ISSN : 2454-9150 Vol-01, Issue 09, Dec 2015.

DATA SECURITY USING VARIOUS CRYPTOGRAPHY TECHNIQUES: A RECENT SURVEY

Roshan M. Pandav[1], Vijay Kumar Verma[2]
ME Student[1], Asst. Professor[2], Lord Krishna College of Technology, Indore, M.P., India[1,2]
Roshanpandey67@gmail.com[1], vijayvermaonline@gmail.com[2]

***Abstract* — Today internet is widely used tool for communication, exchange of information and sending and receiving of data using computers, mobile phones and other electronic gadgets. Unsecured data that travels through different networks are open and can be read, altered or copied by anyone who has access to that data. Cryptographic algorithms are used to encrypt and decrypt messages. In the past year several algorithm have been developed for improving the efficiency of Cryptographic algorithms. Each and every algorithm used different techniques and process to encryption and decryption the data. In this paper we represent a comparative study of various encryptions, decryption algorithms.**

Keywords*— *Cryptography, Data Security, key, Algorithms.

I. INTRODUCTION

Cryptography is a process of encrypt and decrypt messages or data in such a way that only authorized users can read it. In encryption process the original message or data called plaintext is given as input to form cipher text. In decryption process the cipher text is transforming into plaintext. Cryptographic algorithms are classified as symmetric and asymmetric. Symmetric key algorithms are the quickest and most commonly used type of encryption. Here, a single key is used for both encryption and decryption.

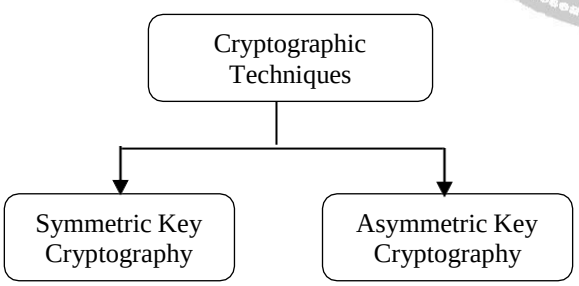

Figure 1Classification of Cryptographic techniques

(1))Secret key cryptography: -Secret key cryptography techniques used single key for both encryption and decryption.

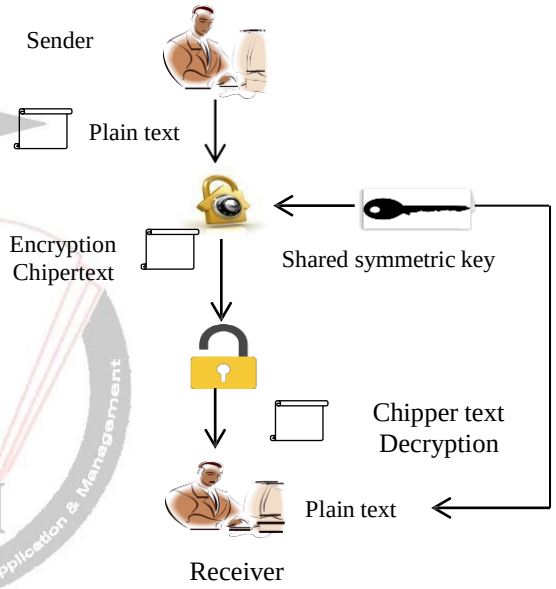

Figure 2 Secret key cryptography

Figure 2 show working process of Secret key cryptography techniques the sender uses the key to encrypt the plaintext and sends the cipher text to the receiver. The receiver applies the same key to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called symmetric encryption.

(2) Public key cryptography

Public key cryptography used of key pairs one private key and one public key. Both are required to encrypt and decrypt a message or transmission. The private key, not to be confused with the key utilized in private key cryptography, is just that, private. It is not to be shared with anyone. The owner of the key is responsible for securing it in such a

manner that it will not be lost or compromised. On the other hand, the public key is just that, public. Public key cryptography intends for public keys to be accessible to all users. In fact, this is what makes the system strong. If a person can access anyone public key easily, usually via some form of directory service, then the two parties can communicate securely and with little effort, i.e. without a prior key distribution arrangement. Figure 3 describes the public key cryptography.

