ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 10, Issue 9, September 2023

# An Enhanced Key Generation and Key Security of Beaufort Cipher Expansion Technique Using Pseudo Random Number, Key Encryption, and Alphabet Extension Applied in Text Data

[1] Andrea B. Bacarisa, [2] Ma. Genina S. Dejacto, [3] Vivien A. Agustin, [4] Mark Christopher R. Blanco, [5] Jonathan A. Morano

[1] [2] Student, College of Engineering, Pamantasan ng Lungsod ng Maynila, Philippines
[3] [4] [5] Faculty, Computer Science Department, Pamantasan ng Lungsod ng Maynila, Philippines
Corresponding Author Email: [1] abbacarisa2019@plm.edu.ph, [2] mgsdejacto2019@plm.edu.ph, [3] vaagustin@plm.edu.ph, [4] mcrblanco@plm.edu.ph, [5] jcmorano@plm.edu.ph

***Abstract*— This study aimed to improve the security of the Beaufort Cipher Expansion Technique by addressing the cipher's vulnerabilities to Kasiski attacks, brute force attacks, and frequency analysis attacks. The research objectives include modifying the key-generation process and the key-encryption process and improving the matrix to mitigate these vulnerabilities. The analysis of the Kasiski attack revealed that the enhanced Beaufort Cipher Expansion Technique showed no pattern in the generated ciphertext, unlike the traditional Beaufort Cipher, which exhibited a trigram pattern. The result indicates that the enhanced technique effectively addressed the vulnerability to pattern recognition attacks. Also, the brute force attack analysis showed that it would take about 3.83376E+17 centuries to break a 10-letter ciphertext. The result indicates that the enhanced Beaufort cipher is strong against brute-force attacks. Regarding frequency analysis, the original Beaufort Cipher Expansion Technique resulted in a ciphertext with frequent occurrences of specific values, making it susceptible to such an attack. In contrast, the enhanced technique distributed characters evenly, making it more secure and challenging for attackers to extract meaningful information through frequency analysis. Furthermore, the avalanche effect analysis compared the enhanced Beaufort cipher expansion technique with other relevant studies, and it achieved an avalanche effect of 51.66%, surpassing the desired value of 50%. The results indicate that determining which bits of the original message change when altering a random bit becomes challenging, thus further enhancing the cipher's security. Overall, the findings demonstrated that the enhanced Beaufort Cipher Expansion Technique effectively addressed the vulnerabilities to the Kasiski attack, brute force attack, and frequency analysis attack. The modifications improved the security and robustness of the cipher, making it a valuable contribution to the field of cryptography.***

***Index Terms*— Alphabet extension, Beaufort cipher, Key encryption, Key generation.***

## I. INTRODUCTION

In this day and age, information continues to extend its reach and increase its value [1]. Transferring vast chunks of data and information over the internet between devices has been crucial for professional and personal use [2]. Information leaks are rampant as it grows in availability [3]. Information protection should be the utmost priority since there will always be a threat to data [1].

Data security is the practice of preventing digital data from being accessed by unauthorized entities, being corrupted, or being stolen at any point in its lifecycle [4]. An example of data security is cryptography, which deals with encrypting data, making information more secure. It offers security through identification and defense against data tampering and theft[3].

Beaufort is one of the cryptographic algorithms that is still being used today. Some of its current usages include text message encryption [5], securing documents in the cloud environment [6], and image steganography [7].

One example of a polyalphabetic substitution cipher is the Beaufort cipher. In the original Beaufort algorithm and

Beaufort Cipher Expansion Technique, the key is made by the user. This makes it subject to cipher attacks if the key length of the input provided by the user is shorter than the length of the plaintext. Furthermore, it does not have key security, which can also result in susceptibility to attacks. Based on the study of [6] Beaufort expansion technique is still prone to security threats, specifically Kasiski attacks, Brute Force attacks, and Frequency Analysis attacks.

This research aims to eliminate the stated problems of the Beaufort expansion technique by enhancing its key generation using pseudo-random numbers and its key security using a key encryption process. Furthermore, an alphabet extension of 256x256 from 26x26 will be implemented. This study was applied in data security, specifically text data, to test the effectiveness of the enhancements.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 10, Issue 9, September 2023

## II. RELATED LITERATURE

Cryptography is the process of encrypting data to increase information's safety. It protects against data tampering and theft and provides security through authentication [3]. Cryptography can be seen as a combination of mathematics and security. The purpose of it is to protect sensitive data and ensure privacy from illicit activity [8].

When the cipher employs repetitive words as keystreams, key patterns in ciphertexts are replicated at a rate equal to the length of the keyword. The Kasiski approach and the Index of Coincidence are two techniques for determining the length of the key [8].

