A Proposed Arabic Text Encryption Method Using Multiple Ciphers

Ammar Sabeen Hmoud Altamimi
University of Baghdad, College of Engineering, Iraq.
E-mail: ammaraltamimi@coeng.uobaghdad.edu.iq

Ali Mohsin Kaittan
Asoul Aldean University College, Iraq.
E-mail: alikaittan@gmail.com

Received March 11, 2021; Accepted June 28, 2021
ISSN: 1735-188X
DOI: 10.14704/WEB/V18SI04/WEB18131

Abstract

Most encryption techniques are deals with English language, but that deals with Arabic language are few. Therefore, many researchers interests with encryption ciphers that applied on text which wrote in Arabic language. This reason is behind this paper. In this paper, there are three cipher methods implemented together on Arabic text. Using more than one cipher method is increase the security of algorithm used. Each letter of plaintext is encrypted by a specified cipher method. Selection process of one of three cipher methods used in this work is done by controlling process that selects one cipher method to encrypt one letter of plaintext. The cipher methods that used in this paper are RSA, Playfair and Vignere. Each one of them has different basis mathematical model. This proposed encryption Arabic text method gives results better than previous related papers.

Keywords

Encryption, RSA, Playfair and Vignere.

Introduction

In information security, the process of transforming information using an algorithm to result unreadable information by anyone except whose having special knowledge in security scope is called encryption. the key is used in encryption to increase complexity of algorithm usually. The encrypted information is result of the process. The reverse procedures of encryption is called decryption [William, 2011]. Generally, there are two types of approaches in encryption process, the first type is symmetric algorithms and the second type is asymmetric algorithms [Wisam et al, 2018]. In symmetric-key algorithms,
the cryptographic keys for both processes encryption of plaintext and decryption of cipher text are used for both. The used keys are either an identical or a simple transformation in between generated keys. practically, the used keys are shared between two or more parties that used to maintain a secret information [Khalid et al,2018]. the main drawback of symmetric key encryption is accessing both linked parties to the secret key. an examples of symmetric key encryption are Advanced Encryption Standard (AES), Twofish, Blowfish and Data Encryption Standard (DES) [Ravi et al,2018].

**RSA, Playfair and Vignere Cipher**

The implementation of RSA algorithm is simple relatively. defining a two prime numbers that named (P, Q) is selected to generate used keys public and private. N is computed via relation N=P*Q, and φ=(P-1) (Q-1), e is random integer that selected and in range 1<e<φ, conditionally the gcd (e, φ) =1. so, by using the extended Euclid's, the d is calculated that satisfy relation ed =1 mod φ. Representing the Public key = (n, e) and private key = (n, d) [Nentawe, 2013]. The encryption steps are shown as in the following:

1. Selecting and generating the public key as (e, n).
2. the plaintext is converted into an integer form.
3. apply the equation c = m^e mod n to obtain cipher text.

While the decryption steps is shown in the following:

1. Generating the private key (d, n).
2. applying the equation m = c^d mod n to obtain plain text.

The Vigenère cipher is considered as simplest polyalphabetic substitution cipher, using multiple alphabets in cipher process is improving the security and making the task of crypt analyser is hard, for each letter, using a key for selecting the alphabet used of the plain text. use each alphabet in turn then repeat from start after end of key is reached as illustrate in the following example[Aphetsi, 2013]:

Plaintext= THISPROCESSCANALSOBEEXPRESSED
Keyword= CIPHERCIPHERCIPHERCIPHERCIPHER
Ciphertext= VPXZTIQKTZWTCVPSWDMTETIGAHLH

In Playfair, The size of key is a 5x5 matrix, there are 25 letters that distributed through matrix with considering j is excluded, two of plaintext letters are encrypted at a time. The Playfair square is a manual symmetric cipher method and it considers the first literal digraph substitution cipher. In 1854, This method was invented by Charles Wheatstone, it encrypts two letters instead of one letters as substitution cipher and more complex. since
the frequency analysis, the Playfair is harder to break significantly. Its work shown in the following: break the plaintext in a two letters diagram:

- Dividing plaintext into two-letters.
- Use X to separate double letter
- Use X to pad the last single letter

BK AO WY UX QI RC TM EH JS RH SX

The keyword is given and distributed in matrix 5X5 such as MONARCHY.

| I | Q | N | V | R |
| G | H | Y/J | U | S |
| E | F | C | O | K |
| T | P | O | D | L |
| B | A | W | X | R |

The work of Playfair are shown in below:

1. The 'X' is inserted if two letters are repeated.
2. if pair letters falls in the same row, then replaces letter to right.
3. if pair letters falls in the same column, replaces letter below it.
4. Else, letter is replaced with the letter in the same row and column [Basim et al, 2017].

Related Works

Shobha et al (2012) via cloud computing environment, the multiple algorithms of encryption are used based on circular queue via adding complexity for increasing the security. Mamta et al (2016), showed many cipher algorithms are applied to work together as hybrid used for ciphering message via circular queue using control key to avoid redundancy. Yahya et al (2013) indicated The modification of Vigenère cipher with adding a key repeatedly $27 = \Psi$, ..., $1 = \Psi$, $0 = \Psi$ and extra symbols indexed to 39 and will modulo 39[Nentawe, 2013; Alizadeh & Roslin, 2021].

