# REVIEW PAPER ON NETWORK SECURITY EMAIL ENCRYPTION

[1]Jyoti Yadav , [2]Taruna Jangra
[1]Student, [2]Teacher
[1]Department of computer Science and Engineering of DPGITM,
[1]Maharshi Dayanand University, Haryana,
India

***Abstract :*** As there is a rapid increase in computer application of mobile and wireless network has changed the features of network security. Nowadays, there is an increase in internet attack and some fraudulent acts on companies and also on some individual networks. The way of protecting the computer networks are firewalls and security encryption are not sufficient and effective. Network security has become very important to personal computer users, organizations, and the military. In this paper RC4 based encryption algorithmic rule is pre-owned to secure Email communications. With the advent of the internet, security became a major concern and the history of security allows a better understanding of the emergence of security technology. Due to rapid requirement of computer's in business and other organizations many networks has been established. Nowadays, attacks on computer networks has increased to a great extend. So, there is a need of some methods for developing new mechanisms to protect wireless networks and mobile applications. This paper will be very important and useful for the network security. As there are many types of attacks which can be penetrated in our networks or edge devices. In this paper we would analyze different available mechanism to protect our network.
Inside the day to day life people constantly uses communication tools that are e-mail promotional, instant communicating, social networking, search engines, bookmarking systems, affiliate systems, print media and direct mail. The encryption and decryption techniques are configured to manage with this security interval.

***IndexTerms*** – **Decryption , Electronic Mail Security, Encryption, POP3, RC4 Algorithm, SMTP.**

## I. INTRODUCTION

Cryptology name appears from ‘kryptos logos’ in Greek language. The intention of the cryptology is to guarantee secure conversation via secure medium among transmitter and receiver sides who requires to secure conversation (sent or receive) in insecure conversation zone. Fig. 1 shows that recognitions to encoding system 3th individuals (theft) doesn’t suggesting the cipher sentence indeed if convinces it. Fig 1: Communication paths above unstable area There are essentially two groups of encryption algorithmic program which are called as symmetric within which encryption and decryption keys are the same or asymmetric in which encryption and decryption keys are different from each other .Inside this paper symmetric encryption algorithmic rule is used for secure Electronic communication Mail (Email) system. The protection of this symmetrical cryptosystem, should not rely on the secrecy of the algorithmic rule, it be based on the secret of keys. There are two kinds of symmetrical encryption algorithms. These are; stream ciphers and block ciphers which contribute bit-by-bit along with block encryption severally. In this paper, RC4 established encryption algorithmic rule applied that is stream cipher was invented in 1987 by Ron Rivest. Acknowledgements to its effectiveness and simpleness, it was used many protocols and levels such as Secure Socket Layer (SSL) to secure internet traffic, Wired Equivalent Privacy (WEP) to secure wireless communication, Wi-Fi Protected Access (WPA) to secure conversation on data link layer preferably of WEP, and Transport Layer Security (TLS) to secure conversation on transport layer .There are various protocols, patterns, systems contribute secure Email system. In primary Email system each person should encrypt their Email. Public Key Infrastructure (PKI) is a foundation that permits individuals of such networks to exchange information by way of the use of a public and private key pair that is obtained as well as shared by way of a trusted authority was utilization secure Email systems. However, Email communicators must also improve a recipient’s public key before encrypting an Email in PKI systems. To solve this problem identity-based encryption (IBE) can be used. The text value of the name/domain name or internet protocol (IP) address is used as key in IBE. In the literature there are some patterns of secure email established system. Lu and Geva represent the implementation of a distributed search engine called SEGPX based on secure email communication. It uses X.509 Public key and attributes systems and uses email servers for associations.

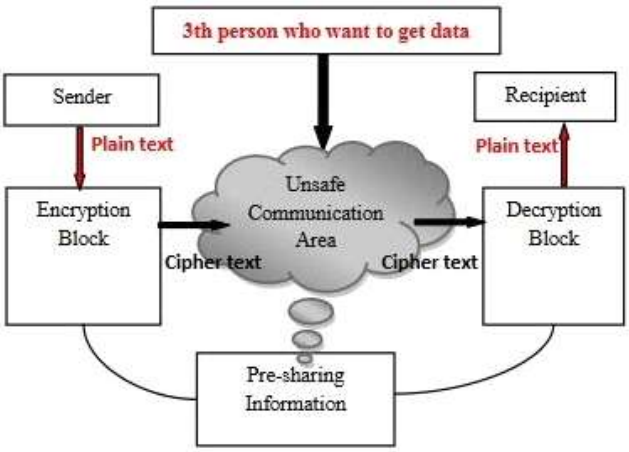


**Fig 1: Communication channels over unsafe area**

.