In a study cited in [8] on the Vigenère algorithm that uses extended special symbols, lowercase letters, and numbers on its matrix. The authors argue that it is possible to resist brute-force attacks by encrypting uncommon letters with the cipher's extended range.

The Beaufort cipher algorithm is one of the examples of polyalphabetic substitution ciphers created by Sir Francis Beaufort [6]. It was said in [9] that Beaufort is a symmetric algorithm where one key is used in encryption and decryption. She also stated that the Beaufort algorithm is a variant of the Vigenère algorithm, which has a similarity in terms of the tabula recta used but is different in its encryption process.

The encryption process of the Beaufort is simple, and it uses a 26x26 table known as the tabula recta [10]. In the encryption process, the plaintext will be substituted by characters on the tabula recta. The sender and receiver share one secret key consisting of a word or a series of words. Each plain text character is encrypted using the key character. When the last key character has been utilized, the algorithm returns to the first key character and uses it. Every plaintext character should use one key character and locate the plaintext character in the topmost horizontal row. The second is scanning through the column until the current key character is found. Lastly, the leftmost character in that row is the equivalent cipher character. During decryption, the Beaufort algorithm has the property referred to as reciprocal cipher, which uses a similar process of encryption but in reverse. This way, when the reverse algorithm is applied to the ciphertext, the receiver can finally decrypt and understand it as plaintext.

According to [11], one random number generation algorithm that is said to have high performance among all other existing algorithms is Fisher-Yates. This is due to the known advantages of the algorithm over others. This modern algorithm has proven to have reduced the time complexity of the traditional algorithm significantly to O(N), as cited in [12], It was stated by [13] that the randomization method and its optimal complexity had been proven effective in avoiding repetition and duplication. This algorithm also produces unbiased results for each permutation of an array that has the same possibility.

It was concluded in [2] that applying two's complement on input values in bits has a significant contribution to cryptographic literature and provides increased security and increased efficiency than other algorithms.

In the [14] study on DNA-based encryption of IoT resources, the researchers used an XOR operation during the substitution phase of the encryption process and bit-swapping during the transposition phase as part of the improved model. The experimental findings demonstrate exceptional outcomes regarding the enhanced technique's random characteristics, significantly increasing potential attackers' difficulty decrypting the key.

Studies have been conducted over the years to enhance the Beaufort cipher algorithm. Here are some foreign studies that aimed to solve different problems using different enhancements to the Beaufort algorithm. [6] conducted a study on the Analysis of the Beaufort Cipher Expansion Technique and Its Usage in Providing Data Security in the Cloud. This aimed to improve the Beaufort algorithm to utilize it for providing security for text documents in the cloud environment.

The researchers cited some of the demerits of the cipher they intend to solve. First, the brute-force attack makes it easy to break the Beaufort cipher. Here, the intruder tries all the words in the dictionary as Beaufort's key to decipher the cipher text. Next, frequency analysis can also be used to decrypt Beaufort cipher text since the Beaufort encryption algorithm does not hide symbols that show up often in the cipher text.

The Beaufort Cipher Expansion Technique uses the original matrix, key generation, but with an expanded process for encryption. First, the plaintext will be ciphered using the original Beaufort cipher technique. The ciphertext is now the intermediate cipher. Then, calculate the ASCII value of the key and the intermediate cipher. Then, calculate the binary value of the key and the intermediate cipher. Now, perform an XOR operation between the binary key and the binary of the intermediate cipher. Lastly, calculate the decimal value of the XOR result to get the final cipher text.

The testing showed an improved frequency analysis, with a result of 23–30% for the most frequent character in the original algorithm and only a 20% result for the most frequent character in the modified algorithm. As for the brute-force attack, no testing was done to show that the changes made to the algorithm fixed the brute-force problem.

The study by [15] is a Hybrid Cryptosystem Using El Gamal Algorithm and Beaufort Cipher Algorithm for Data Security. This research aims to improve the problem of El Gamal regarding its encryption and decryption time.

The researchers enhanced the Beaufort algorithm using the ASCII character for its new matrix and randomizer for its key generation. For encryption, it uses the original Beaufort encryption. After that, the Beaufort key will be encrypted using the El Gamal algorithm before being sent to the sender. The result shows that the average encryption time is 7.6ms.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 10, Issue 9, September 2023

for ten characters, while its average decryption is 4.2ms.

[5] conducted a study entitled Securing Text Messages using the Beaufort-Vigenère Hybrid Method was conducted to be used for Securing Text messages. In this study, the low avalanche effect of both the Vigenère and Beaufort cipher was the problem that the proponents wanted to improve. An avalanche effect is a measuring tool that can determine the strength of encryption from differential attacks.

