***

I. INTRODUCTION

Now a day's high growth in the network technology leads a common practice for interchanging of the data very extremely. Hence it is more unprotected and duplicates data and reorganizes by hackers. Therefore when information is transmitted it has to be secure, while confidential information like ATM cards, credit cards, banking transactions and digital right management need to be protected. For security from unauthorized users encryption techniques are used to avoid the information hacking. For data security in wireless communication encryption techniques plays important role because wireless communication is used in online transmission. Different encryption techniques are used to protect the confidential data from unauthorized use. Encryption is most effective way to achieve data security. The evolution of encryption is moving towards a future of endless possibilities. Everyday new methods of encryption techniques are discovered. This paper explains some of the recent existing encryption techniques and their security issues.

A. Basic Terms Used in Cryptography

1) Plain Text- The original message that is easily readable by humans. It is a term used in cryptography that refers to a message before encryption or after decryption. For example, A is a person wishes to send "Hello Friend how are you" message to the person B. Here "Hello Friend how are you" is a plain text message.

2) Cipher Text- In cryptography, cipher text is data that has been encrypted. This text is unreadable until it has been converted into plain text with a key. For example, "phqgiumealy" is a cipher text produced for "abcdefghijk".

3) Encryption- It is security tool for computer network. It is process of converting information (known as plain text) using an algorithm to make it unreadable (known as cipher text) to anyone except those processing special knowledge, usually referred to as a key. It is the most efficient method to achieve data security. Encryption can protect confidentiality of message. For data encryption, a secret key is used. Encrypted data is called as cipher text and decrypted data is called as plain text.

4) Decryption- It is process of taking encoded or encrypted text and converting it back into original text. Decryption is used for un-encrypting the data with keys or algorithm. Cryptography uses the decryption technique at the receiver side to obtain the original message from non-readable message (Cipher Text). The decryption process requires two things- a Decryption algorithm and a key. A Decryption algorithm indicates the technique that has been used in Decryption. Usually, the encryption and decryption algorithm are same.

5) Key- A key is a numeric or alpha numeric text or may be a special symbol. The Key is used at the time of encryption work on the plain text and at the time of decryption work on the cipher text. The selection of key plays vital rolein cryptography process as the security of encryption algorithm fully depends on it. For example, if A uses a key of 2 to encrypt the Plain Text "University" then Cipher Text produced will be "wpkxgtkva".

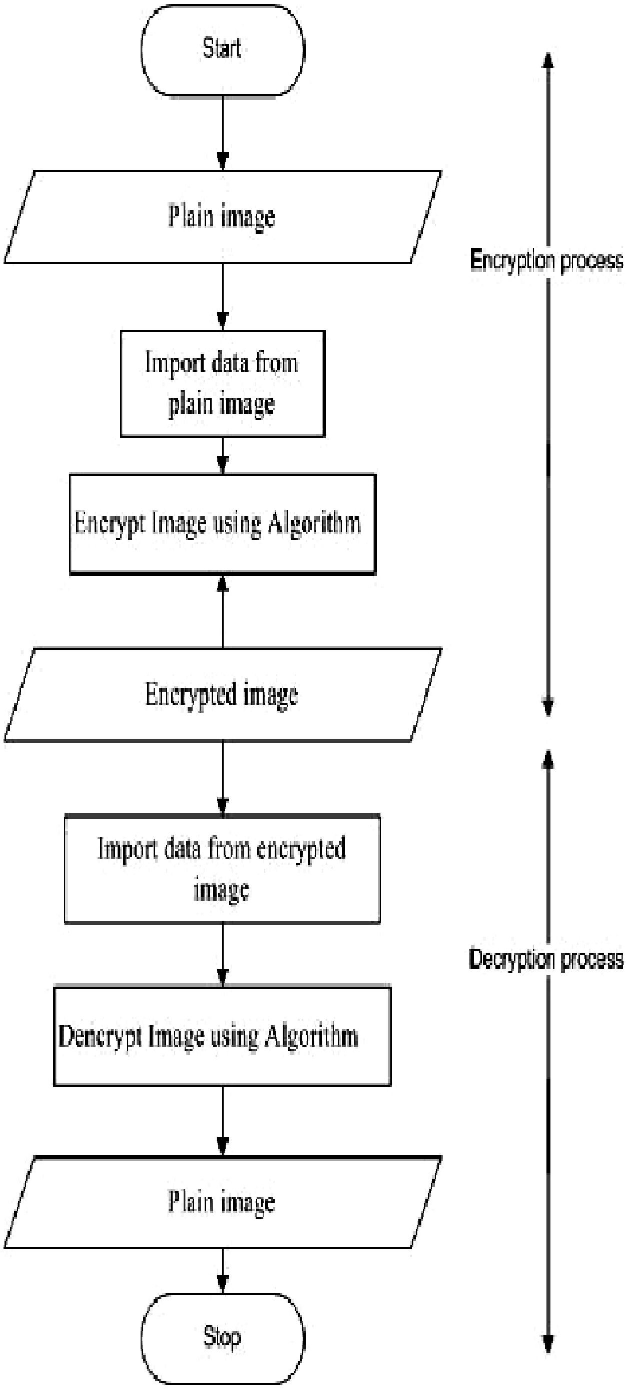
Start
Plain image
Import data from plain image
Encrypt Image using Algorithm
Encrypted image
Import data from encrypted image
Dencrypt Image using Algorithm
Plain image
Stop
Encryption process
Decryption process

