http://ejournal.seaninstitute.or.id/index.php/InfoSains
Jurnal Info Sains : Informatikan dan Sains, Volume 11, No 02 September 2021
E-ISSN.2797-7889, P-ISSN.2089-3329

Analysis Of Voice Data Security Security By Using The Rc4 Algorithm

Rika nurhidayati[1], Salauddin Muis[2]
Sistem Informasi, STMIK Putra Batam
Email: nurhdihayati02@gmail.com[1], salauddi09@gmail.com[2]

Keywords

Security
RC4 algorithm
File
MP3

Abstract. Data security and confidentiality is one of the most important aspects in the field of communication, especially communication using computer media. One of the fields of science that is used to secure data is cryptography. Cryptography is a science that uses mathematical equations to encrypt and decrypt data. Encryption is the process of converting plaintext (readable data) into ciphertext (unreadable data) and decryption is the opposite of encryption, which changes ciphertext back into plaintext. In this study, the RC4 algorithm will be discussed to encrypt and decrypt mp3 files stored on the computer.

1. INTRODUCTION

Security and confidentiality are one of the important aspects of data, messages and information. Sending a message, data and information that is very important requires a high level of security. With the development of information technology today so rapidly, where everyone will be easy to get a message, data and information. Ease of access to communication media has an influence on information security using communication media as a medium of delivery. Information becomes very vulnerable to be known, taken or even manipulated and misused by other parties who are not entitled. During delivery and when it arrives at its destination, such information must be kept confidential and authenticated or not modified. The recipient of the information must be sure that the information really comes from the right sender, and vice versa, the sender believes that the recipient of the information is the real person. Data breaches will occur if there is no good security[1].

The data breach can be in the form of searching for a secret important document. To avoid burglary, the step that must be done is to use a cryptographic security application such as the use of RC4, so that the data can be maintained and safe. Information security in this global era is increasingly becoming a vital need in various aspects of life. An information will have a higher value when it comes to aspects of business decisions, security or public interest. RC4 is one type of stream cipher, which processes units or input data, messages or information at one time. The unit or data is usually a byte or sometimes even a bit (byte in the case of RC4). In this way encryption or decryption can be performed at a variable length [2].

The security of the software is one of the properties that determine the quality of the software. This relates to how the software can be protected from malicious users or code, which can damage the internal data, functionality, and overall system of the software when the software is implemented. There are three poles that determine the quality aspects of software engineering; usability (usability), security (security), functionality (functionality).

Usability relates to how users can use the software easily, while functionality is how the software developed can carry out its functions and behave as expected. Both of these functions can be directly felt by the user when testing the system. While the security aspect is usually ignored, because it is not only difficult to implement but also can reduce the ease of users in using the system.

2. METHOD

2.1 Cryptography

Cryptography comes from the Greek, crypto and graphia. Crypto means secret (secret) and graphia means writing (writing). According to the terminology, cryptography is the science and art of maintaining message security when messages are sent from one place to another. Cryptography is the study of mathematical techniques related to information security aspects such as confidentiality, data integrity, and authentication. maintain message security (Rinaldi Munir, There are various definitions of cryptography, but in essence cryptography is a technique used to ensure the security of data exchange [3].

1. Encryption
   Encryption is the process of converting plaintext into ciphertext which cannot be understood. The encryption process is usually done before the message is sent. To increase the security of message encryption, the encryption process is added which is also required for the decryption process[4].
2. Description
   Decryption is the process of converting ciphertext back into plaintext so that the message can be understood. The decryption process is usually carried out by the recipient of the message so that the message received can be understood. The key used in the decryption process can be different from the key used in the encryption process, it is also called public key cryptography. Conversely, if the key used is the same, it is also called symmetric key cryptography [5].

2.2 Symmetric Key Cryptography

Symmetric key cryptography uses the same key for encryption and decryption. The weakness of symmetric key cryptography is the difficulty in key distribution, because the sender and recipient of the message must know the same key, the key must be sent or notified to other parties. Another problem is the number of keys that must be used, for each pair of senders and recipients of the message there must be at least one key that can be used to encrypt between them[6].

2.3 RC4 Algorithm

RC4 was designed by Ron Rivest who came from RSA Security in 1987. RC itself has an official abbreviation, namely "Rivest Chiper", but is also known as "Ron's Code". deploy RC4 to the Cypherpunks mailing list. Then this news was quickly posted to the sci.crypt newsgroup, and from this newsgroup it spread widely on the internet [7], [8]. The leaked code is confirmed to be authentic because the output issued is the same as software that uses licensed RC4. The name RC4 has been patented, so RC4 but Rivest personally released it. by linking the English Wikipedia to his notes. RC4 has become part of standard and widely used encryption protocols, including WEP and WPA for wireless cards, as well as TLS. A major factor in the success of RC4 is its speed and simplicity in handling multiple applications, making it easy to develop efficient implementations into software and hardware[9]. Multiple streams*Cipher* based on Linear Feedback Shift Registers (LFSRs) which are efficient in hardware but less efficient in software. The design of RC4 avoids the use of LFSRs, and this algorithm is ideal for software implementations because it uses only byte manipulation.RC4 Stream Ciper is one type of algorithm that has an SBox, S0,S1,……,S255, which contains permutations from the numbers 0 to 255. This encryption algorithm will generate pseudorandom bytes from the key which will be subjected to Xor operations on the plaintext

to produce ciphertext. . To generate the original plaintext, the ciphertext will be subjected to an Xor operation against the pseudorandom bytes.