The researchers modified the cipher by using all the ASCII characters for its matrix and a new method for encryption using a switch key (*SK*) with a binary value. If the result of the *SK* is 1, then that character will be encrypted using Vigenère, but if the result is 0, that character will be encrypted using Beaufort; this will be repeated until all the plaintext is transformed into ciphertext. The assessment showed that the average avalanche effect of the proposed enhancement is 46%.

Double-Layered Text Encryption using Beaufort and Hill Cipher Techniques is researched by [16]. They conducted this study to combine Beaufort and Hill algorithms for text encryption. In this research, the issue that the researchers addressed was Beaufort's simple encryption method.

### B. Beaufort Cipher Expansion Technique

The researcher's enhancement was to use a double encryption method by having Hill encryption together with Beaufort. The 98 characters on the keyboard were also used for the new matrix. The modified process includes the original key generation process. Next, Beaufort encryption. Then, Beaufort's ciphertext will be encrypted using Hill cipher to get the final cipher.

To prove the effects of the enhancement, the avalanche test was conducted. The result showed that the proposed method has an avalanche effect value of 33.68%, while the original Beaufort and Hill have a value of 21.94% and 22.10%, respectively.

## III. THEORETICAL FRAMEWORK

### A. Beaufort Cipher Algorithm

The original Beaufort Cipher algorithm can be computed by subtracting the plaintext (P) from the key (K) modulo N which is the number of characters used in the tabula recta in order to obtain the ciphertext. According to [16], the formula for the Beaufort algorithm is:

$$Ciphertext = Key - Plaintext \bmod N \quad (1)$$

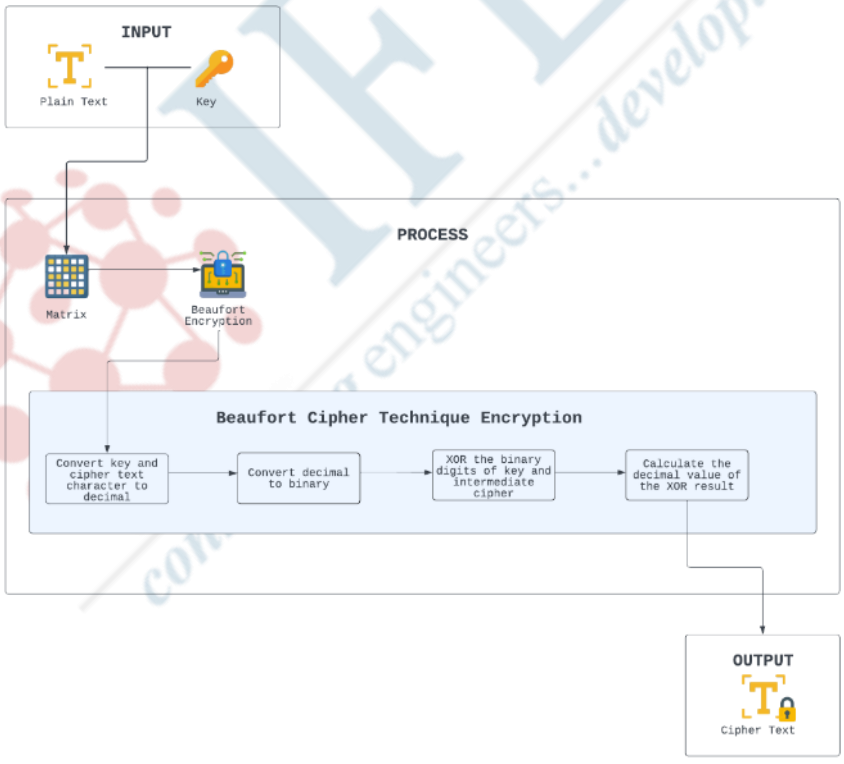


**Fig. 1.** Framework of the Beaufort Cipher Expansion Technique

Fig. 1 shows the Framework of the Beaufort Cipher Expansion Technique enhanced in this study. The encryption starts when a user inputs the plain text and the key. The algorithm utilizes the original size of the tabula recta, which is 26x26, to obtain the intermediate cipher text. This intermediate cipher will be converted into its corresponding ASCII values as well as the key. Then, binary values of these ASCII values will be calculated. Then, the XOR operation will be performed between the intermediate cipher and key. The decimal value of the result of the XOR operation will then be calculated as its final cipher text.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 10, Issue 9, September 2023

### C. Enhanced Beaufort Cipher Expansion Technique

**Table I:** Simulation of Modern Fisher-Yates Shuffle

| Total | Roll | Scratch | Result |
|---|---|---|---|
| | | 1 2 3 4 5 6 7 8 | |
| 8 | 6 | 1 2 3 4 5 **8** 7 | **6** |
| 7 | 2 | 1 **7** 3 4 5 8 | **2** 6 |
| 6 | 6 | 1 7 3 4 5 | **8** 2 6 |
| 5 | 1 | **5** 7 3 4 | **1** 8 2 6 |
| 4 | 3 | 5 7 **4** | **3** 1 8 2 6 |
| 3 | 3 | 5 7 | **4** 3 1 8 2 6 |
| 2 | 1 | **7** | **5** 4 3 1 8 2 6 |

Table I shows the simulation of the Modern Fisher-Yates Shuffle, the randomization method used to generate the randomized key of the Beaufort Cipher Expansion Technique. The Modern Fisher-Yates Algorithm starts by rolling a random number within the range and swapping with the last letter; the random number will be copied to another place. This process will proceed the same way until all the numbers are on the list and the permutation is complete.

