Securing Text Messages using the Beaufort-Vigenere Hybrid Method

E Sugiarto¹, D R I M Setiadi¹, A Fahmi², E H Rachmawanto¹, C A Sari¹, Md K Sarker³ and B Widjajanto²

¹ Department of Informatics Engineering, Dian Nuswantoro University, 207 Imam Bonjol Street, Semarang 50131, Indonesia.
² Department of Information System, Dian Nuswantoro University, 207 Imam Bonjol Street, Semarang 50131, Indonesia.
³ Department of Computer Science, Kansas State University, Manhattan, Kansas 66506, USA

Abstract. Beaufort and Vigenere are fast and strong substitution encryption methods against brute force attacks if they have good key quality. But both of these methods by default can not produce a good avalanche effect. Avalanche effect is a measuring tool that can determine the strength of encryption from differential attacks. This research proposes hybrid techniques of Beaufort and Vigenere algorithms to optimize the security of text message encryption by modifying key generators. With this method, the encryption process can be done by input text messages and keys. The key is processed with a key generator to produce two new keys that are used for encryption using the Beaufort and Vigenere hybrid methods. Based on the test results, the Avalanche effect value rose significantly compared to the standard method, and the value of the avalanche effect was more stable and close to ideal compared to the previous method. The time required is also relatively very fast for the encryption or decryption process, experimental result shows it takes less than 0.1 seconds for more than 43 thousand of characters in the text message.

1. Introduction

Human civilization has changed a lot due to the rapidly developing technology. In the past, sending messages was done manually using couriers. At present, the use of the internet network has become a basic human need for sending messages digitally. The digital age is indeed very fast, practical and real-time. This makes more and more people use the internet especially for sending messages. The security of digital messages when sent to the recipient is very important, so the messaging system must be able to guarantee the security of the message [1,2]. Although the path of sending messages has been provided by security systems such as firewalls or private networks, it is not impossible for hackers to carry out attacks. Secret messages can be stolen and this is very dangerous, especially if the message is very important and valuable, so security must be done on the device sending the message, also on the message itself. Messages can be secured by the cryptographic method. Cryptography is a message encoding technique that makes a message obscure because of changes in its form and meaning [3].

Cryptography on digital data can be done on a variety of digital data. Previous research on cryptography [4] has been proposed using a hybrid encryption method, using two keys and combining two cryptographic methods Beaufort and Vigenere. This hybrid encryption method is performed on
digital images to increase its security before being hidden. If analyzed this method is quite interesting, simple and powerful. But in the research, the analysis and cryptographic tests are less detailed because the research is more focused on data hiding techniques. Cryptographic methods are numerous, such as permutation, substitution, diffusion, and others. Advanced Encryption Standard (AES), Elliptic Curve (EC), hyperchaotic, RC4, Vigenere, Beaufort, and Hill Cipher algorithms [5–13], are some of the most studied cryptographic methods.

In the cryptographic method, there are several important principles that must be fulfilled, namely confidentiality, authentication, integrity [9], where all principles lead to the principle of security. At present many cryptographic types of research do not do complete security testing, there are also many studies that only test computing performance and memory usage[6,7], some review papers or surveys are also limited to discussing the theories, differences, and characteristics of each method [14–16]. In research [4] security testing is also only carried out on the part of embedding and extraction, even though there is a combination of cryptographic methods that are quite interesting, namely Vigenere and Beaufort. Both of these cryptographic methods are classical cryptography which was very popular in its time, and many were developed into new algorithms. This algorithm is superior in computational performance and is simple when implemented.

In research [17], Vigenere method has also been developed to increase safety. Because by default the Vigenere method has a deficiency in the value of the avalanche effect (AE). Plaintext modification or key modification cannot get an ideal AE value. AE is a measurement tool to know the sensitivity level of bit randomness, it is important to know the resilience of cryptographic methods against differential attacks[1]. The avalanche effect test results produced by the method proposed in research [17] turned out to be improved, although not yet ideal and still need to be optimized again. Other research [18] developed the Vigenere method with a combination of the shift method, the results can increase a significant avalanche effect but only on changes in key bits, while the change in plaintext bits still needs to be optimized again. This research aims to research, analyze and develop hybrid encryption methods namely Beaufort and Vigenere to increase security based on various security tests, especially using the avalanche effect measurement tool, as well as computing performance testing.

