Modern Approach: Text to Image Encryption Decryption Algorithm

Hemlata Parmar[1] Rajesh Tanwar[2] Archana Parmar[3]
[1]M.Tech. Scholar [2,3]Assistant Professor
[1,2,3]Department of Information Technology
[1,2,3]TIT&S Bhiwani, India

Abstract— During the last decades security of data has become a major issue. Encryption and decryption is one of the most prevalent and recognized technique. This is a very strong combination for secure communication. There are so many methods for encryption and decryption of data but in this paper, it has been tried to develop "Modern Approach: Text To Image Encryption And Decryption Algorithm." This technique maintains the security on communication channels and makes it difficult for the attackers/unauthorized users to predict the content, by using key generation, key exchange and binary complements for data (text/image) authentication.

Key words: Encryption, Decryption, Key Exchange, Binary Complements

I. INTRODUCTION

Cryptography is quiet instrumental in protecting data from theft or alteration. It is also being used for user authentication purposes. Generally, there are three types of cryptographic schemes used to accomplish these goals:

- secret key (or symmetric) cryptography,
- public key (or asymmetric) cryptography, and
- hash functions.

Increase in exchange of multimedia data over protected and unprotected networks like worldwide available internet and other local networks has encouraged data breach activities such as unauthorized access, illegal usage, disruption and alteration of transmitted or stored data.

This far and wide use of digital media sharing on internet and its storage on local hardwares and on cloud storage systems have increased significantly over the past few years. New and latest data protection techniques and cryptographic systems are needed to meet the current and future demands.

Security of data in transmission and storage has been a major concern for both the transmitters and receivers; hence the security of cyber physical infrastructures as well as their underlying computing and communication architectures and systems becomes a priority of every institution.

Cryptography is the fundamental platform of modern information security that uses the advanced mathematical approaches in solving hard cryptographic issues. It has gained its foothold in the digital world.

The originator of an encrypted message share 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, such crypto-methods have become very complex and its application is widespread. Cryptography includes the following process

A. Symmetric-Key Cryptography

Symmetric-key cryptography refers to methods in which both the sender and receiver share the same key. Symmetric-key encryption can use either stream ciphers or block ciphers.

- Stream ciphers encrypt the digits (typically bytes) of a message one at a time.
- Block ciphers take a number of bits and encrypt them as a single unit, padding the plain text so that it is a multiple of the block size. Blocks of 64 bits have been commonly used. The Advanced Encryption Standard (AES) algorithm

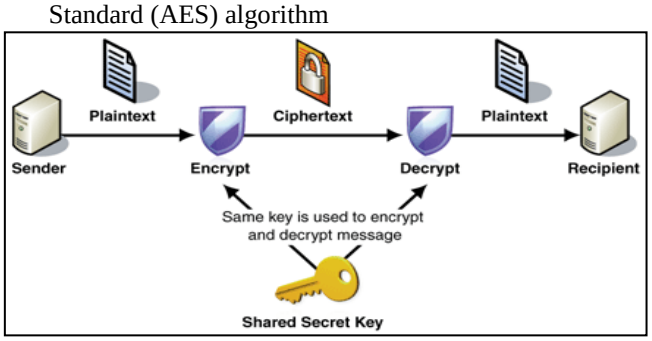

Fig. 1: Symmetric-key Cryptography

Symmetric ciphers have historically been susceptible to known-plaintext attacks, differential cryptanalysis and linear cryptanalysis. Careful construction of the functions for each round can greatly reduce the chances of a successful attack.

B. Asymmetric-Key Cryptography

In a public-key encryption system, any person can encrypt a message using the public key of the receiver, but such a message can be decrypted only with the receiver's private key.

For this to work, it must be computationally easy for a user to generate a public and private key-pair for encryption and decryption. The strength of a public-key cryptography system relies on the degree of complexity of computational impracticality. Security then depends only on keeping the private key private, and public key may be published.

An asymmetric cryptosystem (or public-key cryptosystem), keys exist in pairs:

- A public key for encryption;
- A secret key for decryption.