In RC4 it uses two indexes, namely i and j in the algorithm. Index i is used to ensure that an element changes, while index j will ensure that an element changes randomly. Broadly speaking, the algorithm of the RC4 Stream Cipher method is divided into two parts, namely: key setup and stream*RC4 Stream Cipher*generations. On. Key Setup has three stages of process in it, namely Initialization of S-Box, Storing key in Key Byte Array, Permutation of S-Box. Stream Generation will generate pseudorandom values which will be subjected to XOR operations to generate ciphertext or vice versa, namely to generate plaintext [10], [11].

3. RESULTS AND DISCUSSION

3.1 Stream Generation Algorithm

The algorithm is Stream Generation by following the following rules and regulations
Fill in index i and j with value 0
For i = 0 to i = plaintext length
Fill the value of i with the result of operation (i + 1) mod 256
Fill the value of j with the result of the operation (j + S(i)) mod 256
Swap S(i) and S(j)
Fill in the value of t with the result of the operation (S(I) + (S(j) mod 256)) mod 256
Fill the value of y with the value of S(t)
The value of y is subjected to an XOR operation against the plaintext
Add i by 1, back to 2.

3.2 S-Box Permutations

The RC4 algorithm is quite easy to explain. RC4 has an S-Box, S0,S1,...,S255, which contains permutations from 0 to 255, and permutations are functions of keys of variable length. There are two indices, i and j, which are initialized to zero. To generate random bytes, the steps are as follows: i = (i + 1) mod 256 j = (j + Si) mod 256 swap Si and Sj t = (Si + Sj) mod 256 K = St Byte K XORed with plaintexts for generate ciphertext or XOR with ciphertext to produce plaintext.
First
initialize an S-Box with a length of 8 bytes, with S[0]=0, S[1]=0, S[2]=0, S[3]=1 S[4]=0, S[5]=1, S[6]=1, and S[10]=1 so that the array S becomes:
00010111
Initialize 4 byte array key, Ki. Suppose the key consists of 2 bytes, namely byte 1 and byte 7. Repeat the key until it fills the entire K array so that the K array becomes:
1 7 1 7 1 7 1 7
Next we mix the operations where we will apply the variables i and j to the array indexes S[i] and K[i]. First we give the initial values for i and j with 0. The mixing operation is a repetition of the formula (j + S[i] + K[i] mod 8 followed by exchanging S[i] with S[j]. Because it uses an array of length 8byte then the algorithm becomes:
For i = 0 to 8
j = (j + S[i] + K[i] mod 8
swap S[i] and S[j]
With the algorithm as above, the initial values i = 0 to i = 7 will produce an array S as follows:

First iteration:
i = 0, then
j = (j + S[i] + K[i]) mod 8
= (j + S[0] + K[0]) mod 8
= (0 + 0 + 1) mod 8
= 1
Swap S[0] and S[1] to produce an array S:
10010111
Second iteration:
i = 1, then
j = (j + S[i] + K[i]) mod 8
= (j + S[1] + K[1]) mod 8
= (1 + 0 + 7) mod 8 = 1
Swap S[1] and S[0] to produce an array S:
00010111
Third iteration:
i = 2, then
j = (j + S[i] + K[i]) mod 8
= (j + S[2] + K[2]) mod 8
= (0 + 0 + 1) mod 8
= 1
Swap S[2] and S[3] to produce an array S:
00110111
Fourth iteration:
i = 3, then
j = (j + S[i] + K[i]) mod 8
= (j + S[3] + K[3]) mod 8
= (1 + 1 + 7) mod 8
= 1
Swap S[3] and S[2] to produce an array S:
01100111
Fourth iteration:
i = 4, then
j = (j + S[i] + K[i]) mod 8
= (j + S[4] + K [4]) mod 8
= (1 + 0 + 1) mod 8
= 0
Swap S[4] and S[3] to produce an array S:
01010111
Fourth iteration:
i = 5, then
j = (j + S[i] + K[i]) mod 8
= (j + S[5] + K [5]) mod 8
= (0 + 1 + 7) mod 8
= 0