## II. LITERATURE SURVEY

Existing Schemes to Secure Email System. The most of client-based electronic mail security measures are based on Identity-Based Cryptography or Public Key Infrastructure (PKI) schemes. The preceding security functions are present enforced by these solutions, of which the most reasonable ones are S/MIME and PGP. PGP uses hash purposes and public key encryption algorithms, for example, RSA and MD5, to allow encryption for content-protection and digital signature for non-repudiation. RSA public keys are attached as PGP licences along accompanied by the message. Nevertheless, autographed PGP certificates are used for most users and form a chain-based credential confidence network. This trust method of PGP is only appropriate for small-scale parties and is not appropriate for large-scale parties or anonymous user conditions. Moreover, it is extremely difficult to inform other users in the arrangement, if the private key of a PGP individual has been compromised. S/MIME applies the PKI scheme. Due to the problem of document control in PKI, S/MIME cannot pay no attention to annoying operations, such as licence revocation, confirmation, and so on. Additionally, both S/MIME and PGP use RSA for encrypting and signing email contents. These results in lower effectiveness compared with Elliptic Curve Cryptograph (ECC) with the same level of security. In the IBC plan, it is complicated to prove the specification of the Trust Authority (TA) or the Key Generation Center (KGC). The plan also has trouble with from the difficulty of key escrow, where a central trusted police issues a private key to a someone. Because a central police is responsible for private key generation, it is experienced to work as an authorized individual and could maliciously read the incoming encrypted text or generate false signatures. Several methods have been projected to solve the key written agreement problem in IBC, including they can be clearly categorized into two parties based on the private key generation method:

(i)Multiple authority approach and

(ii) User chosen secret key details approach.

As per our study, numerous techniques accompany the multiple authority approaches, while very few techniques are supported on the secret key information approach. In the multiple police approach, the important task of private key generation is distributed in the midst of several authorities, and as a effect, no single authority can achieve any unauthenticated work. Though these processes favourably solve the key escrow problem, they introduce extra overhead on systems and lack of central control on key issuing policy and are not suitable for email systems. User-chosen secret facts approaches are either licence based or certificate less. The certificate-based a scheme completely overcomes key escrow; however, it loses the benefit of an ID-based scheme. The confidential key conversation protocol established system is also not suited for email systems because a recipient of the email system may not every time be online. Domain Keys Identified Mail (DKIM) permits individuals to claim some role for a message by identifying it with a name that they are recognized to use. This claim is valid through a cryptographic signature and by querying the Signer's domain straight to retrieve the appropriate public key. The approach taken by DKIM differs from previous approaches to message signing such S/MIME and Open PGP is that:

The communication signature is engrossed as a note header field instead of part of the message body, so that neither human recipients nor existing MUA (Mail User Agent) software are puzzled by signature-related content appearing in the message body.

There is no dominion on well-known trusted administration public and private-key pairs.

A new idea called Lightweight Signatures for Email (LES), proposed by Ben Adida, David Chau, Susan Hohenberger, and Ronald L. Rivest, is an extension to DKIM. In LES, particular users verify within a domain, without depending upon extra user validation infrastructure. LES provides a user to send mails via any outgoing mail server, not just the official outgoing mail server

mandated by DKIM. LES also supports repudiable signatures to protect users' privacy. Both DKIM and LES focus only on email authentication. LES requires a restricted email client for authentication. The scheme described as "An End-to-End Secure Mail System Based on Certificateless Cryptography in the Standard Security Model" based on of Certificate-less Public Key Cryptography (CL-PKC) is not suitable for concrete implementation with separate domains. None of these trades are acceptable. Therefore, effective email security systems are in great need .This paper proposes a practical implementation of a secure email system using certificateless cryptography as alternative technology for avoiding the difficulties with PKI and IBC based mailing systems.

## 1.**RC4 ALGORITHM**

There are two basic cryptographic algorithms; these are.

