Cryptanalysis on classical cipher based on Indonesian language

R Marwati* and K Yulianti
Departement of Mathematics Education, Universitas Pendidikan Indonesia, Indonesia

Corresponding author’s e-mail: rinimarwati@upi.edu

Abstract. Cryptanalysis is a process of breaking a cipher in an illegal decryption. This paper discusses about encryption some classic cryptography, breaking substitution cipher and stream cipher, and increasing its security. Encryption and ciphering based on Indonesian Language text. Microsoft Word and Microsoft Excel were chosen as ciphering and breaking tools.

1. Introduction
As the use of technology growth, information becomes more accessible and spreads quickly, sometimes out of control. Unfortunately, some people misuse information and manipulate it. So it could be the information dissemination as the result in the manipulation. To secure the information, either text or picture, encoding can be performed. So that the information becomes disguised, the message (ciphertext) is seen but no one knows its meaning. Cryptography study about this encoding method [1].

Ciphertext is an interesting challenge for cryptanalys to be broken. Cryptanalysis depends on language character that is used to encrypt the message (plaintext). Podstata in [2] analyzed code breaking algorithm for classical cipher and developed a mobile application for iOS operating system. The application has ability to break texts in English, Czezh, Slovak, Polish, German, French, Italian, Spanish, and Portuguese. In this paper ciphering based on Indonesian language character. Here we try to use the Microsoft Word and the Microsoft Excel as a tool to encrypt and ciphering respectively, as both are popular software. So information security can be done by user of both software.

Plaintext is messages to be crypted, and ciphertext is encrypted messages that have been disguised. The process of converting a plaintext into a ciphertext is called encrypt, the otherwise is called decrypt. To encrypt and decrypt required a key cipher.

Stinson [3] defined cryptosystem as following:
A cryptosystem is a five-tuple (P, C, K, E, D) that satisfied: P is a finite set of possible plaintexts; C is a finite set of possible ciphertexts; K, the keyspace, is a finite set of possible keys; For each k ∈ K, there is an encryption rule ek ∈ E and a corresponding decryption rule dk ∈ D. Each ek: P → C and dk: C → P are functions such that dk(ek(x)) = x for every plaintext element x ∈ P.

Cryptography is divided into two types, that is classical cryptography (symmetric cryptography) and modern cryptography (asymmetric cryptography), [4]. Symmetric cryptography is cryptography with the same encrypt key and decrypt key, such as One Time Pad (OTP) and Affine cipher. On the contrary, in the asymmetric cryptography, the encrypt keys and decrypt keys are different, for example RSA and El Gamal. This paper will only consider the symmetric cryptography.

In cryptography, besides algorithm, a cipher key has an important role in securing messages. An unsafe key can affect a susceptible ciphertext being attacked or cracked by cryptanalyst. Ciphertext
breaking can be done by analyzing the frequency of letters, digrams, trigrams or other techniques, [3].
So, the improving of encryption security can be done by modifying the algorithm or key cipher. In doing
encryption, Dodis [5] states that we should pay attention on efficiency, strong security, and leakage
flexibility. Security level of keys can be seen from the number of possible keys or its resistance of
ciphering.

2. Methods
In this paper we highlight the encryption and decryption of some symmetric cryptography, briefly. The
chipering for each cryptography was developed by different method. The security level and the
enhancement of the security also studied.

3. Results and Discussion

3.1. Monoalphabetic substitution cryptography
In this section, we will discuss about encryption and ciphering in classical cryptography, i.e substitution
cryptography and stream cipher.

3.1.1. Substitution Cryptography. Substitution cryptography is mapping from a character to another.
Permutation process is one of substitution cryptography techniques. Alphabetic permutation example
below is taken from [1] with key permutation THE QUICK BROWN FOX JUMPS OVER LAZY
DOG without repeating letter.

![Figure 1. Alphabet permutation, k.]