**Table II.** Characters on the Proposed Alphabet Extension

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| a 1 | b 2 | c 3 | d 4 | e 5 | f 6 | g 7 | h 8 | i 9 | j 10 | k 11 | l 12 | m 13 | n 14 | o 15 | p 16 |
| q 17 | r 18 | s 19 | t 20 | u 21 | v 22 | w 23 | x 24 | y 25 | z 26 | A 27 | B 28 | C 29 | D 30 | E 31 | F 32 |
| G 33 | H 34 | I 35 | J 36 | K 37 | L 38 | M 39 | N 40 | O 41 | P 42 | Q 43 | R 44 | S 45 | T 46 | U 47 | V 48 |
| W 49 | X 50 | Y 51 | Z 52 | 0 53 | 1 54 | 2 55 | 3 56 | 4 57 | 5 58 | 6 59 | 7 60 | 8 61 | 9 62 | ! 63 | " 64 |
| # 65 | $ 66 | % 67 | & 68 | 69 | ( 70 | ) 71 | * 72 | + 73 | , 74 | - 75 | . 76 | / 77 | : 78 | ; 79 | < 80 |
| = 81 | > 82 | ? 83 | @ 84 | [ 85 | \ 86 | ] 87 | ^ 88 | _ 89 | ` 90 | { 91 | \| 92 | } 93 | ~ 94 | ¡ 95 | ¢ 96 |
| £ 97 | ¤ 98 | ¥ 99 | ¦ 100 | § 101 | ¨ 102 | © 103 | ª 104 | « 105 | ¬ 106 | Ù 107 | Ú 108 | Ý 109 | Þ 110 | ß 111 | à 112 |
| á 113 | â 114 | ã 115 | ä 116 | å 117 | æ 118 | ç 119 | è 120 | é 121 | ê 122 | ë 123 | ì 124 | í 125 | î 126 | ï 127 | ð 128 |
| ñ 129 | ò 130 | ó 131 | ô 132 | õ 133 | ö 134 | ÷ 135 | ø 136 | ù 137 | ú 138 | û 139 | ü 140 | ý 141 | þ 142 | ÿ 143 | Ā 144 |
| ā 145 | Ă 146 | ă 147 | Ą 148 | ą 149 | Ć 150 | ć 151 | Ĉ 152 | ĉ 153 | Ċ 154 | ċ 155 | Č 156 | č 157 | Ď 158 | ď 159 | Đ 160 |
| đ 161 | Ē 162 | ē 163 | Ĕ 164 | ĕ 165 | Ė 166 | ė 167 | Ę 168 | ę 169 | Ě 170 | ě 171 | Ĝ 172 | ĝ 173 | Ğ 174 | ğ 175 | G 176 |
| ġ 177 | Ģ 178 | ģ 179 | Ĥ 180 | ĥ 181 | Ħ 182 | ħ 183 | Ĩ 184 | ĩ 185 | Ī 186 | ī 187 | Ĭ 188 | ĭ 189 | Į 190 | į 191 | İ 192 |
| ı 193 | Ĳ 194 | ĳ 195 | Ķ 196 | ķ 197 | ĸ 198 | Ĺ 199 | ĺ 200 | Ļ 201 | ļ 202 | Ľ 203 | ľ 204 | Ŀ 205 | ŀ 206 | Ł 207 | ł 208 |
| Ń 209 | ń 210 | Ņ 211 | ņ 212 | Ň 213 | ň 214 | ŉ 215 | Ŋ 216 | ŋ 217 | Ō 218 | ō 219 | Ŏ 220 | ŏ 221 | Ő 222 | ő 223 | Œ 224 |
| œ 225 | Ŕ 226 | ŕ 227 | Ŗ 228 | ŗ 229 | Ř 230 | ř 231 | Ś 232 | ś 233 | Ŝ 234 | ŝ 235 | Ş 236 | ş 237 | Š 238 | š 239 | Ţ 240 |
| ţ 241 | Ť 242 | ť 243 | Ŧ 244 | ŧ 245 | Ũ 246 | ũ 247 | Ū 248 | ū 249 | Ŭ 250 | ŭ 251 | Ů 252 | ů 253 | Ű 254 | ű 255 | Ų 256 |

Table II shows the characters on the alphabet extension of the 256x256 *tabula recta* differing from the original algorithm by 230 characters**.** The *tabula recta* contain the alphabet, numbers, and symbols that were used in enhancing the key security during the encryption and decryption process of the Beaufort Cipher Expansion Technique Algorithm.

