Hybrid Cryptography for Secure Data Transmission Using Public Network

JitendraSoni

Institute of Engineering & Technology, Devi Ahilya Vishwavidyalaya, Indore, M.P., India.

***Abstract*- In the 21st century internet has become a booming technology for information exchange; the basic technique in use is Cryptography. It is an art to achieve security by making the data to non - readable format, it converts plaintext to cipher text, and this scheme of transforming plaintext to cipher text is called cryptography. There are so many cryptographic techniques available. Like symmetric key cryptography, asymmetric key cryptography and combination of all. But as the most secure algorithm can be breached, proposed work will address some of the key issue and their solution.**

Keywords: Encryption, Decryption, cryptography, cryptanalysis MD5, RSA, IDEA.

I. INTRODUCTION

This paper will propose secure cryptographic technique that will improve the security over internet using hybrid cryptography [1].

A. *Overview*

Increasing trend of data transmission using applications using mobile internet and public internet make data vulnerable, to secure the data we use cryptography. There are a few terms related to these techniques.

B. *Principles of Security*

There are mainly four types of Security Principle claimed by Cryptography Technique

1) *Confidentiality*

It specifies that only the sender and the recipient should be able to access the data or to access the contents of a message. If a person in between the sender and a receiver looks all the information transmitted from sender to receiver, this breach of confidentiality is called interception and the person is called Intruder.

2) *Integrity*

Message send by the receiver should not be changed in between sender and the receiver, when the receiver receives the message it should be same as sender's message, if there is change in the message it is called modification.

3) *Authentication*

It helps to establish proof for the identity of the user. In the Internet era when billions of users transmit data or fetch data from public network it is important that one must have credentials to access the resources over Internet.

4) *Non Repudiation*

After sending a message to receiver if a sender refutes the claim of not sending that message then what? Non Repudiation does not allow the sender to do that.

II. CRYPTOGRAPHY

This section contains basic terminology used in secure data transmission technique.

1) *Cryptology*

This is a combine technique of cryptography and cryptanalysis.

2) *Cryptanalysis*

It is a technique of decoding a message to non readable format back to readable format.

3) *Plain Text*

It is also called clear text. Message in plaintext can be understood by anybody who knows the language. “Hello world”. This is simply written in English language and anybody who knows English can understand the message written.

4). *Cipher text*

Message in unreadable form is called cipher text. It may be that the message still in readable format but not easy to understand.

“Hello world” can be written as “Ifmmpxpsme”by using simple substitution.

But IFMMP XPSME itself does not have any meaning.

5). *Encryption*

Technique to convert plain text to cipher text is called Encryption. Encryption takes place at the sender side. [4]

6) *Decryption*

Technique to convert cipher text to plain text is called Decryption. It takes place at receiver's side.

7) *Cryptographic* Algorithm

An algorithm that converts plain text to cipher text.

8) Public key

Key that is known to everyone.

9) *Private Key*

Key that is known to receiver only [2].

III. CHARACTERISTIC OF CRYPTOGRAPHY

- It is very logical to characterize cryptography and it is quite complicated because almost all the algorithm works in different manner but there are certain features that can be characterize [3].

- Functions: Message secrecy, message integrity, authentication, digital signatures

- Complexity: Complexity of the algorithm depends on Key operations like key generation, bit operations like shift the key or modification or extraction some of the key values from data in order to generate key, Operation for Encryption, Decryption and the size and amount of data as well as size of the key and its time taken to Encryption and Decryption. Modular approach can only increase implementation speed but cannot increase the number of operations.

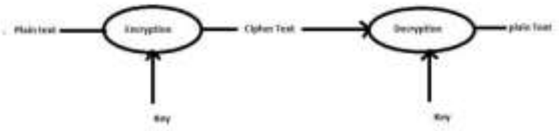
- Strong point of the algorithm rely on the sort of the key and its length, but it also depends on the type of algorithm.

IV. TYPES OF CRYPTOGRAPHY

There are essentially two sorts of cryptography based on the unique key or two key it practises for Encryption and Decryption.