Set of $\mathcal{K}$, permutation is a group. Let $k \in \mathcal{K}$.
The formula to encrypt:
$$c_i = k(p_i), \ \forall \ i = 1, ..., n.$$  

The formula to decrypt:
$$p_i = k^{-1}(c_i), \ \forall \ i = 1, ..., n.$$  

where $c_i = i$-th cipher, $p_i = i$-th plaintext, $n = $ length of plaintext, $k^{-1} = $ inverse of $k$.

For $k$ in Figure 3, the inverse is $k^{-1}$, i.e.

![Figure 2. Inverse Permutation, $k^{-1}$.]

3.1.2. Cripitanalysis by frequency Analysis. The paragraph text follows on from the subsubsection
heading but should not be in italic. The frequency of letters occurrence in each language is different.
In English, ‘e’ is the most letter occurrence, followed by ‘t’, ‘a’, ‘o’, and ‘n’, [1]. In extreme case,
Gadsby write a book without ‘e’, so that frequence of ‘e’ in the book is 0. It means the distribution of
letter frequence is not always the same. However, we can take the general phenomenon. In Indonesian,
‘a’ is much more occur. Marwati, in [6], shows the difference sort of letter frequence of three
Indonesian Novels, i.e Thalita – Stephani Zen, Rembulan Tenggelam di Wajahmu – Tere Liye, and
Supernova – Dee Lestari.

The two first novels have similar distribution frequency occurrence, but the Supernova is the special
case as Gadsby’s book. In Figure 3 we show the distribution of letter frequency of other novels, i.e
‘Tenggelamnya kapal Van Der Wijck’, ‘Layar Terkembang’, ‘Perahu Kertas’, and ‘Laskar Pelangi’.
The figure indicates that the distribution almost similar. Andana [7] studied letter frequency on Indonesian text for fiction, non-fiction, newspaper, speech, and song. He concluded that sort of 10 letter frequency is a, n, e, i, u, k, t, m, s, and g. Almost similar to Figure 3. The first five most frequent usually used as reference to ciphering. Then we can use digram (ex. ‘di’, ‘ke’, or ‘me’), trigram (ex. ‘dan’), and so on.

Steps to break substitution ciphertext are: 1) Let a ciphertext and write all in non capital letter; 2) Take a letter frequency distribution reference; 3) Count each letter frequency of the ciphertext; 4) Replace the most letter frequency of ciphertext with the one of reference in capital letter (i.e ‘A’); 5) Repeat step 4) for the second and the third most letter frequency of the ciphertext; 6) Guess some other letter by possible words; digram and trigram can be used; next letter of sort letter frequency can also be used.

Microsoft Office Word can be used as a tool to break substitution ciphertext. To count a letter frequency use ‘Find’, the letter frequency will be shown on Navigation. To substitute a letter use ‘Replace’ and click on ‘Match Case’. These can be seen on Figure 4.
3.2. **Stream Cipher**

Substitution cipher on Section 3.1 is a monoalphabetic substitution cryptography, which each letter is mapped to exactly another letter. Stream cipher is a polyalphabetic substitution cryptography. One letter can be mapped to more than one different letter.

3.2.1. **Vigenere Cipher**. Vigenere cipher is one of stream cipher. Encrypt process is ‘addition’ between plaintext and key cipher. Length of key on Vigenere cipher is finite. Then if the length of plaintext is more than length of the key, then key is repeated. For example, if the plaintext is ‘balonkuadalmaruparupawarnanya’ and the key is ‘LAGU’, then the key becomes ‘LAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULAGULL
$f_0, f_1, ..., f_{25}$ denote the frequencies of $A, B, ..., Z$. Index of coincidence of Indonesian, due to Figure 6 is 0.08.

Pratama on [8] determined the length of Vigenere key as follows: Let string $y = y_1y_2...y_n$ is Vigenere ciphertext. Write coset $m$ as substrings

\[
y_1 = y_1y_{m+1}y_{2m+1}...
\]
\[
y_2 = y_{2m+2}y_{2m+2}...
\]
\[
\vdots
\]
\[
y_m = y_{mn}y_{2mn}...
\]

It forms rectangular array on size $m \times (n/m)$. Count $I_c(m)$ as mean of $I_c(y_i)$. The length of Vigenere key is $m$ with the closest to the Indonesian index of coincidence.