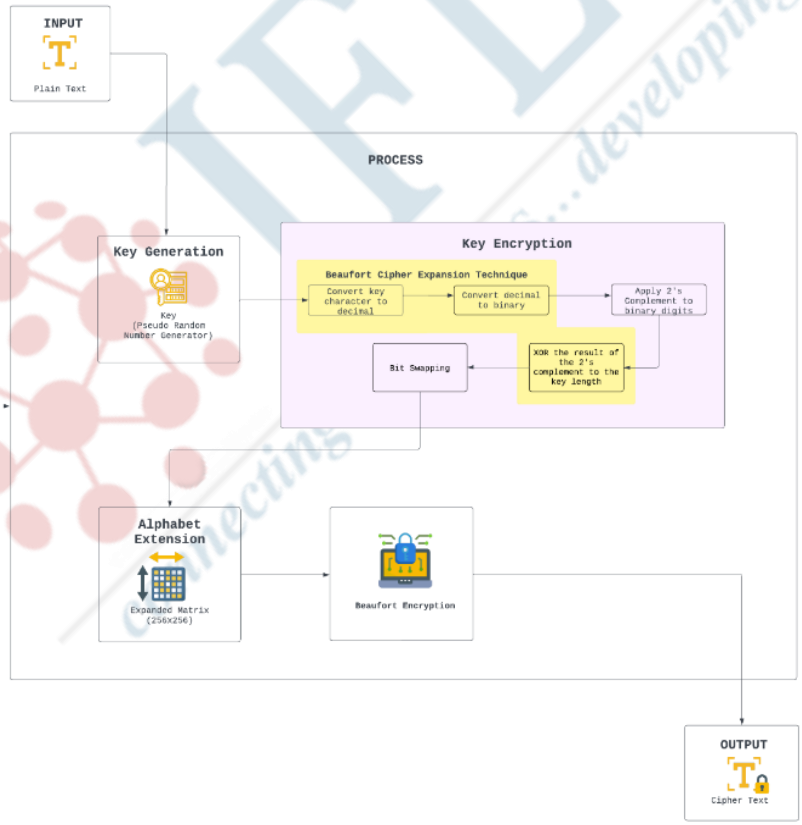


**Fig. 2.** Conceptual Framework of the Proposed Enhancement

Fig. 2 Figure 3 shows the process of the enhancement of the Beaufort Cipher Expansion Technique Algorithm. The process starts by accepting plaintext (PT) from the sender.

Then, pseudo-random numbers will be obtained using the Fisher-Yates algorithm that will be used as the key (K). It also shows key-encryption process starting by converting the character to decimal and decimal to binary. The two's complements of the binary digits will then be obtained, which will be XORed to the length of the generated key. Lastly, bit swapping follows the pattern where the last bit, l, will be in

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 10, Issue 9, September 2023

the first position, followed by the first bit, f, in the second position, the second bit in the third position, and so on. Then the encrypted key will be used to encrypt the plaintext and generate the final ciphertext using the Beaufort encryption with the expanded matrix of 256x256 characters.

***1. Pseudocode of the Enhanced Beaufort Cipher Expansion Technique***

Start
Read the plaintext
Generate key using the pseudo random number generator
Loop i with the length of plaintext
a.Calculate decimal values of key and plaintext
b. Calculate binary values of key and plaintext
c.Obtain the two's complement of the key and the plaintext
d. Perform the XOR operation between the binary values of key and plaintext
e.Perform bit swapping on the result of the XOR operation
Compute for the ciphertext using the extended matrix of 256x256 and Eq. (1)
End

## IV. METHODOLOGY

### A. Requirement Analysis

In this study, the researchers first analyzed the existing problems of the Beaufort Algorithm, which are its vulnerability to Kasiski, Frequency Analysis, and Brute force attacks. From this, the researchers created the set of objectives that this study must meet. Comprising of modification on the key-generation process to increase security against the Kasiski attack, modification on the key-encryption process to increase security against the Brute Force attack, improving the matrix by making it 256x256 to increase security against the Frequency Analysis attack. Lastly, the researchers also considered the scope and limitations of the project. After having a clear understanding of the requirements of the project, the researchers designed the framework of the study.