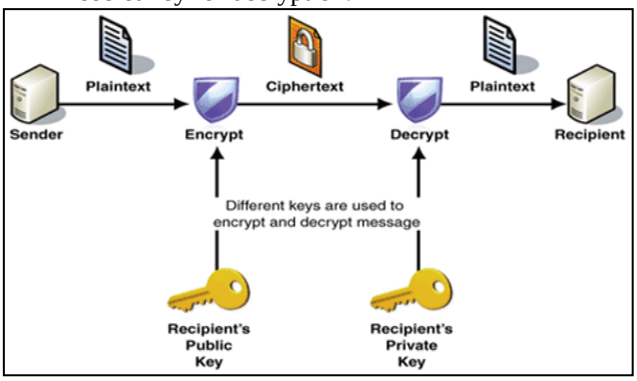

Fig. 2: Asymmetric Cryptosystem

Public-key cryptography systems often rely on cryptographic algorithms based on mathematical problems (like integer factorization, discrete logarithm, and elliptic curve relationships.) It does not provide a well-organized technique for securing the data.

1) Few well-regarded asymmetric key techniques for varied purposes

- Diffie–Hellman key exchange protocol
- DSS (Digital Signature Standard), which incorporates the Digital Signature Algorithm
- ElGamal
- Various elliptic curve techniques
- Various password-authenticated key agreement techniques
- Paillier cryptosystem
- RSA encryption algorithm

II. Encryption and Decryption

The main feature of the encryption/decryption program is the generation of the encryption key. Now days, cryptography has many commercial applications. If it is protecting confidential information then cryptography provides high level of privacy of individuals and groups.

The main purpose of the cryptography is not only to provide confidentiality, but also to provide solutions for other problems like: data integrity, authentication, non-repudiation. Cryptography is a method that allow information to be sent securely in such a way that the only receiver able to retrieve this information.

Presently, constant researches on the new cryptographic algorithms are going on. It is very difficult to identify the algorithm used to protect any particular communication as there are several underlying factors used to create one. Two notable factors are: the time complexity and space complexity.

If taking about security of information then there are following principles

- Confidentiality (privacy)
- Authentication (who created or sent the data)
- Integrity (has not been altered)
- Non-repudiation (the order is final)
- Access control (prevent misuse of resources)
- Availability (permanence, non-erasure)

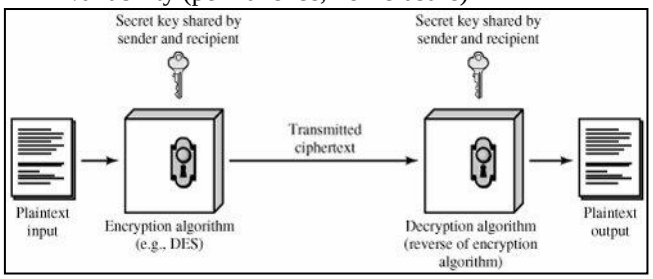

Fig. 1: A Simplified Model of Conventional Encryption Security Services

A. Modern Approach: Text to Image Encryption Algorithm

- Step 1: Take input String character by character.
- Step 2: Convert each cha racter into its corresponding ASCII-7 bit code.
- Step 3: Convert ASCII-7 bit code into 8 bit code placing MSB bit position into 0 to 127.
- Step 4: Divide 8 bit code into 2 equal parts take 4 bits of MSB (M) and remaining 4 bits of LSB (L) together.
- Step 5: Reverse L (4 bits) and then complement it to get L1 (4 bits).
- Step 6: XOR L1 (4 bits) with M (4 bits) to get M1 (4 bits).
- Step 7: Select 8 bit Key.
- Step 8: Divide 8 bit Key into 2 equal parts taking 4 MSB bits (MK) and remaining 4 bits of LSB (LK).
- Step 9: First select MSB bit of L1 and place it on starting MSB position of 8 bit code and then select MSB bit of LK and place it on next position of 8 bit code then repeat the step alternatively and generate 8 bit code from MSB to LSB (C1).
- Step 10: Repeat step 9 and replace L1 with M1 and LK with MK and generate 8 bit code (C2).
- Step 11: Arrange C1 and C2 in array respectively.
- Step 12: Take difference between MK and LK values get N.
- Step 13: Repeat Step 4 to 10 again for N number of times choosing array element C1 and C2 respectively and arrange the result of each number into new array then repeat remaining steps for (N-1) Number of times for new array containing new elements until N not becomes 0.
- Step 14: Get array row for each character.
- Step 15: Select first element of array row and Ex-OR it with resultant of key i.e (First complement key and then right circular shift 3-bit) and then repeat same process of complement and the right circular shift 3-bits sequentially once again on previous resultant to get next resultant in a sequence and Ex-OR with next element and so on. Get the encrypted array row.(use last resultant value key as first resultant key for next array row first element sequentially)
- Step 16: Arrange Encrypted array rows for each character into 2-D array row-wise A.
- Step 17: Convert array A into Grayscale Image.
  Send (key) from secure channel at the end.

