Email Encryption using RC4 Algorithm

Meltem Kurt Pehlivanoğlu
Department of Computer Engineering
Kocaeli University
Kocaeli, Turkey

Nevcihan Duru
Department of Computer Engineering
Kocaeli University
Kocaeli, Turkey

ABSTRACT

In the communication age, in the daily life people constantly uses communication tools that are e-mail marketing, instant messaging, social networking, search engines, bookmarking systems, affiliate systems, print media and direct mail. These tools are used as an internet communication. However as a result of widespread of internet usage, security problems have become more important year by year. Two main problems are related with internet an open system and unsafe area. The encryption and decryption systems are designed to cope with this security gap. In this paper RC4 based encryption algorithm is used to secure Email communications.

Keywords

Decryption, Electronic Mail Security, Encryption, POP3, RC4, SMTP

1. INTRODUCTION

Cryptology word comes from ‘kryptos logos’ in Greek language. The aim of the cryptology is to ensure safety communication via secure channel between sender and recipient sides who wants to secure communication (sent or receive) in unsafe communication area. Fig. 1 shows that thanks to encryption system 3th people (theft) doesn’t meaning the cipher text even if gets it.

Fig 1: Communication channels over unsafe area

There are basically two types of encryption algorithm which are called as symmetric in which encryption and decryption keys are the same or asymmetric in which encryption and decryption keys are different from each other [1].

In this paper symmetric encryption algorithm is used for secure Electronic Mail (Email) system. The security of this symmetric cryptosystem, should not rely on the confidentiality of the algorithm, it depends on the secret of keys. There are two types of symmetric encryption algorithms, these are; stream ciphers and block ciphers which provide bit-by-bit and block encryption respectively [2]. In this paper, RC4 based encryption algorithm used that is stream cipher was invented in 1987 by Ron Rivest. Thanks to its efficiency and simplicity it was used many protocols and standards such as Secure Socket Layer (SSL) to protect internet traffic, Wired Equivalent Privacy (WEP) to secure wireless communication, Wi-Fi Protected Access (WPA) to secure communication on data link layer instead of WEP, and Transport Layer Security (TLS) to secure communication on transport layer.

There are various protocols, standards, systems provide secure Email system. In early Email system everyone should encrypt their Email [3]. Public Key Infrastructure (PKI) is a framework that permits users of such networks to exchange data through the use of a public and private key pair that is obtained and shared through a trusted authority [4] was used secure Email systems. However Email senders must also look up a recipient’s public key before encrypting an Email in PKI systems [4]. To solve this problem identity-based encryption (IBE) [5] 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 designs of secure email based system. Lu and Geva [6] describe the implementation of a distributed search engine called SEGPX based on secure email communication. It uses X.509 Public-key and attributes certificate frameworks and utilizes email servers for communications. Jain and Gosavi [3] encrypt with variable key and compress with code book, compress message must encrypted is needs of today’s E-mail security in their paper. With encryption they maintain secure Email and with compression text is minimizing the overload of traffic over communication channel. Chen and Ma [7] proposed a novel proxy-based secure Email system using IBE cryptography. Li et al [8] analyze both the AES algorithm and the ECC algorithm. Combining with the characteristics of the AES and ECC they designed a mixed Email encryption system. Madni et al [9] have proposed a simple implementation of configuring a secure Email server in Linux platform (Ubuntu OS) to use Local-based Email Transfer Agent such as Postfix. Choukse et al [10] explain inherent weakness in email infrastructure and methodologies to improve the security of the email infrastructure and also will highlight good and weak practices in varying aspects of email infrastructure design paradigm in their paper. Yeh et al [11] introduces an identity-based one-way group key agreement protocol and describes a point-to-point email encryption scheme based on the protocol. Dacosta et al [12] present EmailCloak that an email alias service with public key encryption capabilities, relaxes email encryption requirements by relying on a privacy-respecting third-party. Ojamaa and Lind [13] proposed a solution based public key cryptography and OpenPGP to the costumers for more secure email communication.

RC4 algorithm is introduced in second section. The third section gives information about Simple Mail Transfer Protocol (SMTP) and Post Office Protocol 3 (POP3) servers.
The fourth section examines the improved method. Finally conclusion is given the fifth section.

2. RC4 ALGORITHM

There are two basic cryptographic algorithms; these are symmetric algorithms and asymmetric algorithms. Cryptographic protocols use cryptography, is sequences of actions, which are concern two or more sides, designed to fulfill a goal. A stream cipher is a symmetric algorithm that has two types called as synchronous stream cipher and 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 works in two phases, key setup 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 generate an encrypting variable using two arrays, state and key, and l-number of mixing operations [2].

The algorithm is based on the use of random permutation. The key stream is completely independent of the plaintext used. The algorithm uses a variable length key from 1 to 256 bytes to initialize a 256-byte array. The array is used for subsequent generation of pseudo-random bytes and then generates a pseudorandom stream, which is XORed with the plaintext/ciphertext to give the ciphertext/plaintext [14].