### B. Design

The design phase includes a detailed plan for the creation of the application. The existing problem is Beaufort's susceptibility to specific attacks. The researchers explored ways to mitigate these attacks and devised a framework that solved the existing problems. The new framework includes the using a pseudo-random number generator to generate the key. Then the generated key was encrypted by converting its character to decimal and then decimal to binary. The two's complement of the binary digits was then obtained, which was XORed to the length of the generated key. Lastly, bit swapping was applied. The encrypted key was then used to encrypt Beaufort's cipher using the new 256 x 256 matrix.

According to [11], one random number generation algorithm that is said to have high performance among all other existing algorithms is Fisher-Yates. This is due to the known advantages of the algorithm over others. This modern algorithm has been proven to have reduced the time complexity of the traditional algorithm significantly to O(N), as cited in [12]. It was stated by [13] that the randomization method and its optimal complexity had been proven effective in avoiding repetition and duplication. This algorithm also produces unbiased results for each permutation of an array with the same possibility.

In a study conducted by [2], they concluded that applying two's complement on input values in bits has a significant contribution to cryptographic literature and provides increased security and increased efficiency than other algorithms.

In the [14] study on DNA-based encryption of IoT resources, the researchers used an XOR operation during the substitution phase of the encryption process and bit-swapping during the transposition phase as part of the improved model. The experimental result shows outstanding results regarding its random nature, which will make it hard for the attacker to break the key.

[8] Cited a study on the Vigenère algorithm that uses extended special symbols, lowercase letters, and numbers on its matrix. The authors argue that it is possible to resist brute-force attacks by encrypting uncommon letters with the cipher's extended range.

### C. Development

Python is considered one of the well-liked and widely used high-level programming languages in cryptography for its versatility, simplicity, and security. Moreover, it has an extensive range of libraries freely available to the public that supports cryptography, thus making it easier to implement secure and efficient cryptographic algorithms. The language encourages program modularity and code reuse by having modules and packages. It is continuously used by numerous organizations for their critical applications because of the language's reliability and efficiency.

The Integrated Development Environment (IDE) that was utilized by the researchers is Visual Studio since it has a user-friendly interface and provides an extensive set of tools and features. Visual Studio Code was developed by Microsoft and is widely used due to its dominant features and flexibility as it is available for different operating systems. VS Code supports several programming languages and offers extremely useful features suited to the developer's needs, such as debugging, version control, code completion, and syntax completion. Extensions can also be installed into the VS Code to expand its functionalities. It is an excellent choice for developers as it can work on multiple platforms, lightweight, customizable, and is open-source. Moreover, this IDE is advantageous in Python development as it provides excellent support tools in the development process.

The random library is a Python library used for generating random values in the program. It supplies a set of functions mainly for generating numbers, selecting random elements in

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 10, Issue 9, September 2023

a sequence, and shuffling sequences. These functions are beneficial for different applications, especially cryptography. This library was used for generating a pseudo-random number needed for strengthening the security of the key.

The time library provides a set of functions when working with tasks relating to time. It includes measuring the execution time, scheduling, and other time-related data. In the enhanced algorithm, the time library was used in measuring the execution time of key encryption that will be used for Brute Force Attack Analysis. This analysis is used to determine the estimated amount of time to crack the cipher text successfully.

### D. Testing

Kasiski Attack Analysis is a test used to determine if there is an existing pattern of letters in the ciphertext that can be used in determining the key length. If it is known, cryptanalysis can easily be performed to decrypt the message. Letter repetitions enable the production of repetitive cryptograms [17].

The steps for the Kasiski Attack to be carried out are as follows:

a. Determine all the repeating cryptograms in the ciphertext.
b. Determine the interval between repetitive cryptograms.
c. Calculate all the factors/divisors of the distance that represents the key length.
d. Determine the slices from the group of dividing factors. The value displayed in the slice reflects the number that may be found on every dividing factor of the distances that could be the key length.

The brute force attack is carried out successfully by efficiently predicting each key combination until the appropriate character is found and then comparing the result to the known plaintext. It aims to use all possible combinations until the match is found [3]. The formula for calculating the estimated time to perform a Brute Force attack successfully is as follows:

$$ET = \frac{Number\ of\ Character\ Set^{Key\ Length}}{Encryption\ per\ Second\ (EPS)} \qquad (3)$$

The Brute Force attack's success is dependent on several factors such as key length, no. of characters in the set, as well as its computation speed.

There are letters in the alphabet that frequently occur in words from the dictionary. This testing obtains the distribution of characters on a cipher text. It indicates the frequently occurring symbols that make it easier for cryptanalysis to be carried out.

A desirable feature of encryption algorithms is the avalanche effect, wherein a minor modification to either the key or the plaintext should result in a notable change in the cipher text [18]. The formula for the avalanche effect of a cipher algorithm is shown below:

$$AE\ (\%) = \frac{\#\ of\ Changed\ Bits\ in\ Cipher\ text}{Total\ \#\ of\ Bits\ in\ Cipher\ text} \times 100 \qquad (3)$$

To satisfy the avalanche effect whenever an input bit is changed, each output bits complement should have a probability greater than 50% [19]. This probability is an ideal value since this means that it is impossible to distinguish which bit was modified after flipping a random bit of the original message [20].