- symmetric algorithms
- asymmetric algorithms

Cryptographic code of actions use cryptography, is arrangements of actions, which are concern two or more margins, developed to accomplish a goal. A stream cipher is a symmetrical algorithm that has two type kinds called as synchronous stream cipher along with self-synchronizing stream cipher. The RC4 is a stream cipher, as mentioned before it used lots of standards and protocols for example in the SSL/TLS standards that have been defined for communication between Web browsers and servers. It also used in WEP protocol and WPA protocol. It adds two phases, key structure and ciphering. Both phases must be performed for every new key. During an l-bit key setup (l is the key length) the encryption key is used to produce an encrypting variable using two arrays, state and key, and l-number of mixing operations . The algorithm is based on the use of random permeation. The key stream is entirely separate of the plaintext used. The algorithm uses a variable length key from 1 to 256 bytes to initialize a 2-byte array. The array is used for emerging generation of pseudo-random byte and then produces a pseudo random stream, which is XORed with the plaintext/ciphertext to give the ciphertext/plaintext .As S = {0, 1, 2 ... N-1} is the initial permutation, two parts of the RC4 algorithm which are Key Scheduling Algorithm and Pseudo Random Generation Algorithm, their pseudo codes are given in

**Strengths of RC4**

- The difficulty of knowing where any value is in the table.
- The difficulty of knowing which location in the table is used to select each value in the sequence.
- Encryption is about 10 times faster than DES.

**Limitations of RC4**

- RC4 is no longer considered secure.
- One in every 256 keys can be a weak key. These keys are identified by cryptanalysis that is able to find circumstances under which one of more generated bytes are strongly correlated with a few bytes of the key.
- A particular RC4 Algorithm key can be used only once.

To initiate the performance of RC4 encryption, you require a key, which is often user-defined and among 40-bits and 256-bits.A 40-bit key serves as a five character ASCII code that becomes converted into its 40 character binary equal (for example, the ASCII key "pwd12" is equivalent to0111000001110111011001000011000100110010 in binary).
The next proportion of RC4 is the key-scheduling algorithmic rule (KSA), listed below for

- for i from 0 to 255
- S[i] := i
- endfor
- j := 0
- for i from
- 0 to 255
- j := (j + S[i] + key[i mod keylength]) mod 256
- swap(S[i],S[j])
- endfor

## 2. SMTP AND POP3

SMTP is a code of behaviour that sent Email messages on top of the Internet between transmitter and receiver side's information processing system, only works for social messages. While sending Email, most of Email software is planned to use SMTP. It terminates dissimilar shares of the message into groupings so that it maintains important conversation among two servers. The communications can at that time be retrieved accompanied by an Email client employing either POP or Internet Message Access Protocol (IMAP). POP, that is a protocol, has two forms POP2 and POP3. POP2 became a grade in the mid- 80's and depends upon SMTP to convey messages. POP3 is the newer version that can be used with or lacking SMTP. IMAP is a protocol. Latest form IMAP4, is similar to POP3. All of them deal with getting of Email on the server.
In this work POP3 is used seeing as of it is understandable and well- supported. In order to connect to the Internet, parties need an Internet Service Provider (ISP).
Fig. 2 shows Email code of behaviour in the middle of transmitter and receiver. First step sender builds his/her mail, Email customer forwards this mail to the SMTP server. At that time the SMTP host delivers the mail to the receiver's mailbox. The POP3 server holds the communication for delivery to the receiver. Finally, the receiver retrieves the communication using the POP3 protocol.