Fig. 1.Encryption Decryption Process

B. Goals of Cryptography

Cryptography is a technique used to write data in secret code. It provides a number of security goals to ensure the privacy of data, non-alteration of data and so on. Due to the great security demand, cryptography is widely used today. Following are the various goals of cryptography:

- Confidentiality-Information in computer is transmitted and has to be accessed only by the authorized party and not by anyone else.
- Authentication- The identity of thesender has checkedto assure thatwhether the information received by any system is arriving from an authorized person or a false identity.
- Integrity –Assuring the receiver that the received message has not been altered in any way from the original. Only the authorized user is allowed to alter the transmitted information.
- Non Repudiation-Ensures that neither the sender, nor the receiver of message should be able to deny the transmission
- Access Control-Only the authorized parties are able to access the given information.

II. CLASSIFICATION OF CRYPTOGRAPHY

The encryption algorithms are classified into two broad categories: Symmetric Key and Asymmetric Key encryption as shown in Fig. 2.

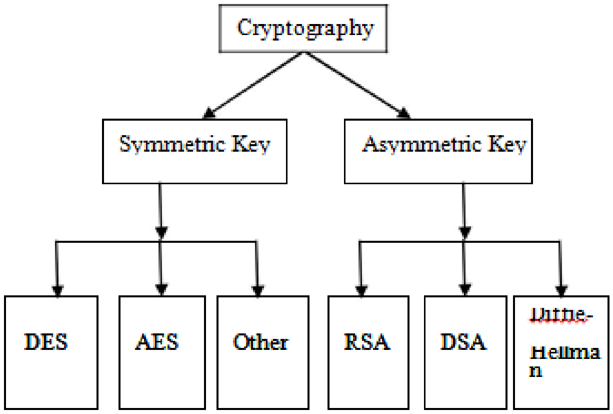

Fig. 2. Overview of Most Common encryption algorithm

A. Symmetric Encryption- This type of cryptography uses a single key,which is used for encryption and decryption. The sender uses the key to encrypt the plaintext and sends the cipher text to the receiver. At the receiver side, same key will be used to decrypt the message and get the plaintext. Because there is common key used for encryption and decryption process, the secret key cryptography is also known as symmetric encryption. This was the only type of encryption method widely known until June 1976. There are various symmetric key algorithms such as DES, TRIPLE DES, AES, RC4, RC6, and BLOWFISH [2].

