The Implementation of the RC4 algorithm For Sale and Purchase Agreements Data Security On Notary Office

Trisna Setiawaty\textsuperscript{1, 2}, Olven Manahan\textsuperscript{2}

\textsuperscript{1, 2}Information Engineering Study Program, STMIK Pelita Nusantara, Jl. Iskandar Muda 1
Medan, Nort Sumatera, Indonesia, 20154

E-mail: trisnawaty437@gmail.com\textsuperscript{1}, olven_manahan79@yahoo.com\textsuperscript{2}

Abstract—Security wheel is one of the essential needs of the data, or information. With this regard the importance of the information or data by the party or person of interest. This research aims to design and build a system for data security deed of sale that can help the Notary / PPAT. The system was built using the RC4 (Rivest Code 4) which is a symmetric key cryptographic algorithms and is stream cipher, there is a process of encryption and decryption. The encryption is the process of encoding the original message or plaintext into ciphertext encrypted text. While decryption is the process of encoding back to ciphertext to plaintext (original data). This research resulted in a system that is able to change the data that can be read into the data that is not easily understood.

Keywords: Cryptography, Encryption and Decryption, RC4.

1. Pendahuluan

Data deed of sale is one of the important data on office Notary / PPAT as proof of the transaction between buyers and sellers who are known by the notary / PPAT, the data containing the identity of the client given to the office of Notary / PPAT authorized for processing a deed more various ways to be done by employees of the Notary / PPAT to overcome the problem of data security. One way is to provide a password on the computer, but it does not ensure data confidentiality deed that is stored on a computer system. \cite{1}. Therefore to keep a secret the pentingmakadi datayangsangat dan beadreki perluangkan encryption techniques, which berfungusiag modahdicuri and client data are not entitled to change the content of the data and the data bukanditujuan damage to the client. If the data changes deed of sale occurred and given to someone else to change the data and manipulate the deed of sale with its own interests, it will be a problem for Notary / PPAT to account for the deed of sale. \cite{2} So to maintain the confidentiality of a data message, or information should be used with encryption techniques (encryption) yaitusebuahcarayang melanukkanperubahan code of language that can be understood be bahasayang incomprehensible.

2. Theory

2.1 Security

A variety of security threats such as destruction of hardware, software, information, data or computer influence is very important. There are a variety of threats or change information from a data deliberate or unplanned causing fatal damage to the individual or others. In other cases the intruders also prove its existence by leaving a message on the computer after the data destruction (Agency, 2011: 1).

2.2 ASCII (American Standard Code for Information Interchange)

ASCII requires eight (8) bit to get by one character and a block of code has 64 bits for by one block. Control characters contained in ASCII divided into 5 groups according to the use that respectively include logical communication, device control, Information separator, Code extension, and physical communication. ASCII code is often found on a computer keyboard or digital instruments.

2.3 Algorithms Rivest Cipher 4 (RC 4)

RC4 has two Substitution Box (S-Box) is dengandenganarray along 256 that contains a permutation of the numbers 0 to 255, and the S-box second. Then the state-of the array will be hashed back and will be processed to generate an encryption key that will be XOR of the plaintext or ciphertext. RC4 algorithm is divided into two main processes, namely the Setup Key or Key scheduling algorithm (KSA) and Stream Generation or Pseudo Random Generation Algorithm (PRGA) and the XOR with the data stream.

Berikut RC4 algorithm processing method:

a) Key Setup or Key scheduling algorithm (KSA)
In this section there are several stages of the process in it, namely:

1) Initialize S-Box
At this stage the S-box will be filled with a value corresponding to the index to get the S-BoxadapunAlgoritmany a are as follows:
- for i = 0 to i = 255 do,
- fill s the value of i,
- add i by 1, return to step 2.

### Table 1.
Initialize S-Box by entering the serial data in each block

| 0 | 1 | 2 | ... | 255 |

2) Storing keys in Key Byte Array
At this stage, the key (key) to be used is inserted into the array size of 256 repeatedly until the entire array is filled. The algorithm is as follows:
1. j fill with 1,
2. for i = 0 to i = 255 do,
3. if j> key length then,
4. j holds a value of 1,
5. end if,
6. i k contents into the ascii value of the key characters to j,
7. j value increased 1,
8. add i by 1, back to 2.