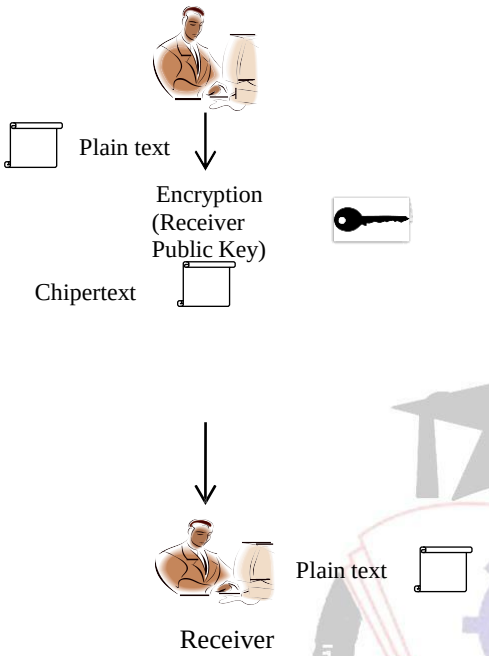

Figure 3Public key cryptography

II. LITERATURE REVIEW

In 2011 B. Ravi Kumar and Dr. P. R. K. Murti proposed "Data Encryption and Decryption process Using Bit Shifting and Stuffing (BSS)Methodology". They proposed BSS method I which they stuffing a new bit in the place of unused bit which is shifting from another printable character. So in BSS methodology after encryption, for every eight bytes of plain text it will generate seven bytes cipher text and in decryption, for every seven bytes of cipher text it will reproduce eight bytes of plaintext.

In 2012 Ch. Santhosh Reddy, Ch. Sowjanya and Shalini L proposed" Poly-alphabetic Symmetric Key Algorithm Using Randomized Prime Numbers. They give brief description about symmetric key algorithms and proposed new algorithm in symmetric key cryptography. The proposed algorithm contains two levels of Exclusive OR (XOR) operation. The algorithm is useful in transmission of messages and data between one user and another.

In 2014 Ezeofor C. J. Ulasi A. G. proposed "Analysis of Network Data Encryption &Decryption Techniques in Communication Systems". They present analysis of network data encryption and decryption techniques used in communication systems. Basic simulation program that encrypt and decrypt data were developed, written and tested. Different data block sizes analysis was made based on the graph result.

In 2013 Obaida Mohammad Awad Al-Hazaimeh proposed "A New Approach for Complex Encrypting and Decrypting Data". They proposed A New Approach for Complex Encrypting and Decrypting Data" which maintains the security on the communication channels by making it difficult for attacker to predicate a pattern as well as speed of the encryption / decryption scheme.

In 2013RachnaArora, Anshu Parashar proposed "Secure User Data in Cloud Computing Using Encryption Algorithms". They discussed about cloud computing security issues, mechanism, challenges that cloud service provider face during cloud engineering and presented the metaphoric study of various security algorithms.

In2014 Satyajeet R. Shinge , Rahul Patil proposed " An Encryption Algorithm Based on ASCII Value". They present a symmetric cryptographic algorithm for data encryption and decryption based on ASCII values of characters in the plaintext. The algorithm encrypts the plaintext using their ASCII values. The secret key is converted to another string and that string is used as a key to encrypt or decrypt the data.

In 2013 Vineet Sukhraliya, Sumit Chaudhary, Sangeeta Solanki Encryption and Decryption Algorithm using ASCII values with substitution array Approach This is the algorithm in which randomly generated numbers are used with the help of modulus and remainder by making program in any language i.e. c, c++ and java. Carefully, using these modulus & remainder for getting a new method for encrypting and decrypting the message. Though complex

encryption techniques have been employed in safe guarding data. Three or more keys can also be used to make the enciphering process more complicated. The main focus is to provide with an encryption decryption algorithm with secure strength, bringing failure to the intruder effort to break the cipher.

III. ALGORITHMS EVALUATION PARAMETERS

Some of the basic parameters that have been used for analyzing the algorithms performance are

(1))Architecture: -This determines that the algorithm is symmetric or asymmetric and the structure and operations that an algorithm can perform.

(2) Flexibility:-This determines whether the algorithm is able to endure minor modifications according to the requirements

(3) Security: -Security of an encryption algorithm depends on the key size used to execute the encryption. Generally, greater the keys size stronger the encryption. Length of key is measured in bits.