## V. RESULTS AND DISCUSSION

**Table III.** Result of Kasiski Attack Analysis

| | Traditional Beaufort Cipher | Enhanced Expansion Technique |
|---|---|---|
| **No. of Chars** | **25** | **25** |
| **Plaintext** | hellohellohellohellohello | hellohellohellohellohello |
| **Key** | key | œåjòzæŮąďõ=ĎJŰAɆčČŤóŰDũ,ĭ |
| **Ciphertext** | danzqrgtnwxuztkdanzqrgtnw | ĆĹēNâ%kĠġĂŀ5^eŤ\ÍZaĖbēï/đ |
| **Pattern** | trigram | no pattern |

Table III presents the result of the Kasiski Attack analysis for both the traditional and enhanced expansion techniques. The purpose of the Kasiski method is to find two or more repetitive cryptograms to determine the length of the key [17]. If no pattern is found using the Kasiski examination in the ciphertext, the cryptanalyst must explore other methods for breaking the cipher. The table shows that the traditional Beaufort Cipher formed a pattern called "trigram," while the enhanced Expansion Technique did not form any pattern.

**Table IV:** Trigram Result of the Traditional Beaufort Algorithm

| **Trigram result** | | |
|---|---|---|
| **DAN** | 2× | 25% |
| **ZQR** | 2× | 25% |
| **GTN** | 2× | 25% |
| **WXU** | 1× | 12.50% |
| **ZTK** | 1× | 12.50% |

Table IV presents the trigram result of the Traditional Beaufort Algorithm. The generated ciphertext is "danzqrgtnwxuztkdanzqrgtnw." Where "dan" appeared twice, "zqr", appeared twice, and "gtn" appeared twice, which means that the trigram pattern exists in this set of characters.

**Table V.** Bigram Result of the Enhanced Beaufort Expansion Technique

| **Bigram result** | | |
|---|---|---|
| **ĆĹ** | 1× | 8.33% |
| **ēN** | 1× | 8.33% |
| **â%** | 1× | 8.33% |
| **kĠ** | 1× | 8.33% |

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 10, Issue 9, September 2023

| Bigram result | | |
|---|---|---|
| ġĂ | 1× | 8.33% |
| l·5 | 1× | 8.33% |
| ^e | 1× | 8.33% |
| Ť\ | 1× | 8.33% |
| ĬZ | 1× | 8.33% |
| aĖ | 1× | 8.33% |
| bê | 1× | 8.33% |
| ï/ | 1× | 8.33% |

Table V shows the bigram result of the Enhanced Beaufort Expansion Technique. The generated ciphertext is "ĆĹēNâ%kĠġĂl·5^eŤ\ĬZaĖbêï/đ". As presented in the table, all possible bigrams occurred only once in the ciphertext, meaning no pattern is evident.

**Table VI.** Trigram Result of the Enhanced Beaufort Expansion Technique

| Trigram result | | |
|---|---|---|
| ĆĹē | 1× | 12.50% |
| Nâ% | 1× | 12.50% |
| kĠġ | 1× | 12.50% |
| Ăl·5 | 1× | 12.50% |
| ^eŤ | 1× | 12.50% |
| \ĬZ | 1× | 12.50% |
| aĖb | 1× | 12.50% |
| êï/ | 1× | 12.50% |

Table VI exhibits the trigram result of the Enhanced Beaufort Expansion Technique. The generated ciphertext is "ĆĹēNâ%kĠġĂl·5^eŤ\ĬZaĖbêï/đ". As presented in the table, all of the possible trigrams occurred only once in the ciphertext, meaning that no pattern is evident in the ciphertext.

**Table VII.** Brute Force Attack Analysis Result

| Unit | Estimated Time to Crack |
|---|---|
| Minutes | 2.02E+25 |
| Hours | 3.36E+23 |
| Days | 1.40E+22 |
| Years | 3.83E+19 |
| Decades | 3.83E+18 |
| Centuries | 3.83E+17 |

Table VII displays the result of the Brute Force Attack Analysis performed in a word with a 10-letter count. It identifies the modified algorithm's level of security as it shows the estimated time to crack the cipher text successfully. The result shows that the estimated number of centuries that it will take for an attacker to crack the ciphertext is 3.83376E+17. A similar brute force attack analysis based on the study of [18] on Playfair cipher uses a 10-character key. The result shows that it takes 432400402.6 century to break the cipher, which signifies that there is much time to break the security.