B. Modern Approach: Text to Image Decryption Algorithm

- Step 1: Take received Grayscale image.
- Step 2: Get the 2-D array A of gray scale image.
- Step 3: Repeat steps 4 to 16 to get each character of string to each encrypted array row of A.
- Step 4: Take key of 8-bit.
- Step 5: Select first element of encrypted array row and Ex-OR it with resultant of key i.e (First complement key and then right circular shift 3-bits) and then repeat same process of complement and right circular shift 3-bits sequentially once again on previous resultant to get next resultant in a sequence and Ex-OR with next element and so on. Get the array row. (use last resultant value key as first resultant key for next array row first element sequentially)
- Step 6: Divide Key into 2 equal parts and convert the MSB-4 and LSB-4 bits into MK and LK respectively.
- Step 7: Get the difference of MK and LK as N=|MK-LK|.

- Step 8: Repeat Steps 9 to 14 for N+1 number of times choosing pairs of 2 Number of array Row-wise as C1 and C2 as 8 bit code every time till we reach to last pair of elements then arrange it into a new array n so on repeat till we get Single element.
- Step 9: First select MSB bit of 8-bit code (C1) and place it on starting MSB position of 4 bit(L1) and then select next bit of 8-bit code (C1) and place it on MSB position of 4-bit(LK) then repeat the step alternatively and generate 4 bit code L1 and LK from MSB to LSB (C1).
- Step 10: Repeat step-9 for 8-bit code (C2) Similarly and get M1 and MK respectively as like L1 and LK.
- Step 11: Combine MK at MSB positions 4 bits and place LK at LSB position 4 bits to get Key-1 and check it with received key.
- Step 12: XOR L1 (4 bits) with M1 (4 bits) to get M (4 bits).
- Step 13: Reverse L1 (4 bits) and then complement it to get L (4 bits).
- Step 14: Combine 4-bits of MSB (M) and remaining 4 bits of LSB (L) together to get 8 bit code.
- Step 15: Convert 8-bit code into ASCII 7-bit code extracting MSB bit position.
- Step 16: Convert each character into its corresponding ASCII-7 bit code.
- Step 17: Get the Decrypted Text

C. Languages Suitable For AIEDA

This algorithm can be implemented in all the languages which carry Unicode system facility like Java, C# .Net, etc. Also, this can be implemented using C/C++ subject to few limitations. I used the MATLAB tool for this algorithm.

III. CONCLUSION AND FUTURE SCOPE

In this paper we have introduced the new encryption techniques along with a secure policy based routing. The algorithm is successfully tested on text file. The proposed direction for the future work could be to analyze following factors:

1) Hardware implementation of this algorithm.
2) Introduced more security by finding out the pitfalls of the algorithms.
3) Compression techniques could be implemented along with encryption procedure.

REFERENCES

[1] Computer Networks, by Andrew S. Tanenbaum, Fourth Edition, Prentice hall, 2004
[2] P.Gope, "Extended Multi Operator Delimiter Based Data Encryption Standard(XMODDES)" ICFN, 2010, China.
[3] D. Clark, Policy Routing in Internet Protocols, RFC 1102, SRI Network Information Center, May 1989.
[4] Y.Rekhter,T. Li,S.Hares, "A Border Gateway Protocol 4(BGP-4),"RFC 4271,June 2006.
[5] "Constraint-Based Routing in the internet: Basic Principles and Recent Research." www.comsoc.org/pubs/surveys.
[6] E.Crawley et al., "A Framework for QOS-based Routing in the internet," RFC 2386,Aug 1998
[7] D. Awduche et al., "Requirements for traffic Engineering over MPLS,"RFC 2702, Sept.1999.
[8] P. Gope "An efficient cryptographic approach for secure policy based routing: (TACIT Encryption Technique)" ICECT, 2011 Kanyakumari, India.