2. Research Method

Beaufort and Vigenere encryption methods are cryptographic substitution techniques that use XOR operations for binary numbers and modulo operations for integers as the main process [4,12]. Substitution techniques change values based on keys. The combination of the two encryption methods is mostly done in sequence, where the first encryption is performed and then followed by the second encryption to create super encryption[13]. In this research, a hybrid encryption technique is proposed by mixing two methods using two keys. Where the first key for the main encryption operation and the second key to determining the encryption method. These two keys come from processing only one key. This key comes from user input so that users can create keys that are custom and easy to remember. This is different from previous research [4], where the HBV encryption method uses a randomly generated key, so the key must be stored for the decryption process. The objects used are also different, and in this research, the key input was modified to be customized by the user. However, the length and complexity of the key will still affect the security of the encoded message. In more detail, the proposed method is answered in the steps below.

2.1. Encoding stage

At the encoding stage text messages and keys are entered. Because the key comes from user input, it will be read as a string. The key can be in the form of letters, numbers, or symbols which will later be converted into ASCII characters. Then the key will be processed to create two other keys that are used in the encoding process. In detail the encoding process can be explained as follows:

1. Text messages are read, then converted to ASCII values and stored in a variable (t), text messages are also calculated in length and stored in variables (lt).
2. Read key, then save in variable (k) and key length in the variable (lk).
3. Sum the ASCII value of the t variable then save it in the sumt variable.
4. Sum the ASCII value of the k variable then save it in the sumk variable.
5. Create a key for the encryption \((ek)\) process by extending \(k\) to the same length as the \(lt\) variable, use looping to extend. For example:
   \[ t = \text{Dian Nuswantoro University}; \ lt=26 \]
   \[ k = \text{polke}; \ lk=5 \]
   \[ ek = \text{polkepolkepolkepolkepolke} \]
6. Create a switch key \((sk)\) using the mod operation to generate binary value. For more detail, see the formula (1).
   \[ sk_i = \text{mod}((\text{sumt} + \text{sumk} + ek_i + i), 2) \quad (1) \]
7. Encrypt Beaufort with the formula (2) if the value \(sk_i=1\), encrypt Vigenere with the formula (3) if the value \(sk_i=0\).
   \[ et_i = \text{mod}((ek_i - t_i), 256) \quad (2) \]
   \[ et_i = \text{mod}((t_i + ek_i), 256) \quad (3) \]
8. Get the encrypted message from step seven, then add the \(\text{sumt}\) value variable to the end of file encrypted message. To see the encoding process, see Fig. 1.

**Figure 1.** Encoding process

2.2. Decoding stage
The decoding stage is the process of returning encrypted messages to original messages. At this stage, encrypted messages and the same key are used at the encoding stage. In detail, the process is as follows.
1. Read the encrypted message and then retrieve the \(\text{sumt}\) value at the end of the file.
2. Convert encrypted messages to ASCII value \((et)\).
3. Read key, convert to ASCII value then save in variable \((k)\) and key length in the variable \((lk)\).
4. Run step 4 through step 6 in the encoding process to get the variable \( su^k, e^k, \) and \( sk \).
5. Decrypt using formula (4) to get the text decryption \( (dt) \) in the ASCII value.

\[
\begin{align*}
    & dt_i = mod((ek_i - et_i), 256), sk_i = 1 \\
    & dt_i = mod((et_i - ek_i), 256), sk_i = 0
\end{align*}
\]

(4)

6. Decryption results in the form of ASCII values are converted into strings to produce text message decryption. For a clearer picture, see Fig. 2.

**Figure 2.** Decoding process

### 3. Implementation and Testing

At the first stage of implementing the method was tested using short texts like messages, namely “Universitas Dian Nuswantoro” and the key was to use the string “polke”. Then the process is as follows:

- Text message \( (t) = \) Universitas Dian Nuswantoro;
- Length of the text message \( (lt) = 26 \);
- ASCII value of \( t = 68\ 105\ 97\ 110\ 32\ ...\ 121 \);
- Sum of \( t \) ASCII value \( (sumt) = 2622 \)
- Key \( (k) = \) polke;
- Length of key \( (lk) = 5 \);
- ASCII value of \( k = 112\ 111\ 108\ 107\ 101 \);
- The sum of \( k \) ASCII value \( (sumk) = 539 \);
- Extended key \( (ek) = \) polkepolkepolkepolkepolke

Next, create the switch key \( (sk) \) using formula (1). Perform the encryption process so that the results obtained = 'śżęûöÉôůyłñÁyO(ôÉôO-ôûł+ył' s as an encrypted message. To find out the quality of encryption several measuring tools are used, namely the avalanche effect (AE), bit error ratio (BER) and time taken. AE serves to measure the resilience of the encoding results against differential
attacks, how to calculate it by comparing the value of encoded message bits with other encoded messages that are slightly modified on the key or plaintext. Calculation of AE values can be seen with the example below:

