International Journal of Scientific Engineering and Research (IJSER)
www.ijser.in
ISSN (Online): 2347-3878
Volume 2 Issue 2, February 2014

Analysis and Review of Encryption and Decryption for Secure Communication

Vikas Agrawal[1], Shruti Agrawal[2], Rajesh Deshmukh[3]

BE 8th Semester, CSE, Shri Shankaracharya Institute of Professional Management & Technology
Raipur, Chhattisgarh, India

BE 8th Semester, ET&T, Shri Shankaracharya Institute of Professional Management & Technology
Raipur, Chhattisgarh, India

Assistant Professor, Department of CSE, Shri Shankaracharya Institute of Professional Management & Technology
Raipur, Chhattisgarh, India

Abstract: ***The Process of Encryption and Decryption is performed by using Symmetric key cryptography and public key cryptography for Secure Communication. In this paper, we studied that how the process of Encryption and Decryption is perform in case of Symmetric key and public key cryptography using AES and DES algorithms and modified RSA algorithm.***

Keywords: Encryption, Decryption, AES, DES, RSA

1. Introduction

Cryptography is the practice and study of techniques for secure communication in the presence of third parties (called adversaries). More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation. Cryptography prior to the modern age was effectively synonymous with encryption, the conversion of information from a readable state to apparent nonsense. The originator of an encrypted message shared the decoding technique needed to recover the original information only with intended recipients, thereby precluding unwanted persons to do the same. Since World War I and the advent of the computer, the methods used to carry out cryptology have become increasingly complex and its application more widespread. Cryptography includes the following process:

1.1 Encryption and Decryption:

It is the process of converting ordinary information (called plaintext) into unintelligible text (called ciphertext). Decryption is the reverse, in other words, moving from the unintelligible ciphertext back to plaintext. A cipher is a pair of algorithms that create the encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm and in each instance by a "key". This is a secret (ideally known only to the communicants), usually a short string of characters, which is needed to decrypt the ciphertext.

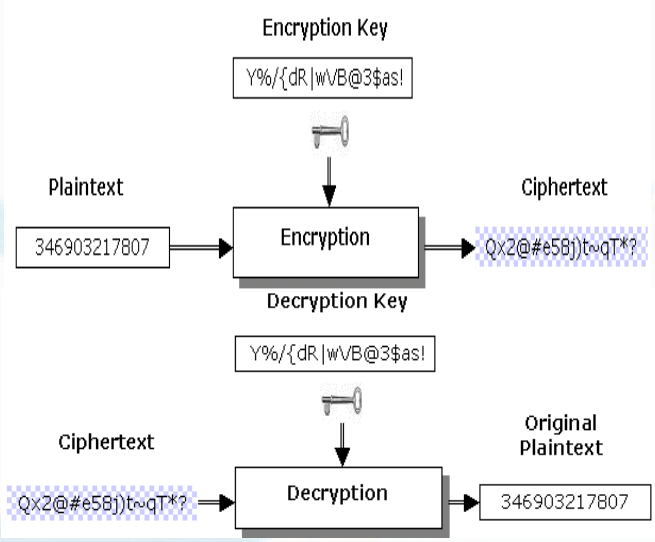

Figure 1: Process of Encryption and Decryption

2. Modern Cryptography

2.1 Modern Cryptography

Following are the modern field of cryptography:

a) Symmetric-Key Cryptography
Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key. Symmetric key ciphers are implemented as either block ciphers or stream ciphers. A block cipher enciphers input in blocks of plaintext as opposed to individual characters, the input form used by a stream cipher. The Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) are block cipher designs which have been designated cryptography standards by the US government

b) Public-Key Cryptography

Symmetric-key cryptosystems use the same key for encryption and decryption of a message, though a message or group of messages may have a different key than others. 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 ciphertext 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 consistent and secret. Diffie and Hellman's publication sparked widespread academic efforts in finding a practical public-key encryption system. This race was finally won in 1978 by Ronald Rivest, Adi Shamir, and Len Adleman, whose solution has since become known as the RSA algorithm.

c) Cryptanalysis

The goal of cryptanalysis is to find some weakness or insecurity in a cryptographic scheme, thus permitting its subversion or evasion. It is a common misconception that every encryption method can be broken. In connection with his WWII work at Bell Labs, Claude Shannon proved that the one-time pad cipher is unbreakable, provided the key material is truly random, never reused, kept secret from all possible attackers, and of equal or greater length than the message. Most ciphers, apart from the one-time pad, can be broken with enough computational effort by brute force attack, but the amount of effort needed may be exponentially dependent on the key size, as compared to the effort needed to make use of the cipher.

3. Literature Survey

Amrita Sahu et.al proposed a new key generation algorithm based on palm print which is used for encryption and decryption of an image. Our scheme allows one party to send a secret image to another party over the open network, even if many eavesdroppers listen. This scheme gives reliable security. They presented an image encryption/decryption scheme based on bit XOR method in this paper. The salient features of the proposed asymmetric image encryption scheme can be summarized as: (a) Lossless encryption of image. (b) Less computational complexity. (c) Convenient realization. (d) Choosing a suitable size of matrix according to the size of image. (e) Encryption/decryption scheme uses integer arithmetic and logic operations. [1].