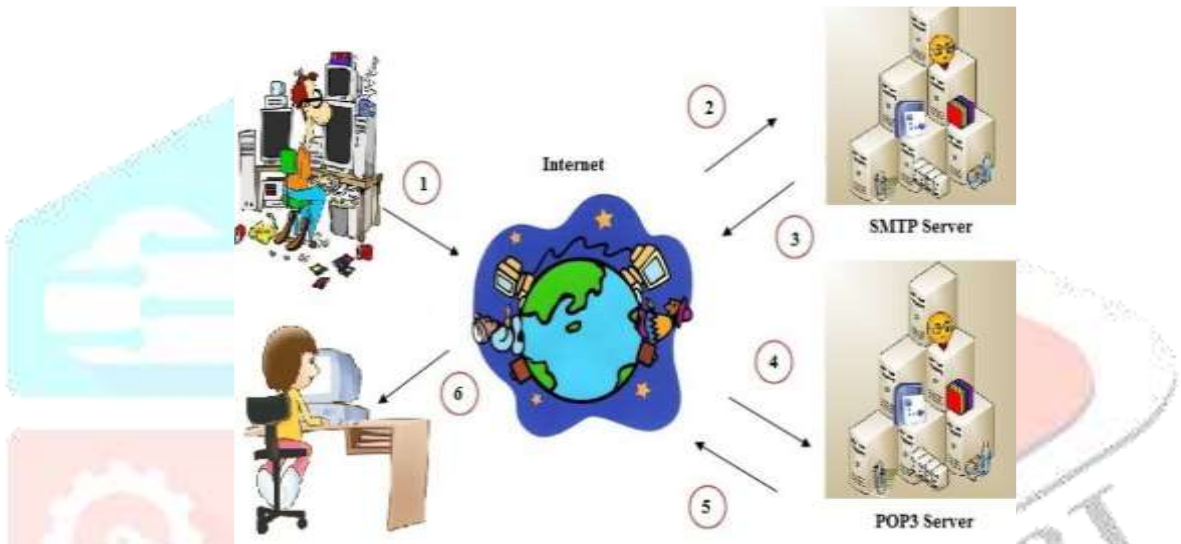


**Fig 2: Email protocols between sender and recipient**

As mentioned before credits to the internet, people can initiate real-time communication with everybody they want. It provides with lots of facilities like Email, video conferencing, chat etc. Internet possesses groups of advantages nevertheless there are some drawbacks. One of them together with the most significant is security gap. In the dangerous and unsafe area produces our private and secret information susceptible to third persons who wish for to steal this information. The other is e-mailing, it refers to forwarding unwanted mails that make lazier to access our Email accounts. To manage with security difficulty, especially safe messaging, suggested use of MRC4 encryption algorithm while sending mail to the recipient. Thus, mails can be protected from thefts.

## III. METHODOLOGY

Planned approach in this paper has four classes. These are new message, default, messages and MRC4. java programming language is used.
The new message class put together new Email package deal and then Email object and content is encrypted using encrypt approach in the MRC4 class. In the default class, POP3 and SMTP servers' session instruction is registered. At that time this incoming information is through to the messages class. In the messages class joins to the POP3 server, encrypted Email is decrypted with decrypt process in MRC4 class. Fig. 3 is a flow diagram that shows steps of new message form. Firstly the Email package is composed than Email subject and Email content are encrypted with MRC4 algorithm. SMTP customer is composed, after that use details is entered to the client. Using SMTP customer Email collection is sent.

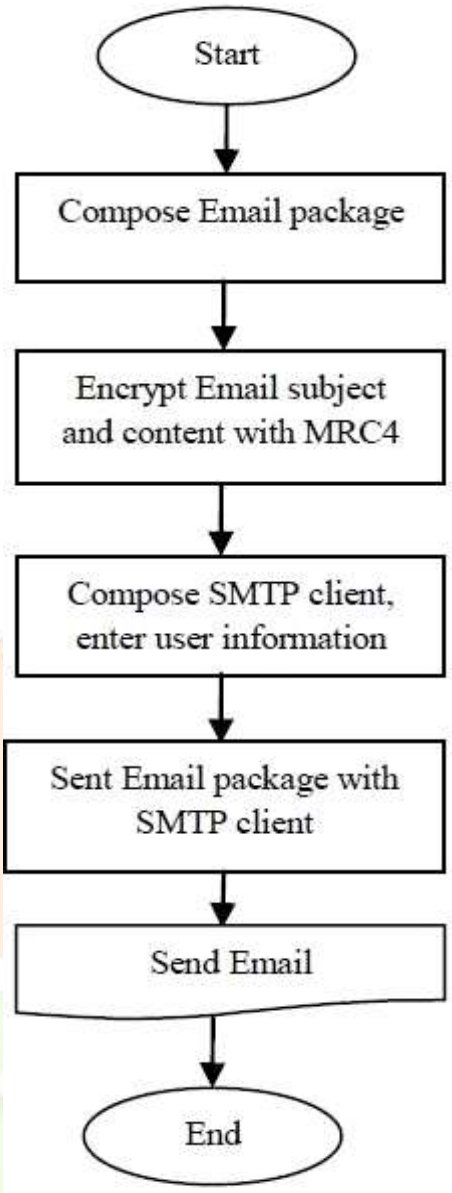


**Fig 3: Flowchart of sending Email**

In the MRC4 class, before encoding subject and content of the mail with MRC4, conceding to our Email encryption organization sender and recipient use Elgamal encryption system for key contract to work out the RC4 key administration points that was recommended in . Structure of the key agreement is given Fig. 4.

