Prototype of Learning Applications for Modern Cryptographic Techniques Using RC4 Algorithms to Support Computer Security Courses

Muhammad Iqbal¹, Nasrul Nazar¹, Cut Ita Erliana², Defi Irwansyah²*, Nuning Kurniasih³, Edi Susilo³, Akbar Iskandar⁵, Rini Suryani⁶, Supriyono⁷, Sudarmaji⁸, Erwin Putera Pernama⁹, Alfian Erwinsyah¹⁰, Sujinah¹¹, Haimah¹² and I Ketut Sudarsana¹³

¹Department of Computer System, Universitas Pembangunan Panca Budi, Medan, Indonesia
²Department of Industrial Engineering, Universitas Malikussaleh, Aceh, Indonesia
³Faculty of Communication Sciences, Library and Information Science Program, Universitas Padjadjaran, Bandung, Indonesia
⁴Department of Agrotechnology, University of Ratu Samban, Bengkulu, Indonesia
⁵Department of Informatics, Universitas Malikussaleh, Lhokseumawe, Indonesia
⁶Department of Agrotechnology, Sekolah Tinggi Ilmu Pertanian Rejang Lebong, Bengkulu Indonesia
⁷Department of Geography Education, Universitas Prof. Dr. Hazairin SH. Bengkulu, Bengkulu, Indonesia
⁸Faculty of Computer Sciences, Universitas Muhammadiyah Metro, Indonesia
⁹Department of Elementary School Teacher Education, Universitas Nusantara PGRI Kediri, Indonesia
¹⁰Faculty of Education and Teacher Training, IAIN Sultan Amal Gorontalo, Indonesia
¹¹Faculty of Education, University Muhammadiyah of Surabaya, Surabaya, Indonesia
¹²Department of Education Management, Universitas Prof. Dr. Hazairin SH.
Bengkulu, Bengkulu, Indonesia
¹³Department of Religious Education, Institut Hindu Dharma Negeri Denpasar, Indonesia

* defiirwansyah@unimal.ac.id

Abstract. Abstract The security of information 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. This study presents a learning application to explain how to secure data using cryptographic techniques. This study aims to design a prototype learning application of cryptographic techniques using algorithm RC4 method. Based on the results of data analysis and after completing the design of RC4 algorithm cryptographic learning software, the authors found this software shows every step and stages of the processes (data input process (Plaintext or Ciphertext string), Key padding process (U), formation process in S-Box table, the Key-Flow formation process (K-keystream), encryption process and decryption process) contained in RC4 algorithm cryptography, so it can help understanding or learning work procedures of algorithms in the cryptographic method. Microsoft Visual Basic 2008 is an IDE (Integrated Development Environment) application that is used to create and develop
1. Introduction

The security of information 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 the public interest. The information will certainly in great demand by various parties who also have an interest in it.

In everyday life, humans depend a lot on information technology, from small things to complex problems. For examples of information technology in everyday life are ATM, Internet Banking, Mobile Banking, Email, SMS, MMS, Chat and so on[1]. The improvement of information technology provides many benefits for human life. But the benefits offered by information technology also lead to crimes such as data theft. So the development of knowledge to secure data is increasingly enhanced so the users of technology always feel safe. Various methods was taken to maintain the security of the data. One of them is by encoding the data into codes that are not understood, so when tapped it will be difficult to find out the actual information.

The first encoding method was made using the secret algorithm method. This method builds on the confidentiality of the algorithm used. But this method is not efficient due to it must to communicate with many people. Therefore, one people must create a new algorithm if want to exchange confidential information with others. Because the user feels inefficient, the secret algorithm begins to be abandoned and introduced a new method called the key algorithm. This method does not stack security on the algorithm, but on the confidentiality of the keys used in this process. The algorithm can be known and learned by anyone. The key algorithm method has a better level of efficiency and security than the secret algorithm. The key algorithm known as cryptography has covered aspects of human life today. Once the importance of cryptography, when talking about computer security it cannot separate it from cryptography[2].

2. Related Works

Cryptography is very important to learn. At this time, it is began to packaged in a more practical and interesting way through computer media because computers were able to display text, color, sound, video, motion, image and were able to display intelligence that could present an interactive process. According to Suyadi (2008), computer media is used to learning because it provides benefits that other learning media do not have, such as the ability of computers to interact individually with students[3].

The learning model applied in computer-assisted learning can generally classified into four models, like: 1) tutorial, 2) drill and practice, 3) simulation, and 4) problem-solving. In models 1 and 2, the computer acts as a teacher, whereas models 3 and 4, used to develop of problem solving skills through discovery or exploratory approaches[4].

3. Research Methodology

Analysis is a software design task that connected the gap between system level software allocation and program level software design, in this case the design of application program interfaces learning modern cryptographic techniques using RC4 algorithm to support computer security courses, enabling system design to determining functions and software performance, showing software interfaces with other system elements and building restriction that must fill by software[5].