Finding the length of Vigenere key by Microsoft Excel may be failed because of ciphertext is too short as shown in example in Figure 6 (b). Contradict to the length of key ($m=4$), the closest to 0.08 is for $m=3$ and $m=5$.

![Figure 6](image.png)

Figure 6. Index of Coincidence for $m=1, m=2, m=3, m=4, m=5$

To find each letter of the key is, as suggested by Cameron [1], by try all possible letters then count the fitting by Chi-Square. The Chi-Square, notated by $\chi^2$, is defined as follows:

\[
\chi^2 = \sum_{i=0}^{25} \frac{(f_i - F_i)^2}{F_i}
\]

where $f_i$= $i$-th letter frequency of ciphertext; $F_i$= $i$-th letter frequency of distribution letter frequency.

3.3. Cryptography Security Level

Cryptography security level can be seen by the number of possible keys or the easiness of algorithm.

On classical cryptography, the key and the algorithm are hidden. On modern cryptography, the public key and the algorithm are open, but private key is secured in hand receiver.

3.3.1. The Number of Possible Key. Substitution cryptography by shifting permutation, as Caesar cipher, has $n$ possible keys, where $n$ is the number of character. So that, the ciphering can be done by trying one by one of all this possible keys. It is not too difficult.
Refer to substitution monoalphabetic cipher on Section 2.1.1., the number of possible keys are equal to \( n! \). As a result, the possible keys to ciphering 26 character cipher is 26!. So, we have to find 1 of 26! possibilities. Not an easy thing. So that the Letter Frequency Analysis Techniques is helpful.

Even Vigenere cipher key (Section 2.2.2.) looks more simple than monoalphabetic substitution cipher, but the number of possibility keys is uncountable. Fortunately, because of the repeated key, we can use index of coincidence and Chi-Square to find the key. So, the weakness of the Vigenere cipher is this repeated key.

### 3.3.2. One Time Pad Cipher (OTP) with Fibonacci Sequence

OTP in [1], which introduced by Frank Miller in 1882, used unrepeated key cipher. The process on OTP is equal to the Vigenere cipher process, i.e. adding on arithmetic modulo. The formula of OTP encryption is:

\[
c_i \equiv (p_i + k_i) \mod m,
\]

where \( c_i \) = cipher \( k_e \)-i, \( p_i \) = plaintext \( k_e \)-i, \( m \) = the number of character, \( n \) = length of plaintext = length of OTP key. The formula of OTP decryption is:

\[
p_i \equiv (c_i - k_i) \mod m,
\]

Although OTP cipher is unbreakable, but determining a long key could make the encryption complicated. Firdaus [9] developed OTP by Fibonacci sequence. The key is generated by two first numbers \( a \) and \( b \). For example, let \( a=2 \) and \( b=5 \), then the OTP key is 2, 5, 7, 12, 19, ..., a simple and safe key. Others infinity sequence can be an OTP key.

OTP cipher with Fibonacci key by Microsoft Excel tools are shown in Figure 7.

![Figure 7. OTP cipher with Fibonacci Key](image)

Fill in cell A9: =HLOOKUP(A8;$A3:$Z4;2); then copy to the right; Let Fibonacci \( a=2 \) on cell C12 and \( b=5 \) on cell C13; next cell A14: =B12; cell B14: =B13; cell C14: =MOD(A14+B14;26), then copy to the right; cell A17: =MOD(A9+A14;26), copy to the right; cell A18: =HLOOKUP(A17;$A4:$Z5;2), copy to the right. The OTP ciphertext with key \( a=2 \) and \( b=5 \) is DFSGP5SEQRAXCCBLPEKVJZEDNFG. Cryptanalysis for OTP with infinity sequence key can be learn more.