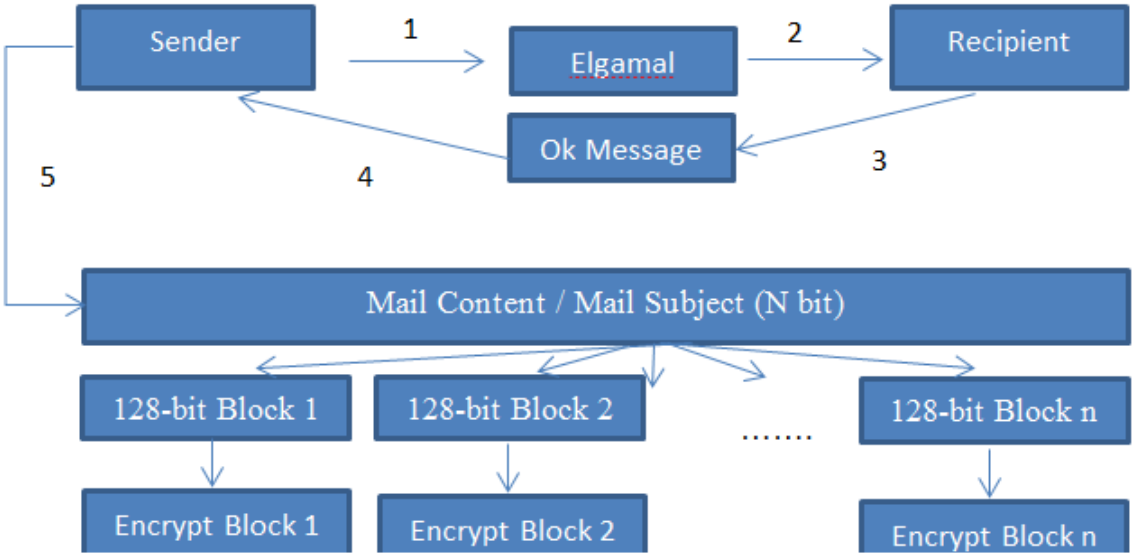


**Fig 4: The encryption process of each block with MRC4 algorithm**

## IV. CONCLUSION

To review the state of safe e-mail software, we can declare that software is present now to set up trust among two parties or within a small party so they can exchange text-based e-mail. Such application has really been free for some time, but the standard and ease of use of accessible executions has recently begun to enhance. Software is free to secure MIME-based e-mail in a analogous manner, though it is not about as universal and is mostly available commercially.

Local certificate administrations are continue deployed and large development is being made, however they are not yet popular or mature. As their utilization increases and as a popular protection structure is improved, it will become within the bounds of possibility to acquire all e-mail you send and accept. Software for use by single associations to found enterprise wide authorization authorities has also become more commercially available. This will enable companies to secure their conversations independent of any public licence authorities.

In spite of the seeming confusion of levels, there is important hope that ability will exist for safe e-mail. The algorithmic rule, licence formats, and trust control systems being enforced today will likely become standard to most of the dissimilar e-mail levels. Of the four elements discussed here, the message arrangement is the only one that truly cannot be common by different performances, but even there it is possible for extraordinary effecting to support multiple formats and levels. Thus, in the short term we can believe problems with ability, but in the expanded expression these are disposed to be resolved as individual demand for ability increases.

## REFERENCES

[1] Rivest, R., Shamir, A., and Adleman, L. 1978. A Method for Obtaining Digital Signatures and Public Key Cryptosystems. Communications of the ACM.

[2] Allam Mousa, Data Encryption Performance Based on Blowfish, 47th International Symposium ELMAR-2005 focused on Multimedia Systems and Applications, pp. 131- 134, Zadar, Croatia, 08-10 June 2005

[3] Madi, N. K. M., Salehian, S., Masoumiyan, F., and Abdullah, F. 2012. Implementation of Secure Email Server in Cloud Environment. International Conference on Computer and Communication Engineering (ICCCE).

[4]Fiuhrer, S., Mantin, A. and Shamir. 2001. Weaknesses in the key scheduling algorithm of RC4. 8th Annual International Workshop (SAC).

[5] David Groth, Network+ ™, Study Guide, Third Edition, SYBEX, Inc., Alameda, CA, 2002

[6] Glover, P. and M. Grant, Digital Communications, 2nd edition, Person Education, 2004

[7] Wenbo Mao, Modern Cryptography Theory and Practice, Prentice Hall, New Jersey, 2004