RC4 generates keystream which is become XORed with plaintext during the encryption process (or XORed with the ciphertext during the decryption process). It is not like flow ciphers that processing data in bits, RC4 processing data in byte sizes (1 byte = 1 bit = 1 letter). For examples of cases that will be discussed and simulated in the writing of this thesis is to show the following data:

| Plaintext   | “Sabana Azmi” |
|-------------|---------------|
| Key         | “islam”       |

Cryptographic analysis using RC4 algorithm is as follows:
A. Initialization of array S (S-Box or Substitution Box), so \( S_0 = 0, S_1 = 1, S_2 = 2, \ldots S_n = n \ldots \), \( S_{243} = 243, S_{244} = 244, S_{255} = 255 \).

1. Initialization is giving a meaningful value to a variable. So before initializing, a variable called the array S (S-Box) must be made first. Array S is a one-dimensional variable that provides 256 places. So array S has an index of 0 to 255. In the visual basic programming language is written as follows:

\[
\text{Dim S As Integer}() = \text{New Integer}(255)\
\]

Following is the S array creation table.

### Table 1. Construction of Array S

| S-0 | S-1 | S-2 | S-3 | S-4 | S-5 | S-6 | S-7 | S-8 | S-9 | S-10 | S-11 | S-12 | S-13 | S-14 | S-15 |
|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|------|------|------|------|------|------|
| null | null | null | null | null | null | null | null | null | null | null | null | null | null | null | null |
| S-16 | 17 | 18 | 19 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
| null | null | null | null | null | null | null | null | null | null | null | null | null | null | null | null |
| S-32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 |
| null | null | null | null | null | null | null | null | null | null | null | null | null | null | null | null |
| S-64 | 65 | 66 | 67 | 68 | 69 | 70 | 71 | 72 | 73 | 74 | 75 | 76 | 77 | 78 | 79 |
| null | null | null | null | null | null | null | null | null | null | null | null | null | null | null | null |
| S-80 | 81 | 82 | 83 | 84 | 85 | 86 | 87 | 88 | 89 | 90 | 91 | 92 | 93 | 94 | 95 |
| null | null | null | null | null | null | null | null | null | null | null | null | null | null | null | null |
| S-96 | 97 | 98 | 99 | 100 | 101 | 102 | 103 | 104 | 105 | 106 | 107 | 108 | 109 | 110 | 111 |
| null | null | null | null | null | null | null | null | null | null | null | null | null | null | null | null |
| S-112 | 113 | 114 | 115 | 116 | 117 | 118 | 119 | 120 | 121 | 122 | 123 | 124 | 125 | 126 | 127 |
| null | null | null | null | null | null | null | null | null | null | null | null | null | null | null | null |
| S-128 | 129 | 130 | 131 | 132 | 133 | 134 | 135 | 136 | 137 | 138 | 139 | 140 | 141 | 142 | 143 |
| null | null | null | null | null | null | null | null | null | null | null | null | null | null | null | null |
| S-144 | 145 | 146 | 147 | 148 | 149 | 150 | 151 | 152 | 153 | 154 | 155 | 156 | 157 | 158 | 159 |
| null | null | null | null | null | null | null | null | null | null | null | null | null | null | null | null |
| S-160 | 161 | 162 | 163 | 164 | 165 | 166 | 167 | 168 | 169 | 170 | 171 | 172 | 173 | 174 | 175 |
| null | null | null | null | null | null | null | null | null | null | null | null | null | null | null | null |
| S-176 | 177 | 178 | 179 | 180 | 181 | 182 | 183 | 184 | 185 | 186 | 187 | 188 | 189 | 190 | 191 |
| null | null | null | null | null | null | null | null | null | null | null | null | null | null | null | null |
| S-192 | 193 | 194 | 195 | 196 | 197 | 198 | 199 | 200 | 201 | 202 | 203 | 204 | 205 | 206 | 207 |
| null | null | null | null | null | null | null | null | null | null | null | null | null | null | null | null |
| S-208 | 209 | 210 | 211 | 212 | 213 | 214 | 215 | 216 | 217 | 218 | 219 | 220 | 221 | 222 | 223 |
B. Generate keystream K and encrypt plaintext P as follows:

Dim Input As String = Plaintext/Ciphertext
Dim tempSwap As Integer = 0 : Dim K As Integer = 0
Dim Output As Integer = 0 : Dim t As Integer = 0
Dim OutputSTSB As New System.Text.StringBuilder
Dim i As Integer = 0 : Dim j As Integer = 0

For idx As Integer = 0 To Input.Length - 1
    i = (i + 1) Mod 256
    j = (j + S(i)) Mod 256
    tempSwap = S(i) \ S(j)   ' swap value of S[i] and S[j]
    S(i) = tempSwap /
    t = (S(i) + S(j)) Mod 256
    K = SBox(t)
    Output = K Xor Asc(Input(idx))
    OutputSTSB.Append(Chr(Output))
Next
Dim OutputText As String = OutputSTSB.ToString