From the algorithm will get an array of key sequences for example as follows for a key with a length of 4 characters that DEED with the ASCII character sequence "97 34 109 96".

### Table 2.
The results of the key on the key byte storage array

| 0 | 1 | 2 | 3 | ... | 253 | 254 | 255 |
|---|---|---|---|-----|-----|-----|-----|
| A | K | T | A | ... | K   | T   | A   |

3) Permutation on S-Box
At this stage would have taken a value of S-Box. The algorithm is as follows:
1. contents of the value j to 0,
2. for i = 0 to i = 255 do,
3. enter the value j with the operating result (j + s (i) + k (i)) mod 256,
4. swapp value s (i) and s (j),
5. plus i by 1.

The algorithm will be obtained from the S-Box which has undergone the process so the sequence randomized tranposisi suppose to lock in the following example.

### Table 3.
Results of randomized S-Box is based on key array used

| 65 | 141 | 227 | 53  | 108 | 35  | ... | ... | 208 |
|----|-----|-----|-----|-----|-----|-----|-----|-----|
| K  | K   | A   | K   | A   | A   | A   | A   |

b) Stream Generation / Pseudo Random Generation Algorithm (PRGA)
In further calculations will be generated pseudo-random value that will be done for XOR operations, and to produce ciphertext ataupunplaintext. The algorithm is as follows:
1) enter the index i and j with a value of 0,
2) for i = 0 to i = length of the plaintext,
3) the contents of the value of i with the results of operations (i + 1) mod 256,
4) contents of the value j with the operating result \((j + s(i))\) mod 256,
5) The exchange value of \(s(i)\) and \(s(j)\).
6) enter the value \(t\) with the results of the operation \((s(i) + (s(j) \text{ mod } 256))\) mod 256,
7) the contents of the value of \(y\) with the value \(s(t)\),
8) XOR operation value \(y\) subject to plaintext,
9) \(i + 1\), back to 2.

Thus will be generated ciphertext by XOR result between stream key of the S-Box and plaintext sequence.

c) Encryption And Decryption With XOR operation

Encryption or decryption process begins by converting each plaintext into binary values. The formula is as follows:

1) Formula encryption process
   \[ C = P \oplus K \]
2) Formula decryption process
   \[ P = C \oplus K \]

3. Research methods

3.1 Data collection

Data collection was conducted researchers to obtain the information needed in order to achieve appropriate goals.

3.2 Data analysis

Data analysis is the stage where the collected data obtained from observation, interview and literature study. After doing the above, the data collection phase of the manufacturing is done the deed of sale which is managed by the operational staff of the deed of sale in the form of a *.docx. To the deed of sale that the data does not fall to a third party then the process is carried out by means of encryption data security, encryption techniques are used as for yaitudengan RC4 algorithm.

3.3 Design

The design of this system will be built based on the information obtained in the study area using UML (Unified Modeling Language).

3.4 examination

Setelah perancangan akan makatahapselanjutnya untuk find errors on the system to be built and then be repaired.

3.5 Application

Implementation is a way to implement something based on a theory, usually done as an implementation in completing certain goals that have been planned and arranged, and apply information in the operation. Implementation will be done ie Data Security Sale and Purchase Agreements with RC4 algorithm.

4. Analysis And Design

At the stage of the analysis that will be built starting with collecting literature on methods of cryptography especially RC4 algorithm method. Literature study methods used by looking at existing research and refers to research that has been done.
4.1 Method Analysis Algorithm of RC4

The calculation will be done as follows:

**plaintext**: DEED OF SALE & PURCHASE

**Key**: TRISNA

More specifically, RC4 operates with the following steps:

1) Initialize S-Box

   Initialization of the S-box with a length of 256 bytes, with $S[0], S[1], \ldots, S[255]$.