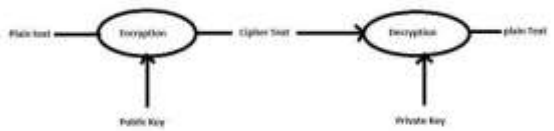
1) *Symmetric key cryptography*

Cryptographic skill where solitary one key is castoff for Encryption and Decryption.



2) *Asymmetric key cryptography*

Cryptographic skill where open key is castoff for Encryption and reserved key is castoff for Decryption.



V. PREVIOUS WORK

- This section provides the study on the recent contribution placed in the domain of hybrid cryptography. As per **Mohammad Reza Najaf[5]** there occurs a request for pioneering protected electronic communications knowledge attacker are growing rapidly. There is a necessity of idle safety protocol that leaves no trapdoor for attacker, DNA steganography is described as an inventive standard to reduce the practice of public cryptography to interchange session key. In this etiquette, session key amongst a source and receiver is concealed by novel DNA data hiding technique. Consequently, the enemies are not alert of communication of session key over unsecure channel.

- **Georgiana Mateescu et al [6]** want to verify their effectiveness by equating the diverse types of crypto algorithms and by awarding their weaknesses and strengths. In directive to maximize the benefits of the crypto techniques, we recommend a hybrid methodology that associates three crypto algorithms.

- **Hatem M. Abdul Kader et al [7]** suggests a novel cross cryptographic system. The system is deliberated using blend of two symmetric cryptographic practices and two Asymmetric cryptographic practices. This conventions affords three cryptographic primitives, integrity, confidentiality and authentication. It is a amalgam encryption means where elliptical curve cryptography (ECC) and advanced encryption (AES) are joint to deliver node encryption. (RSA) algorithm and (Blowfish) are pooled to offer authentication and (MD5) for integrity. We applied this protocol on one type of wireless sensor network (Zigbee) to be evaluated and compared it with other four hybrid cryptography protocol. The outcomes display that the anticipated fusion cryptographic algorithm provides improved performance in terms of calculation time and the size of cipher text.

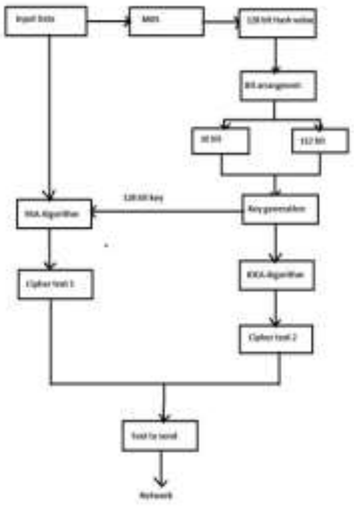
- **Omar M.Barukab et al [8]** anticipated a methodology to defend safe and secured transfer of data or information for satellite centred communication using symmetric and asymmetric cryptographic skills.

- **Prokash Barman et al [9]** propose a new hybrid DNA encoded Elliptic Curve Cryptography scheme in this paper. DNA encoded ECC cryptography uses smaller key size and less computation power with multilevel security. The main attraction of the proposed system is that it has two level of security. First is unknown DNA sequence based encoding and the second is Light weight ECC based encryption and decryption system.

VI. PROPOSED METHODOLOGY

Overview of the proposed methodology covered in this section

- **Encryption process**

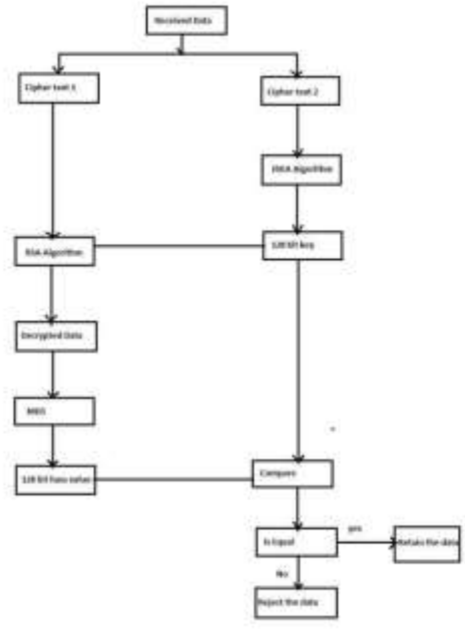


1. Encryption process

Figure shows the Encryption Process that will convert normal file to unreadable file. During this process user need to Encrypt the file using Hybrid cryptographic algorithm.