**Table 1.** Sample encryption results using a slightly different key.

| Message       | Universitas Dian Nuswantoro | polke | polkf |
|---------------|-----------------------------|-------|-------|
| Encrypted (ASCII) | [UTF-8 encoded]              | [UTF-8 encoded] |
| Encrypted (binary) | [Binary encoded] | [Binary encoded] |

| Message       | Universitas Dian Nuswantoro | Universitas Dian Nuswantoro |
|---------------|-----------------------------|-----------------------------|
| Key           | polke                       | polke                       |
| Encrypted (ASCII) | [UTF-8 encoded]              | [UTF-8 encoded] |
| Encrypted (binary) | [Binary encoded] | [Binary encoded] |

From the results presented in Table 1 and Table 2, there are results in the form of binary encryption. Two binary-shaped encryption results from key differences and plain differences compared to the difference in bits to calculate the AE value. AE formula can be seen in formula (1).

\[
AE = \frac{\sum \text{diff}B}{\text{all}B} \times 100\%
\]

(1)

Where \(e1\) is encrypted message1 bits, \(e2\) is encrypted message2 bits, \(i\) is bit index, \(\text{diff}B\) are total different bits of both encrypted message, \(\text{all}B\) is the length of encrypted message bits (\(e1\) and \(e2\) must have the same length)

Based on the formula (1), the AE value = 40.2778\% in Table 1 and 44.9074\% for the AE value in Table 2. The AE value produced is indeed slightly less ideal, but the AE value generated in the key or text modific is in the range above 40\%. When compared with the method proposed by Salam et al [18], there is a significant AE value gap between key and text modifications. The results of the AE on the key modification are very good while the plain modification is very far from ideal, to see more clearly, a comparison of the results of the AE is presented in Fig.1.

From the results presented in Fig.1, it appears that the AE value in the proposed method is more stable and has a smaller gap compared to the previous method. After testing the AE in the sample text above, the test is also performed on a longer text message. Another test, namely BER, is also performed, the BER test is used to determine the level of standards on the encryption results, while the BER decryption results can be used to measure the percentage of the similarity of the original message to
the decrypted message. It should be noted that the correct decryption result is exactly the same as the 
original message with the decrypted message. Just a little difference can change the meaning of the 
message. To calculate the value of BER you can use the formula (2).

\[
BER = \sum \text{diff}B \\
\text{diff}B \begin{cases} 
\text{diff}B_i = \text{diff}B_i + 1, & o_i \neq d_i \\
\text{diff}B_i = \text{diff}B_i + 0, & o_i = d_i 
\end{cases}
\]

Where \( \text{diff}B \) are total different bits of the original and decrypted message, \( o \) and \( d \) must have the 
same length, \( o \) is original message bits, \( d \) is decrypted message bits, \( i \) is bit index. It also measured the 
performance of computing in the encryption and decryption process. Table 3 presents the results of the 
calculation of the measurement tool from the message encryption results, where the message used is 
the Lorem Ipsum text which can be found at the link address https://www.lipsum.com/feed/html, the 
text is then copied on the notepad, only enter characters are omitted, so there are 2,707 characters in 
the text with a size of 2,707 bytes. The message with more characters is Lorem Ipsum text that is 
copied 2, 4, 8, and 16 times. The key used to encrypt is 'password' and the key modification is 
'passwore'. As for the modification of plain text, the letter L is changed to K at Lorem at the beginning 
of the message.

![Avalanche Effect Comparison](image)

**Figure 3.** Comparison avalanche effect with previous method[18].

Note the BER results and the encryption times presented in Table 3 are the first encryption of the 
original message text with the 'password' encryption key. The BER value and execution time can be
different, depending on the number of keys, the text of the message, while the computing time is also affected by the hardware used.

| Number of char | BER | Decryption Time (seconds) |
|---------------|-----|--------------------------|
| 2,707         | 0   | 0.007632                 |
| 5,414         | 0   | 0.010829                 |
| 10,828        | 0   | 0.017137                 |
| 21,656        | 0   | 0.031962                 |
| 43,312        | 0   | 0.063022                 |

At the decoding stage, testing is also carried out to measure the quality of decryption. Decryption can be measured by using BER and computational time. The BER formula decryption process is the same as the BER formula with the encryption process, the difference is the input being compared. The BER decryption process compared is the original text message and decrypted text message. BER value must be 0, this means the process of decryption is perfect. Imperfect decryption process must be avoided because it can result in changes in the meaning of text messages. The results of the calculation of BER values of the decryption process are presented in Table 4.

In this study the encryption and decryption time is calculated using the tic toc function in Matlab. The results of the measurement of the time required for both the encoding and decoding process presented in Table 3 and Table 4 appear to be very fast. Both the encryption and decryption process takes less than 0.1 seconds. Tests carried out with AMD A12 7th generation processor and 4 GB RAM.