2) Key initialization

   Initialization 6 bytes key = $i \cdot K_i$ array. Suppose a separate key on the 6 bytes "TRISNA" then the sentence is converted to decimal form "84 82 73 83 78 65"

| Table 4. | Key initialization |
|----------|--------------------|
| S-Box $[i]$ | 0 | 1 | 2 | 3 | 4 | 5 | ... | ... | 254 | 255 |
| Key | T | R | I | S | N | A | ... | ... | 1 | S |
| decimal Key | 84 | 82 | 73 | 83 | 78 | 65 | ... | ... | 73 | 83 |

3) KSA (Key scheduling Algorithm)

   Inisialisasi dan ini diakukan KSA dengan parameter key yang acak. Explanation iteration lebih lanjut dapat dijelaskan sebagai berikut:

   - If $j = 0$;
   - for $i = 0$ to $255$
   - $j = (j + S[i] + K[i]) \mod 256$
   - Swap $S[i]$ dan $S[j]$

   Then the algorithm as above obtained value of $i = 0$ to $i = 255$ will generate an array $S$:

   **Iteration 1**
   - $i = 0$
   - $j = 0$
   - $i = (i + 1) \mod 256$
   - $j = (j + S[i]) \mod 256$
   - Swap $S[i]$ and $S[j]$

   **Iteration - 256**
   - $i = 255$
   - $j = (j + S[i] + K[i]) \mod 256$
   - $K = S[(S[i] + S[j]) \mod 256]

4) PRGA (Pseudo-RandomGenerationAlgorithm)

   After doing the calculations KSA, then that will be conducted PRGA (Pseudo-RandomGenerationAlgorithm). This PRGA used to get random bytes for encryption, it is because dibutuhkan 1 key (key) and 1 pengoprasian XOR for each character in the plaintext.

   **Iteration 1**: Initialization 1 and $j$ with $i = 0$, $j = 0$

   **Iteration 1**
   - $i = (i + 1) \mod 256$
   - $j = (j + S[i]) \mod 256$
   - Swap $S[i]$ and $S[j]$
   - $K = S[(S[i] + S[j]) \mod 256]$

   Here Iteration 1: Initialization 1 and $j$ with $i = 0$, $j = 0$

   **Iteration 1**: $i = (i + 1) \mod 256$
   - $j = (j + S[i]) \mod 256$

   - $K = S[(S[i] + S[j]) \mod 256]$

   Here Iteration 1: Initialization 1 and $j$ with $i = 0$, $j = 0$

   **Iteration 1**: $i = (i + 1) \mod 256$
   - $j = (j + S[i]) \mod 256$

   - $K = S[(S[i] + S[j]) \mod 256]$

   Here Iteration 1: Initialization 1 and $j$ with $i = 0$, $j = 0$
Swap S[1] and S[202]

\[ K = S[i] + S[j] \mod 256 \\
    = S[1] + S[202] \mod 256 \\
    = (167 + 202) \mod 256 \\
    = 113 \]

\[ K = S[113] = 240 = 11110000 \]

**Iteration 2:**

\[ i = (i + 1) \mod 256 \\
    = (1 + 1) \mod 256 \\
    = 2 \]

And \( j = (j + S[i]) \mod 256 \)

\[ = (202 + S[2]) \mod 256 \\
    = (202 + 129) \mod 256 \\
    = 75 \]

Swap S[2] and S[75]

\[ K = S[i] + S[j] \mod 256 \\
    = S[2] + S[75] \mod 256 \\
    = (155 + 75) \mod 256 \\
    = 230 \]

\[ K = S[230] = 230 = 11,101,011 \]

**Iteration 14:**

\[ i = (i + 1) \mod 256 \\
    = (13 + 1) \mod 256 \\
    = 14 \]

And J

\[ = (J + S[i]) \mod 256 \\
    = (214 + S[14]) \mod 256 \\
    = (214 + 250) \mod 256 \\
    = 208 \]

Swap S[14] and S[208]

\[ K = S[i] + S[j] \mod 256 \\
    = S[14] + S[208] \mod 256 \\
    = (200 + 208) \mod 256 \\
    = 152 \]

\[ K = S[152] = 166 = 10.10011 \text{ million} \]