Input file will first be processed using Message Digest (MD5) to generate 128 bit data, bit arrangement will rearrange the first bit of each 16 block of 8 bit and append it to last of the bit stream. This 128 bit key then used as key for RSA to convert data or file to cipher text. Key will be processed again with IDEA that will again produce a different cipher text. Combination of these two cipher text is ready to be send over the network.

- **Decryption Process**



2. Decryption Process

Figure shows the reverse process of Encryption process, the received data will then again is separated, second part of that cipher text will again processed with IDEA to generate 128 bit key. Bit will be rearranged, and will be used by RSA to generate decrypted data Message Digest of the key then compared to check the integrity of the data.

VII. APPLICATION DOMAINS

Secure data transmission using private network: with this hybrid approach. It will be virtually impossible to decrypt the data for any attacker.

Disk utilization: for host based application less data will be generated as output after Encryption. It will also affect data transfer rate that will be improved after this algorithm because data will be less and there will be no need to apply further Encryption and Decryption.

VIII. EXPECTED OUTCOMES

Implementation of the proposed cryptographic algorithm may secure the channel using newly derived technique, every algorithm used in this process is Linear and can't be rolled back so it will improve the following:

- Cipher text will be reduced.
- It will decrease the Space and Time complexity.
- Nearly impossible man in the middle attack.
- Efficient and robustness.

IX. CONCLUSION

Proposed algorithm is based on hybrid technique of Cryptography it uses asymmetric key that is sender and receiver's key and symmetric key that is used by both sender and receiver for Encryption and Decryption, algorithm is secure because the key is generated secretly. Hybrid RSA with IDEA is quite complex to implement as well as for as hacker is concerned nearly impossible to break.

REFERENCES

[1]D Elizabeth Rob, l Denning, "Cryptography and Data Security", http://faculty.nps.edu/dedennin/publications/Denning -CryptographyDataSecurity.pdf

[2] V Gampala, S Inuganti, S Muppidi, "Data Security in Cloud Computing with Elliptic Curve Cryptography", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-3, July 2012

[3] N D. Jorstad, L T. Smith Jr, "Cryptographic Algorithm Metrics", Directorate for Freedom of Information and Security Review (OASD-PA) Department of Defense, January 1997

[4] S J Lin and W H Chung, "A Probabilistic Model of Visual Cryptography Scheme With Dynamic Group", IEEE Transactions On Information Forensics And Security, Vol.7, No.1, February 2012

[5] Mohammad Reza Najaf Torkaman, Nazanin Sadat Kazazi, AzizallahRouddini, "Innovative Approach to Improve Hybrid Cryptography by Using DNA Steganography", International Journal on New Computer Architectures and Their Applications (IJNCAA) 2(1): 224-235

[6] Georgiana Mateescu, Marius Vladescu, "A Hybrid Approach of System Security for Small and Medium Enterprises: combining different Cryptography techniques", Proceedings of the 2013 Federated Conference

[7] Hatem M. Abdul Kader, Mohie M. Hadhoud, Salah M El-Sayed, DiaaSalamaAbdElminaam, "Performance Evaluation Of New Hybrid Encryption Algorithms To Be Used For Mobile Cloud Computing", INTERNATIONAL JOURNAL OF TECHNOLOGY ENHANCEMENTS AND EMERGING ENGINEERING RESEARCH, VOL 2, ISSUE 4 63

[8] Omar M.Barukab, Asif Irshad Khan, MahaboobShariefShaik , MV Ramana Murthy, "Secure Communication using Symmetric and Asymmetric Cryptographic Techniques", I.J. Information Engineering and Electronic Business, 2012, 2, 36-42 Published Online April 2012 in MECS.

[9] Prokash Barman, BananiSaha, "An Efficient Hybrid Elliptic Curve Cryptography System with DNA Encoding", International Research Journal of Computer Science (IRJCS) ISSN: 2393-9842 Issue 5, Volume 2 (May 2015).