4. Conclusions
This research successfully combined two substitution encryption methods, namely Beaufort and Vigenere. With a slight modification to the key build algorithm, this combination of methods succeeded in getting an avalanche effect value above 46%. This value is quite close to ideal and better than the previous method because the value of the avalanche effect has a stable value on the modification of keys and plain text.

5. References
[1] Al-Muhammed M J and Zitar R A 2019 j-Lookback random-based text encryption technique J. King Saud Univ. – Comput. Inf. Sci. 31 92–104
[2] Al-Shakarchy N D, Al-Shahad H F and Al-Nasrawi D A 2018 Cryptographic system based on Unicode Journal of Physics: Conference Series vol 1032 (Institute of Physics Publishing)
[3] Kodabagi M M, Jerabandi M V. and Gadagin N 2016 Multilevel security and compression of text data using bit stuffing and Huffman coding Proceedings of the 2015 International Conference on Applied and Theoretical Computing and Communication Technology, iCATccT 2015 (Davangere: Institute of Electrical and Electronics Engineers Inc.) pp 800–4
[4] Susanto A, Setiadi D R I M, Rachmawanto E H, Sari C A, Ali R R and Wahyu Mulyono I U 2019 Dual Security Method for Digital Image using HBV Encryption and Least Significant Bit Steganography J. Phys. Conf. Ser. 1201
[5] Keerthi K and Surendiran B 2017 Elliptic curve cryptography for secured text encryption Proceedings of IEEE International Conference on Circuit, Power and Computing Technologies, ICCPCT 2017 (Kollam: Institute of Electrical and Electronics Engineers Inc.)
[6] Natanael D, Faisal and Suryani D 2018 Text Encryption in Android Chat Applications using Elliptical Curve Cryptography (EC) Procedia Computer Science vol 135 (Elsevier B.V.) pp 283–91
[7] Chaturvedi S and Sharma R 2015 Securing text & image password using the combinations of persuasive cued click points with Improved Advanced Encryption Standard Procedia Computer Science vol 45 (Elsevier B.V.) pp 418–27
[8] Dolendo Singh L and Manglem Singh K 2015 Implementation of Text Encryption using
Elliptic Curve Cryptography *Procedia Comput. Sci.* **54** 73–82

[9] Venkata Vidy Deepti D, Homer Benny B, Sreenu K and Id E 2019 Various Ciphers in Classical Cryptography *J. Phys. Conf. Ser.* **1228**

[10] Mathur N and Bansode R 2016 AES Based Text Encryption Using 12 Rounds with Dynamic Key Selection *Procedia Computer Science* vol 79 (Elsevier B.V.) pp 1036–43

[11] Irawan C, Setiadi D R I M, Rachmawanto E H, Sari C A and Doheir M 2019 Hybrid Encryption using Confused and Stream Cipher to Improved Medical Images Security *J. Phys. Conf. Ser.* **1201** 012022

[12] Najih M N M, Setiadi D R I M, Rachmawanto E H, Sari C A and Astuti S 2017 An improved secure image hiding technique using PN-sequence based on DCT-OTP 2017 *1st International Conference on Informatics and Computational Sciences (ICICoS)* (Semarang: IEEE) pp 47–52

[13] Putrie V M, Sari C A, Setiadi D R I M and Rachmawanto E H 2018 Super Encryption using Transposition-Hill Cipher for Digital Color Image *2018 International Seminar on Research of Information Technology and Intelligent Systems (ISRITE)* (IEEE) pp 152–7

[14] Abood O G and Guirguis S K 2018 A Survey on Cryptography Algorithms *Int. J. Sci. Res. Publ.* **8**

[15] Tayal S, Gupta N, Gupta P, Goyal D and Goyal M 2017 A Review paper on Network Security and Cryptography *Adv. Comput. Sci. Technol.* **10** 763–70

[16] Bokhari M U and Shallal Q M 2016 A Review on Symmetric Key Encryption Techniques in Cryptography *Int. J. Comput. Appl.* **147** 975–8887

[17] Singh G and Supriya 2013 Modified Vigenere Encryption Algorithm and Its Hybrid Implementation with Base64 and AES 2013 *2nd International Conference on Advanced Computing, Networking and Security* (IEEE) pp 232–7

[18] Salam A, Setiadi D R I M, Rachmawanto E H and Sari C A 2019 ShiftMod Cipher: A Symmetrical Cryptosystem Scheme *International Seminar on Application for Technology of Information and Communication (iSemantic)* (Semarang: IEEE) pp 34–8