B. Asymmetric Encryption- Public-key cryptography, where key used to encrypt a message is differ from key used to decrypt a message. In asymmetric or public-key cryptography, there are two cryptographic keys: a private key and a public key are used. The private key is kept secret, while public key may be distributed. Messages are encrypted with recipients' public key and decrypted with private key. Some commonly used asymmetric cryptography techniques are RSA (Rivest Shamir and Adleman), Diffie-Hellman, and DSA (Digital Signature Algorithm).

A significant disadvantage of symmetric ciphers is the key management necessary to use them securely. Each distinct pair of communicating parties must, ideally, share a different key, and perhaps each cipher text exchanged as well. The number of keys required increases as the square of the number of network members, which very quickly requires complex key management schemes to keep them all straight and secret.

III. ANALYSIS OF DIFFERENT TECHNIQUES

A. RSA (Rivest Shamir and Adleman) Algorithm

RSA is an algorithm for public-key cryptography that is based on the presumed difficulty of factoring large integers, the factoring problem [10]. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described the algorithm in 1977.In RSA,user firstly creates and then publishes the product of two large prime numbers and their public key as an auxiliary value [11]. These prime numbers must be kept secret. Public keycan be used by anyone to encrypt a message.

The RSA algorithm involves three steps:

- Key generation
- Encryption and
- Decryption

B. Digital Signature Algorithm

A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient cause to believe that the message was created and sent by a known sender; such that the sender cannot refuse having sent the message (authentication and non-repudiation) and that the message was not altered in transmission (integrity)[12]. Digital signatures are commonly used for financial transactions, software distribution, and in many other cases where it is important to detect forgery or tampering. Digital signatures are often used to implement electronic signatures, which refer to any electronic data that carries the intent of a signature. It is not true that all electronic signatures use digital signatures.

Digital signatures employ a type of asymmetric cryptography. For messages sent through a non secure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender [13]. Digital signatures are equivalent to traditional handwritten signatures in many respects, but properly implemented digital signatures are more difficult to forge than the handwritten type. Digital signature schemes in the sense used here are cryptographically based, and must be implemented properly to be effective. Digital signatures can also provide non-repudiation, meaning that the signer cannot successfully claim they did not sign a message, while also claiming their private key remains secret; further, some non-repudiation schemes offer a time stamp for the digital signature, so that even if the private key is exposed, the signature is valid. Digitally signed messages may be anything representable as a bitstring: examples include electronic mail, or a message sent via some other cryptographic protocol.

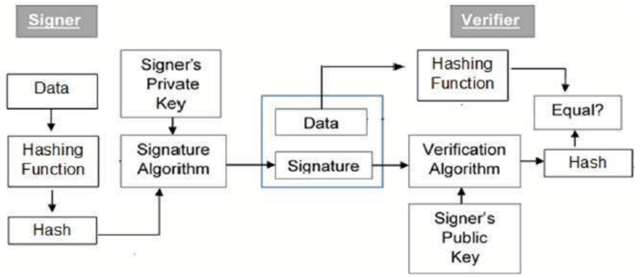

Fig.3. Digital Signature Algorithm

C. Diffie–Hellman Algorithm

Diffie–Hellman key exchange is a specific method of exchanging cryptographic keys [14]. It is one of the earliest practical examples of key exchange implemented within the field of cryptography. The Diffie–Hellman key exchange method allows twounknown parties to jointly establish a shared secret key over an insecure communications channel [15]. This key can be thenused to encrypt subsequent communications using a symmetric key cipher.The method was followed shortly afterwards by RSA, an implementation of public key cryptography using asymmetric algorithms.

D. Data Encryption Standard

The DES algorithm is the most widely used encryption algorithm in the world [16]. For many years, and among many people, "secret code making" and DES have been synonymous. The DES was published by the United States' National Bureau of Standards in January 1977 as an algorithm to be used for unclassified data (information not concerned with national security). DES applies a 56-bit key to each 64-bit block of data. This process can run in several modes and involves 16 rounds. Although this is considered "strong" encryption, many companies use "triple DES", which applies three keys in succession. This is not to say that a DES-encrypted message cannot be "broken."