(4))Scalability:-It is one of the major element on which encryption algorithms can be analyzed. Scalability depends on certain parameters such as Memory Usage, Encryption rate, Software hardware performance; Computational efficiency.

Name of Algorithm	Architecture
DES	The DES is a block cipher that uses a 64 bit plain text with 16 rounds and a Key Length of 56-bit
Triple DES	The 3DES uses a 64 bit plain text with 48 rounds and a Key Length of 168-bits permuted into 16 sub- keys each of 48- bit length.
Blowfish	Blowfish is a block cipher that uses a 64 bit plain text with 16 rounds, allowing a variable key length

Table 1 Basic parameters Architecture

Name of Algorithm	Security
DES	The security strength of DES depend on its 56 bit key size generating 7.2 x 1016 possible keys
Triple DES	DES operations (encrypt-decrypt-encrypt) are performed 3 times in 3DES with 2-3 different keys, offering "112 bits of security" , avoiding so-called meet-in-the-middle attack
Blowfish	Blowfish's security lies in its variable key size (128-448 bits) providing high level of security,

Table 2 Basic parameters Security

Name of Algorithm	Flexibility
DES	The structure of DES doesn't support any modifications
Triple DES	DES operations (encrypt-decrypt-encrypt) are performed 3 times in 3DES with 2-3 different keys, offering "112 bits of security" , avoiding so-called meet-in-the-middle attack
Blowfish	Blowfish key length must be multiples of 32 bits

Table 2 Basic parameters Flexibility

IV. CONCLUSION

Cryptography plays an important role for securing data for communication and storage. The main goal of data security is confidentiality, integrity, authentication, non-repudiation. The main purpose of this paper is to spread the basic knowledge about the cryptographic algorithms and comparison of available symmetric and asymmetric key encryption techniques based advantage and disadvantage.

REFERENCES

[1] Ezeofor C. J., Ulasi A. G "Analysis of Network Data Encryption &Decryption Techniques in Communication Systems" International Journal of Innovative Research in Science, Engineering and Technology(An ISO 3297: 2007 Certified Organization)
Vol. 3, Issue 12, December 2014

[2] Obaida Mohammad Awad Al-Hazaimeh A New Approach For Complex Encrypting And Decrypting Data International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.2, March 2013

[3] Rachna Arora and Anshu Parashar Secure User Data in Cloud Computing Using Encryption Algorithms Rachna Arora, Anshu Parashar / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 3, Issue 4, Jul-Aug 2013, pp.1922-1926

[4] Satyajeet R. Shinge , Rahul Patil An Encryption Algorithm Based on ASCII Valueof Data Satyajeet R. Shinge et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (6) , 2014, 7232-7234

[5] B. Ravi Kumar, Dr. P R. K. Murti Data Encryption and Decryption process Using Bit Shifting and Stuffing (BSS)Methodology B. Ravi Kumar et al. International Journal on Computer Science and Engineering (IJCSE) Vol. 3 No. 7 July 2011

[6] Ch. Santhosh Reddy, Ch. Sowjanya, P. Praveena, Prof Shalini L Poly-alphabetic Symmetric Key Algorithm Using Randomized Prime Numbers International Journal of Scientific and Research Publications, Volume 2, Issue 9, September 2012 1 ISSN 2250-3153

[7] Sombir Singh and Sunil K. Maakar Enhancing the Security of DES Algorithm Using Transposition Cryptography Techniques " International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 6, June 2013

[8] Sanket A. Ubhad, Prof. Nilesh Chaubey, Prof. Shyam P. Dubey Advanced ASCII Based Cryptography Using Matrix Operation, Palindrome Range, Unique id International Journal of Computer Science and Mobile Computing IJCSMC, Vol. 4, Issue. 8, August 2015, pg.66 – 71

[9]Mansoor Ebrahim Shujaat Khan Symmetric Algorithm Survey: A Comparative Analysis International Journal of Computer Applications (0975 – 8887) Volume 61– No.20, January 2013

[10] Suchita Tayde, Asst. Prof. Seema Siledar File Encryption, Decryption Using AES Algorithm in Android Phone International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 5, May 2015.