Irfan.Landge et.al describes that Both colour and black & white image of any size saved in tagged image file format (TIF) can be encrypted & decrypted using blowfish algorithm. Histogram of encrypted image is less dynamic and significantly different from the respective histograms of the original image. Blowfish cannot be broken until an attacker tries 28r+1 combinations where r is the number of rounds. Hence if the number of rounds are been increased then the blowfish algorithm becomes stronger. Since Blowfish has not any known security weak points so far it can be considered as an excellent standard encryption algorithm. [2].

Rajan.S.Jamgekar et.al shows that MREA algorithm is used to encrypt files and transmit encrypted files to other end where it is decrypted. The project works efficiently for small size while it consumes time for large size of files. At a instant only one file can be encrypted and transmitted. As a future work multiple file encryption and decryption can be possible. It has broad development prospects. The project application was designed to take the efficiency and reusability into account. Great level of security is achieved using this algorithm. Modified RSA algorithm for file transmission algorithm can be used where high security file transmission required in public forums. [3].

Akanksha Mathur et.al represents that the proposed algorithm has the following limitations:

1) More Execution time
2) Key Length and length of plain text must be same

In the future wok related to proposed algorithm, the limitations of proposed algorithm are overcome by encrypting and decrypting data may or may not be same key length size in comparison with input size. [4].

Monisha Sharma et.al describes that the method proposed in this paper has got a lossless encryption of image. This also gives access to variable lengths of the encryption keys. Another main feature of this method is that it satisfies the properties of Confusion and diffusion and also has a perfect guess of encryption key makes decryption impossible. This Encryption uses only integer arithmetic and it can be easily implemented in the hardware. [5].

4. Conclusion

The salient features of the proposed asymmetric image encryption scheme can be summarized as: (a) Lossless encryption of image. (b) Less computational complexity. (c) Convenient realization. (d) Choosing a suitable size of matrix according to the size of image. (e) Encryption/decryption scheme uses integer arithmetic and logic operations. Both colour and black & white image of any size saved in tagged image file format (TIF) can be encrypted & decrypted using blowfish algorithm. MREA algorithm is used to encrypt files and transmit encrypted files to other end where it is decrypted. Main feature of this method is that it satisfies the properties of Confusion and diffusion and also has a perfect guess of encryption key makes decryption impossible.

5. Future Scope

In this paper we analyze that the process of encryption and decryption is perform by using DES, AES and RSA algorithms. In future we will apply and implement these processes for secure and better communication.

Reference

[1] Amrita Sahu, Yogesh Bahendwar, Swati Verma, Prateek Verma, "Proposed Method of Cryptographic Key Generation for Securing Digital Image", International

Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 10, October 2012.
[2] Irfan.Landge, Burhanuddin Contractor, Aamna Patel, Rozina Choudhary, "Image encryption and decryption using blowfish algorithm", World Journal of Science and Technology 2012, 2(3): 151-156.
[3] Rajan.S.Jamgekar, Geeta Shantanu Joshi, "File Encryption and Decryption Using Secure RSA", International Journal of Emerging Science and Engineering (IJESE), Vol-1, Issue-4, February 2013.
[4] Akanksha Mathur, "A Research paper: An ASCII value based data encryption algorithm and its comparison with other symmetric data encryption algorithms", International Journal on Computer Science and Engineering (IJSCE), Vol. 4 No. 09 sep 2012.
[5] Monisha Sharma, Chandrashekhar Kamargaonkar, Amit Gupta, "A Novel Approach of Image Encryption and Decryption by using partition and Scanning Pattern", International Journal of Engineering Research & Technology (IJERT), Vol. 1, Issue 7, September- 2012.

Author Profile

Vikas Agrawal is persuing Bachelor of Engineering (CSE) from Shri Shankaracharya Institute of Professional Management & Technology, Raipur and presently is in Final Year. His research interests are Data Structure, Computer Networks, Operating System and Cryptography.

Shruti Agrawal is persuing Bachelor of Engineering (ET&T) from Shri Shankaracharya Institute of Professional Management & Technology, Raipur and presently is in Final Year. Her research interests are Communication System, VLSI, Cryptography and Computer Networks.

Rajesh Deshmukh received Master of Technology in C.S.E. from Chhattisgarh Swami Vivekanand Technical University, Bhilai. Currently he is perusing Doctor of Philosophy in CSE from Dr. C.V. Raman University, Bilaspur and working as Assistant Professor in Shri Shankaracharya Institute of Professional Management & Technology (Department of Computer Science Engineering), Raipur, India. He has published more than 15 research papers in various National / International Journals and Conferences. His area of research includes Mobile Ad hoc Network Routing Protocols, Wireless Sensor Networks, Distributed System, Cloud Computing and Operating System.