Based on the results above, the permutation value (K) is obtained from permutations as many iterations it took was 14 iterations. The results obtained can be seen in the following table:

| \( K \) | Binary       |
|-------|-------------|
| 240   | 11110000    |
| 235   | 11101011    |
| 137   | 10001001    |
| 148   | 10010100    |
| 246   | 11110110    |
| 167   | 10100111    |
| 69    | 01000100    |
| 203   | 11001011    |
| 230   | 11100110    |
| 229   | 11100101    |
| 145   | 10010001    |
| 91    | 01011011    |
| 59    | 00111011    |
| 166   | 10100110    |

5) XOR encryption process

Here is an encryption process that is XOR-kan pseude random byte plaintext, the plaintext is taken from the "DEED SALE" change characters into numbers Decimal and Binary. The operations within XOR:
Perform XOR between characters in plaintext with the key generated from PRGA \([K]\) above:

### Table 6

| A | B | A ⊕ B |
|---|---|---|
| 1 | ⊕ | 0 |
| 0 | ⊕ | 1 |
| 1 | ⊕ | 1 |
| 0 | ⊕ | 0 |

### Table 7

| Character | Decimal | binary     |
|-----------|---------|------------|
| A         | 65      | 01000001   |
| K         | 75      | 01001011   |
| T         | 84      | 01010100   |
| A         | 65      | 01000001   |
| J         | 74      | 01001010   |
| U         | 85      | 01010101   |
| A         | 65      | 01000001   |
| L         | 76      | 01011000   |
| 32        | 00100000 |
| B         | 66      | 01000010   |
| E         | 69      | 01000101   |
| A         | 65      | 01000001   |
| L         | 76      | 01011000   |
| 32        | 00100000 |

### Table 6

**Encrypting plaintext results of “A”**

| plaintext | A | K | ⊕ (XOR) | ciphertext |
|-----------|---|---|---------|------------|
| A         | 65| 11110000 | 10110001 | 177        |

### Table 7

**Results Encryption Plaintext “L.”**

| plaintext | L | K | ⊕ (XOR) | ciphertext |
|-----------|---|---|---------|------------|
| L         | 76| 00111011 | 01110111 | 119        |

### Table 8

**After Encrypted Text**

\[± ÝŐÑ♭ŚÅÔ Wİ\]

#### 4.2 System planning

Designing the system to be built using modeling Unified Modeling Language (UML). As for the use case diagram of the proposed:
5. Conclusion

The key length does not affect the time used during the process. Increasingly panjangkunci used, the higher the security level of the encrypted file. The use of encryption applications to secure data or information into something that must be improved. For the owners and users of data and information if the data and information they do not want to be known by the irresponsible and can be detrimental. The system is very simple and of course by adding some other support functions are expected to enhance the functionality of the system. The level of data security on these systems need to be improved by using another cryptographic method deed of sale so that data can be safe again.

6. Reference

[1] Andi. 2008. "Microsoft Visual Basic 6.0 for beginners". Yogyakarta: Andi.
[2] Home Agency. 2011. "Security Total Data and Important Information". PT.ElexMedia Komputindo.
[3] Basri. "Symmetric and Asymmetric Cryptography In danKompleksitas Computing Data Security Perspective", Journal of Scientific Computer Science, 2016, 2 (2).
[4] Kurniadi, Irwansyah, Fatmasari. "The implementation of the RC4 algorithm to encrypt data security". 2015.
[5] Marbun pure. "The implementation of a data security system of goods at PT. MatahariPutra Prima, TBK ", Journal Mantik Penua, 2015, 18 (2).
[6] Rosa United States, and Msalahudin. 2018. "Software Engineering".
[7] Ruri Hartika Zain. "The design and implementation of the RC4 algorithm cryptography method on the type of document file using Visual Basic 6.0 programming language". Momentum Jurnal, 2012.12 (1), 71-80.
[8] Sukma Rizqi Kharisma, Muhammad Ariz Fatchu Richman. "Making Application Notes Using Polyalphabetic Substitution Cipher Cryptographic Algorithms The combination of ASCII codes and Android-Based XOR operations". Journal of Information Technology, 2017, XII (35).
[9] Wikipedia, The Free Encyclopedia, (2019, April 23) "Flow Chart". Be identified May 31, 2019, from https://id.wikipedia.org/w/index.php?title=Diagram_alir&oldid=15019984