Swap S[5] and S[4] to produce an array S:
01100011
Fourth iteration:
i = 6, then
j = (j + S[i] + K[i]) mod 8
= (j + S[6] + K[6]) mod 8
= (0 + 1 + 1) mod 8
= 0
Swap S[6] and S[5] to produce an array S:
01100011
Fourth iteration:
i = 7, then
j = (j + S[i] + K[i]) mod 8
= (j + S[3] + K[3]) mod 8
= (0 + 1 + 7) mod 8
= 0
Swap S[7] and S[6] so as to produce an array S:
01100001
Fourth iteration:
i = 8, then
j = (j + S[i] + K[i]) mod 8
= (j + S[8] + K [8]) mod 8
= (0 + 1 + 1) mod 8
= 0
Swap S[8] and S[0] to produce an array S:
00110000
After getting the results of the S array from the fourth iteration, the next process is to XOR the pseudo randombyte with plaintext, with the entered plaintext is 10110000.
Because the plaintext consists of two characters, two iterations occur. The first iteration is:
Initialize i and j with i = 0; j = 0.
i = 0; j = 0;
i = (i + 1) mod 8
= (0 + 1) mod 8
= 1
And
j = (j + S[i]) mod 8
= (0 + 2) mod 8
= 0
Swap S[i] and S[j], namely S[1] and S[2] so that the array S becomes:
01100000
t = (S[i] + S[j]) mod 8
= (3 + 1) mod 8
= 0
K = S[t] = S[0] = 0
*Bytes*these two/K's are XORed with the plaintext "1010". Then the second iteration is:

i = 1; j = 2
i = (i + 1) mod 8
 = (1 + 1) mod 8
 = 0
And
j = (j + S[i]) mod 8
 = (2 + 0) mod 8 = 0
Swap S[i] and S[j], namely S[2] and S[0] so that the array S becomes:
10100000
t = (S[i] + S[j]) mod 4
 = (2 +1) mod 4
 = 3
K = S[t] = S[3] = 2
Swap S[i] and S[j], namely S[7] and S[6] so that the array S becomes:
11100000

4. CONCLUSION

After testing and analyzing the system, the following conclusions can be obtained. With the RC4 Algorithm, voice data will be difficult to identify and keep confidential. it is known that the encryption-decryption process in the RC4 algorithm with the same password between encryption and decryption with the same plaintext will produce different ciphertext, but the plaintext result remains the same.

REFERENCE

[1] Y. S. Fatmala, A. Kusyanti, and M. Data, "Implementasi Algoritme Speck untuk Enkripsi dan Dekripsi pada QR Code," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 2, no. 12, 2018.

[2] A. Widarma, "KOMBINASI ALGORITMA AES, RC4 DAN ELGAMAL DALAM SKEMA HYBRID UNTUK KEAMANAN DATA," *CESSJournal Comput. Eng. Syst. Sains*, vol. 1, no. 1, 2016.

[3] A. Prameshwari and N. P. Sastra, "Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen," *Eksplora Inform.*, vol. 8, no. 1, 2018, doi: 10.30864/eksplora.v8i1.139.

[4] S. Retno and N. Hasdyna, "ANALISIS KINERJA ALGORITMA HONEY ENCRYPTION DAN ALGORITMA BLOWFISH PADA PROSES ENKRIPSI DAN DEKRIPSI," *TECHSI - J. Tek. Inform.*, vol. 10, no. 2, 2018, doi: 10.29103/techsi.v10i2.858.

[5] A. Farisi, "Analisis Kinerja Algoritma Kriptografi Kandidat Advanced Encryption Standard (AES) pada Smartphone," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 4, no. 2, 2018, doi: 10.35957/jatisi.v4i2.103.

[6] D. A. Meko, "Perbandingan Algoritma DES, AES, IDEA Dan Blowfish dalam Enkripsi dan Dekripsi Data," *J. Teknol. Terpadu*, vol. 4, no. 1, 2018.

[7] D. P. O. Simamora, "Implementasi Algoritma RC4 dan Playfair Cipher untuk Menggunakan Data Teks," *J. Pelita Inform.*, vol. 16, 2017.

[8] R. Dewi, T. M. Johan, and I. Muslem R., "Aplikasi Kriptografi Dalam Mengamankan Pesan Teks Dengan Metode Algoritma Rc4 Berbasis Android," *J. TIKA*, vol. 6, no. 01, 2021, doi: 10.51179/tika.v6i01.416.

[9] M. Sholeh, Isnawaty, and B. Pramono, "IMPLEMENTASI ALGORITMA RC4 STREAM CIPHER SEBAGAI METODE OBFUSCATION STRING PADA DATABASE MySQL," *semanTIK*, vol. 5, no. 1, 2019.

[10] I. Afrianto and N. Taliasih, "Sistem Keamanan Basis Data Klien P.T. Infokes Menggunakan Kriptografi Kombinasi RC4 Dan Base64," *J. Nas. Teknol. dan Sist. Inf.*, vol. 6, no. 1, 2020, doi: 10.25077/teknosi.v6i1.2020.9-18.

[11] D. Putra *et al.*, "IMPLEMENTASI ALGORITMA RC4 DAN PLAYFAIR CIPHER Permutasi Untuk S-Box," *Pelita Inform.*, vol. 16, 2017.