The Proposed Method

The Arabic text is encrypted by using different cipher methods that works together with different manner. The obtained outputs of this proposed cipher method is more complexity than other cipher methods if applied separately. The proposed method consists of setup stage, controlling stage, encryption stage, moving stage, decryption stage. The general block diagram is shown in figure 1. The table 1 shows all possible letters used in Arabic language.
Table 1 The used Arabic letters

<table>
<thead>
<tr>
<th>Arabic Letter</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>ح</td>
<td>5</td>
</tr>
<tr>
<td>ج</td>
<td>4</td>
</tr>
<tr>
<td>ظ</td>
<td>3</td>
</tr>
<tr>
<td>ث</td>
<td>2</td>
</tr>
<tr>
<td>ت</td>
<td>1</td>
</tr>
<tr>
<td>ا</td>
<td>0</td>
</tr>
<tr>
<td>س</td>
<td>11</td>
</tr>
<tr>
<td>ز</td>
<td>10</td>
</tr>
<tr>
<td>ر</td>
<td>9</td>
</tr>
<tr>
<td>د</td>
<td>8</td>
</tr>
<tr>
<td>ن</td>
<td>7</td>
</tr>
<tr>
<td>خ</td>
<td>6</td>
</tr>
<tr>
<td>ع</td>
<td>17</td>
</tr>
<tr>
<td>ظ</td>
<td>16</td>
</tr>
<tr>
<td>ط</td>
<td>15</td>
</tr>
<tr>
<td>ض</td>
<td>14</td>
</tr>
<tr>
<td>ص</td>
<td>13</td>
</tr>
<tr>
<td>ض</td>
<td>12</td>
</tr>
<tr>
<td>س</td>
<td>11</td>
</tr>
<tr>
<td>ز</td>
<td>10</td>
</tr>
<tr>
<td>ر</td>
<td>9</td>
</tr>
<tr>
<td>ذ</td>
<td>8</td>
</tr>
<tr>
<td>د</td>
<td>7</td>
</tr>
<tr>
<td>ن</td>
<td>6</td>
</tr>
<tr>
<td>م</td>
<td>35</td>
</tr>
<tr>
<td>ل</td>
<td>34</td>
</tr>
<tr>
<td>ك</td>
<td>33</td>
</tr>
<tr>
<td>ق</td>
<td>32</td>
</tr>
<tr>
<td>ف</td>
<td>31</td>
</tr>
<tr>
<td>غ</td>
<td>30</td>
</tr>
</tbody>
</table>

Figure 1 The Proposed Method Block Diagram

**Setup Stage**

In this stage, initialize and create coding table that contains all Arabic letters with adding letters that are 36. With this stage, each letter has code number. This task is most important because it enable cipher methods dealing with Arabic letters efficiently. The second task of this stage is loading the file of plaintext.

**Controlling Stage**

In this stage, the queue as data structure is created. The required size of created queue is three since the number of cipher methods that used in the proposed method is three. The control key is used to select cipher method that will apply. This stage allows encrypting each letter of plaintext with different cipher method that scheduled in queue.
Encryption Stage

In this stage, reading the created queue with an integer values. The value 1 represents RSA method, The value 2 represents Playfair method and The value 3 represents Vigneere method. If control key equal 1 then RSA method is applied, If control key equal 2 then Playfair method is applied and If control key equal 3 then Vigneere method is applied.

Moving Stage

In this stage, the encrypted text is transmitted via communication channel from sender to receiver. Some noises are added to transmitted encrypted text because the effects of transmission and channeling.

Decryption Stage

The outputs of previous stage are as inputs in this stage for applying decryption algorithm. the decryption algorithms are selected based on control key that generated in controlling stage. then storing result text in new file.

<table>
<thead>
<tr>
<th>Algorithm 1: Process of Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input: $f_i$, $p_i$</td>
</tr>
<tr>
<td>Output: $c_i$.</td>
</tr>
</tbody>
</table>

Load plaintext file as $m_i$ file; 
repeat 
  Read $f_i$; 
  Read controlling key 
    If $k=1$ then playfair encryption method 
    Else if $k=2$ then vigneere encryption method 
    Else RSA encryption method 
  Key generation according to pointed cipher method by control key. 
  Apply pointed cipher method by control key on $f_i$ using $p_i$; 
  result Saving $C_i$ in new file; 
  Until $f_i$ file is empty
Algorithm 2: Process of Decryption.
Input: $c_i$
Output: $f_i, p_i$

Load encrypted text as $ff_i$ file;
repeat $c_i$ file is not empty
Read $c_i$;
Read controlling key
If $k=1$ then play fair decryption method
Else if $k=2$ then vigneere decryption method
Else RSA decryption method
Key generation according to pointed cipher method by control key.
Apply pointed de-cipher method by control key on $ff_i$ using $c_i$;
obtaining $p_i$ original text.
Until $ff_i$ file is empty

Results

This section deals with practical implementation of the proposed cryptographic method. The type of language that used to write sensitive information is Arabic. The space and special symbols built in plaintext are ciphered generally. The execution time of used cryptosystem methods is calculated. The proposed hybrid text cryptography method is more effectiveness than other cipher methods which used if they performed alone. The encryption process when vigneere is used is shown in figure 2, The encryption process when playfair is used is shown in figure 3, and the encryption process when RSA is used is shown in figure 4.

Figure 2 The encryption process of vigneere method
Figure 3 The encryption process of playfair method

Figure 4 The encryption process of RSA method
Conclusions

There are some conclusions that concluded by implementing a proposed cipher Arabic text method as following:

1. The proposed method can encrypt spaces and special characters with sensitive information or plaintext.
2. The proposed method deals with texts that written Arabic language only.
3. Each letter of sensitive information is ciphered by different cipher method since scheduling it in controlling stage and using queue.
4. The proposed method is more robust than other cipher methods against a chosen cipher text attack.
5. The execution time of the proposed method is equal the execution time of other cipher methods when implemented alone approximately.

References

Alizadeh Tari, Z., & Roslin, V.P. (2021). Language Learning Styles and Writing Strategies as Predictors of Writing Anxiety among Iranian EFL Learners. KURMANJ; The Journal of Culture, Humanities and Social Science, 3(1), 12-22.