Based on the code and the input received, the key stream K will be generated = “h®äwåSaÙ”, with character length equal to plaintext Input. Plaintext Input = “Sabana Azmi” will be encrypted using the XOR operation against the K key to produce Ciphertext Output Text = “;ÎÓŠÅG)°”.

| Character | ASCII | BINER  | Xor Key-Flow |
|-----------|-------|--------|-------------|
| S         | 83    | 01010011 | 01101000 | 104 | H |
| a         | 97    | 01100001 |             |    |
| b         | 98    | 01100010 |             |    |
| a         | 97    | 01100001 |             |    |
| n         | 110   | 01101110 |             |    |
| a         | 97    | 01100001 |             |    |
| 32        | 00100000 |       |             |    |
| A         | 65    | 01000001 |             |    |
| z         | 122   | 01111010 |             |    |
| m         | 109   | 01101101 |             |    |
| i         | 105   | 01101001 |             |    |

Table 2. Encryption Process

| Ciphertext Result of Xor Plainteks P Process to Key-Flow K |
|----------------------------------------------------------|
| Cipherteks                                              |

Table 3. Cipherteks Result of Xor Plainteks P Process to Key-Flow K
To describe the ciphertext again to plaintext, it is enough to XOR the keystream with the ciphertext byte.

4. Result and Discussion

Hardware Specification
This program was run using recommended hardware as follows:

a. Processor AMD Dual Core C60 with Turbo Core 1.333 GHz.
b. Memory 2 GB.
c. Harddisk 500 GB.
d. VGA card AMD RADEON 256 MB.
e. LED with resolution of 1366 X 768 pixel.
f. Keyboard and Mouse.

Software Specification
This program was created and run using the recommended software as follows:

a. The recommended operating system for running this application is the Microsoft operating system Windows 7 Ultimate Edition x86 Service Pack 1.
b. Microsoft Visual Studio .NET2008 Service Pack 1, to design the appearance of the design and program codes.

Interface
The interface is the result of implementing a design sketch of a designed form in draft form into a programming display that used Visual Studio .NET 2008. These following are the results of the interface:

1. Main Form – Main Page Tab
   Main Form - The Main Page tab above is a display when the program first run. If the Cryptographic Tab RC4 selected it will display Main Form - Cryptographic Theory Tab RC4. If RC4 Learning Tab is selected it will display Main Form - RC4 Learning Tab. Press the [x] button to close the program.

2. Main Form - Cryptographic Theory Tab RC4
   Main Form - Cryptographic Theory Tab RC4 displays slides containing the cryptographic theory of RC4. There is a Next button and a Previous button. The Next button to proceed the next slide and the Previous button to return the previous slide. Cryptographic theory RC4 is used as an introduction to courses to convey short and solid theories to students who study.
3. Main Form – RC4 Learning Tab
   In this tab, a step by step of display learning RC4 cryptographic techniques will be presented. In this tab there are several more tabs, which are 6 (six) tabs.

5. Conclusion
   Based on the research that the author has carried out, it can be concluded as follows:
   a. This software shows each step and stages of the processes (data input process (string Plainteks or Ciphertext), Key padding process (U), the process of forming S-Box tables, the process of Key-Flow formation (K - keystream), encryption process and decryption process) contained in RC4 algorithm cryptography, so it can help understanding or learning work procedures of algorithms in the cryptographic method.
   b. The processes shows with animation, so they can present interesting learning for students thus they can understand the cryptographic method properly.
   c. The calculations that occur in the process are also displayed as the character conversion process becomes ASCII code, the process of converting ASCII code into BINER numbers.
   d. Microsoft Visual Basic 2008 is an IDE (Integrated Development Environment) application used to create and develop software. In this application there were various features that facilitate programming such as compilation, debugging, project settings, designing and editing visual interfaces, and so on.

References
[1] D. Ariyus, *Pengantar Ilmu Kriptografi: Teori Analisis & Implementasi*. Penerbit Andi, 2008.
[2] Z. A. Munir, U. Anselmi-Tamburini, and M. Ohyanagi, “The effect of electric field and pressure on the synthesis and consolidation of materials: A review of the spark plasma sintering method,” *J. Mater. Sci.*, vol. 41, no. 3, pp. 763–777, 2006.
[3] I. Suyadi, “The influence of leadership, infrastructure, organizational learning on technology, services, markets and brands in ecommerce strategies in Indonesia.” Dissertation, Universitas Brawijaya, 2008.
[4] S. Padmanthara, “Computer Assisted Learning (Pbk) And Benefits As Learning Media,” *TEKNO*, vol. 1, no. 1, 2012.
[5] R. H. Zain, “Designing and Implementing Cryptography with the Rc4 Algorithm Method in Document File Type Using Visual Basic 6.0 Programming Language,” *J. Momentum*, vol. 12, no. 1, 2013.