As $S = \{0, 1, 2 ... N-1\}$ is the initial permutation, two parts of RC4 algorithm which are Key Scheduling Algorithm and Pseudo Random Generation Algorithm, their pseudo codes are given in Table 1.

### Table 1. Pseudo Code for RC4 Algorithm

<table>
<thead>
<tr>
<th>Key Scheduling Algorithm (K)</th>
<th>Pseudo Random Generation Algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Initialization:</strong></td>
<td></td>
</tr>
<tr>
<td>for i = 0 to N-1</td>
<td>j = 0</td>
</tr>
<tr>
<td>S[i] = i</td>
<td>j = 0</td>
</tr>
<tr>
<td>T[i] = K[i mod l]</td>
<td></td>
</tr>
<tr>
<td><strong>Scrambling:</strong></td>
<td></td>
</tr>
<tr>
<td>j = 0</td>
<td>while (true)</td>
</tr>
<tr>
<td>j = (j + S[i] + T[i]) mod l</td>
<td></td>
</tr>
<tr>
<td>swap (S[i], S[j])</td>
<td></td>
</tr>
<tr>
<td><strong>Generation Loop:</strong></td>
<td></td>
</tr>
<tr>
<td>i = (i + 1) mod l</td>
<td></td>
</tr>
<tr>
<td>j = (j + S[i] mod l)</td>
<td></td>
</tr>
<tr>
<td>swap (S[i], S[j])</td>
<td>output = S[S[i]+S[j] mod l]</td>
</tr>
</tbody>
</table>

However in the literature there are lots of cryptanalysis researches about RC4 algorithm [15, 16, 17, 18]. Many weakness have been revealed. Modified RC4 (MRC4) encryption algorithm is recommended by Jindal and Singh [19], in this paper this algorithm is used because it focuses on WEP protocol security. MRC4 uses the same key scheduling algorithm (KSA) with RC4 but with two different keys and two S boxes (S1 and S2). Structure of MRC4 KSA is given Fig. 2. In the pseudo random generator (PRG) part is given Fig. 3.

3. SMTP AND POP3

SMTP is a protocol that sent Email messages over the Internet between sender and recipient side’s servers, only works for
outgoing messages. While sending Email, most of Email software is designed to use SMTP. It breaks up different parts of message into categories so that it provides meaningful communication between two servers. The messages can then be retrieved with an Email client using either POP or Internet Message Access Protocol (IMAP). POP that is a protocol has two versions POP2 and POP3. POP2 became a standard in the mid-80’s and requires SMTP to send messages. POP3 is newer version that can be used with or without SMTP. IMAP is a protocol, latest version IMAP4, is similar to POP3. All of them deal with receiving of Email on the server.

In this work POP3 is used because of it is simple and well-supported. In order to connect to the Internet, parties need an Internet Service Provider (ISP).

Fig. 4 shows Email protocols between sender and recipient. First step sender compose his/her mail, Email client sends this mail to the SMTP server. Then the SMTP server forwards the mail to the recipient’s mailbox. The POP3 server holds the message for delivery to the recipient. Finally the recipient retrieves the message using the POP3 protocol.

As mentioned before thanks to internet, people can initiate real-time communication with everybody they want. It provides lots of services like Email, video conferencing, chat etc. Internet has lots of advantages nevertheless there are some disadvantages. One of them and the most important is security gap. In the insecure and unsafe area makes our personal and secret information vulnerable to third persons who want to steal this information. The other is spamming, it refers to sending unwanted mails that make slower to access our Email accounts. To cope with security problem, especially safe messaging, suggested use of MRC4 encryption algorithm while sending mail to the recipient. Thus mails can be protected from thefts.

4. IMPROVED METHOD
Proposed method in this paper has four classes. These are newmessage, default, messages and MRC4. C++ programming language is used.

The newmessage class composes new Email packages and then Email subject and content is encrypted using encrypt method in the MRC4 class. In the default class, POP3 and SMTP servers’ session information is registered. Then this registration information is direct to the messages class. In the messages class connects to the POP3 server, encrypted Email is decrypted with decrypt method in MRC4 class.

Fig 5: Flowchart of sending Email

400x300

Fig 6: The encryption process of each block with MRC4 algorithm

This system allows to user the selection of between 64-128 bit key while encryption with MRC4.
In the Fig. 7 the steps of the messages class are given. In the messages class firstly POP3 server information is entered, than Email package is downloaded. Using decrypt method in the MRC4 class, encrypted mail content and subject. Finally decrypted Email or that can be called as plain text is obtained. Thereby Email is securely transmitted to the recipient over the unsafe area. The mail content and subject decryption process is given in the Fig. 8.

In the Fig. 9 login screen is given, SMTP and POP3 server names are entered to this screen. Using Email sending screen that is given in the Fig. 10, people can sent encrypted Email to the recipient side.