### 3.4. Security Enhancement

Cryptography security enhancement can be done before encryption process or at the time of encryption. Eliminating spaces in plaintext is one of the simplest ways to improve cipher security, as well as replacing a word with common terms or abbreviations, such as words 'tanggal' with 'tgl', 'tempat' with 'tmp', and so on. Another way to enhance the security is by writing down plaintext into a matrix form and then setting up the matrix arrangement, such as Transposition Cipher and Hill cipher [1].
3.4.1. **Row Transposition Cipher (RTC).** In Row Transposition cipher, plaintext is arranged into an \( m \times n \) matrix. The key changes the order of the columns. For example, plaintext ‘balonkuadalimaruparupawarnanya’ is arranged into 5\( \times \)6 matrix, then using transposition 415263, we have a matrix as on Figure 8.

![Figure 8. Transposition Cipher](image)

RTC ciphertext is read following column from top to bottom, oauaabumpanlrxaanxldrw.

3.4.2. **Combining.** Enhancement security can also be done by combining two cryptography algorithm. Mishra [10] combining RTC and Caesar cipher. Firdaus [9] combining OTP and Affine cipher. Enhancement security can also done by combining classical cryptography and modern cryptography, as Ristiana in [11] which combining OTP dan RSA.

4. **Conclusion**

Simple classical cryptography can be done using a common software so that information security can be done easily. Substitution monoalphabetic cryptography can be done using Microsoft Word. Stream cipher can be done using Microsoft Excel.

Monoalphabetic substitution cipher cryptanalysis for Indonesian text can be done by using analysis letter frequency based on distribution of letter frequency in Indonesian Language. Vigenere Cipher cryptanalysis is done by calculating the index of coincidence to calculate the length of the key, and proceed by calculating the chi square to determine the key or by analysis letter frequency technique. The calculation of the key length can be done by using Microsoft Excel.

Cryptographic security can be seen from the number of possible keys. The more keys the more complicated the cryptanalysis will be. The Fibonacci row which is generated by two letters is a simple OTP key, but it is difficult to solve.

Cryptographic security enhancement can be done by developing unbreakable key, using cipher transformation techniques, or combining cryptography.

5. **References**

[1] Cameron P J and Mary Q 2003 Notes on cryptography *Lond. Univ. Lond* 16
[2] Podstata J and Podstata J Cryptanalysis of classical ciphers.
[3] Stinson D R 2005 *Cryptography: theory and practice* (CRC press)
[4] Ariyus D 2008 *Pengantar Ilmu Kriptografi: Teori Analisis & Implementasi* Penerbit Andi
[5] Dodis Y, Haralambiev K, López-Alt A and Wichs D 2010 December. Efficient public-key cryptography in the presence of key leakage *In International Conference on the Theory and Application of Cryptology and Information Security* pp 613-631 Berlin : Springer
[6] Marwati R 2017 Pengantar Kriptografi Bandung: Matematika FPMIPA UPI
[7] Andana G 2010 *Analisis Frekuensi pada Teks Bahasa Indonesia dan Modifikasi Algoritma Kriptografi Klasik* (repository.usu.ac.id/bitstream/handle/123456789/67062/)
[8] Pratama A 2017 *Penggunaan Metode Chi-Square Dalam Memecahkan Sandi Vigenere* Doctoral dissertation Universitas Pendidikan Indonesia
[9] Firdaus I L, Marwati R and Sispiyati R 2018 Aplikasi Kriptografi Komposisi One Time Pad Cipher Dan Affine Cipher *Jurnal EurekaMatika* 5 2 42-51
[10] Mishra A 2013 Enhancing security of caesar cipher using different methods *International Journal of Research in Engineering and Technology* **2** 9 327-332

[11] Ristiana M G, Gozali S M and Marwati R 2017 Algoritma Hybrid Kriptografi RSA dengan Kriptografi One Tipe Pad (pre printed)