E. AES (Advanced Encryption Standard)

The Advanced Encryption Standard (AES) is an encryption algorithm for securing sensitive but unclassified material by U.S. Government agencies and, as a likely consequence, may eventually become the de facto encryption standard for commercial transactions in the private sector. It is robust replacement for the Data Encryption Standard (DES) and to a lesser degree Triple DES. The specification called for a symmetric algorithm using block encryption of 128 bits in size, supporting key sizes of 128, 192 and 256 bits, as a minimum. The algorithm was required to be royalty-free for use worldwide and offer security of a sufficient level to protect data for the next

20 to 30 years. It's hardware and software implementation is easyeven in restricted environments (for example, in a smart card) and also offers good protection against various attack techniques.

IV. CONCLUSION

Cryptography plays important role in increasing growth of digital data storage and communication. It is used to achieve the mains of security goals like confidentiality, integrity, authentication, non-repudiation. It is analyzed that in Diffie-Hellman key exchange cryptography algorithm, secret keys are exchanged between two users. Whereas a digital signature is used by receiver in digital signature algorithm to verify that the signal received is notaltered. It is also concluded that all the techniques are useful for real-time encryption. Each technique is unique in its own way, which might be suitable for different applications. Many new encryption techniquesdevelopingtherefore fast and secure standard encryption techniques will always work out with high rate of security.

REFERENCES

[1] William Stallings "Network Security Essentials (Applications and Standards)", Pearson Education, 2004.

[2] National Bureau of Standards, " Data Encryption Standard," FIPS Publication 46, 1977.

[3] Daemen, J., and Rijmen, V. "Rijndael: The Advanced Encryption Standard." Dr. Dobb's Journal, March 2001.

[4] Ramesh G, Umarani. R," Data Security In Local Area Network Based On Fast Encryption Algorithm",International Journal of Computing Communication and Information System(JCCIS) Journal Page 85-90. 2010.

[5] DiaaSalama Abdul Minaam, Hatem M. Abdual-Kader, and Mohiy Mohamed Hadhoud "Evaluating the Effects of Symmetric Cryptography Algorithms on Power Consumption for Different Data Types" International Journal of Network Security, Vol.11, No.2, PP.78-87, Sept.

[6] SimarPreet Singh, and Raman Maini "Comparison of Data Encryption Algorithms" International Journal of Computer Science and Communication Vol. 2, No. 1, January-June 2011, pp. 125-127

[7] ChallaNarasimham, JayaramPradhan," Evaluation of Performance Characteristics of Cryptosystem using Text Files" Journal of Theoretical and Applied Information Technology,pp55-59 2008.

[8] Abdel-Karim Al Tamimi, "Performance Analysis of Data Encryption Algorithms"

[9] Prasithsangaree.P and Krishnamurthy.P(2003), "Analysis of Energy Consumption of RC4 and AES Algorithms in Wireless LANs," in the Proceedings of the IEEE GLOBECOM 2003, pp. 1445-1449.

[10] A. Perrig, J. Stankovic, and D. Wagner,"Security In Wireless Sensor Networks," ACM,Vol. 47, No.653.2004.

[11] Chandra M. Kota et al.,"Implementation of the RSA algorithm and its cryptanalysis," In proceedings of the 2002 ASEEGulf-Southwest Annual Conference, March 20 –22, 2002.

[12] ErfanehNoorouzil et al, "A New Digital Signature Algorithm", International Conference on Machine Learning and Computing, IPCSIT,vol.3, 2011

[13] William-Stallings, http://williamstallings.com /Extras/Security Notes/lectures/authent.html, Dated: 13-dec-2012at 14:05.

[14] Wikipedia,"http://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange," Dated: 13-dec-2012 at10:33

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

[16] The DES 15 years of public scrutiny. dorothy e denning.

[17] http://faculty.nps.edu/dedennin/publications /DES-15Years.pdf

[18] https://www.tutorialspoint.com/cryptography/cryptography_digital_signatures.htm

[19] https://www.researchgate.net/figure/276230307_fig1_Figure-2-The-flow-chart-diagram-for-the-encryption-and-decryption-process