**Table VIII(a).** Result of the Frequency Analysis of the Beaufort Cipher Expansion Technique

| Beaufort Cipher Expansion Technique | | | | |
|---|---|---|---|---|
| Plaintext | Ciphertext | Unique | Frequency | Percentage |
| N | 1 | 0 | 2 | 13.33333 |
| E | 3 | 1 | 3 | 20 |
| T | 2 | 2 | 2 | 13.33333 |
| W | 8 | 3 | 2 | 13.33333 |
| O | 7 | 4 | 0 | 0 |
| R | 5 | 5 | 1 | 6.666667 |
| K | 0 | 6 | 1 | 6.666667 |
| | 3 | 7 | 1 | 6.666667 |
| | 9 | 8 | 1 | 6.666667 |
| | 1 | 9 | 2 | 13.33333 |
| | 6 | 10 | 0 | 0 |
| | 2 | | | 100 |
| | 9 | | | |
| | 0 | | | |
| | 1 | | | |

**Table VIII(b).** Result of the Frequency Analysis of the Enhanced Beaufort Cipher Expansion Technique

| Enhanced Beaufort Cipher Expansion Technique | | | |
|---|---|---|---|
| Ciphertext | Unique | Frequency | Percentage |
| ī | ī | 1 | 14.2857143 |
| © | © | 1 | 14.2857143 |
| ő | ő | 1 | 14.2857143 |
| m | m | 1 | 14.2857143 |
| C | C | 1 | 14.2857143 |
| Ļ | Ļ | 1 | 14.2857143 |
| ! | ! | 1 | 14.2857143 |

Table VIII presents the comparison of the results of frequency analysis performed on the Original Beaufort Cipher Expansion Technique and the Enhanced Beaufort Cipher Expansion Technique. The original version obtained a ciphertext that contains frequently occurring values such as 1,0,2,3 and 9, which is prone to frequency analysis attacks since there are dominant values that can be found from the letters in the dictionary. On the other hand, the enhanced version obtained a ciphertext that has a fair distribution of characters which masks it from the attacker.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 10, Issue 9, September 2023

**Table IX:** Avalanche Effect Comparison

| Title | Avalanche Effect (%) |
|---|---|
| **Securing Text Messages using the Beaufort-Vigenere Hybrid Method (2019)** | 46% |
| **Double Layered Text Encryption using Beaufort and Hill Cipher Techniques (2020)** | 33.68% |
| **Proposed Enhancement** | 51.66% |

Table IX presents the avalanche effect comparison of the latest enhancements of the Beaufort Cipher, including the avalanche effect result of the Enhanced Beaufort Cipher Expansion Technique. The result shows that the enhancement obtained the highest avalanche effect of 51.66%, which is above the desired value of 50%, signifying that it is impossible to identify which bits of the original message change once a random bit has been changed.

## VI. CONCLUSION

Based on the results collected, the enhanced expansion technique was tested against the Kasiski attack using bigram and trigram frequency analysis. The findings indicate that the generated ciphertext using the enhanced expansion technique did not reveal any discernible bigram or trigram patterns, rendering it impracticable for the Kasiski attack to be executed. Therefore, it can be inferred that the enhanced expansion technique is a robust encryption method that can withstand attacks based on pattern recognition.

Moreover, findings on frequency analysis revealed that the original Beaufort Cipher Expansion Technique produced a ciphertext vulnerable to frequency analysis attacks due to its frequently occurring values. In contrast, the enhanced Beaufort Cipher Expansion Technique distributed characters evenly, making it more secure and difficult for attackers to deduce meaningful information from the ciphertext through frequency analysis. Therefore, the enhanced Beaufort Cipher Expansion Technique offers improved protection against such attacks.

Additionally, based on the Analysis of Brute Force Attack, results revealed that the estimated time to crack a 10-letter ciphertext using the Beaufort Cipher is approximately 3.83376E+17 centuries. This suggests that the Beaufort Cipher provides a high level of security against brute force attacks. The long-estimated time to crack indicates that it would be impractical for an attacker to decrypt the ciphertext using brute force alone, making the Beaufort Cipher a robust encryption method for protecting sensitive information.

Lastly, the latest enhancements made to the Beaufort Cipher Expansion Technique have successfully achieved a high avalanche effect of 51.66%, surpassing the desired value of 50%. This result indicates that it is extremely difficult to determine which bits of the original message have changed when a random bit is altered. These findings demonstrate the effectiveness of the enhancements in enhancing the security.

## REFERENCES

[1] "The Importance of Data Security in a Remote World | University of Nevada, Reno," 2021. https://onlinedegrees.unr.edu/blog/importance-of-data-security/ (accessed Jan. 02, 2023).

[2] F. Qazi, F. H. Khan, K. N. Kiani, S. Ahmed, and S. A. Khan, "Enhancing the Security of Communication Using Encryption Algorithm Based on ASCII Values of Data," *International Journal of Security and Its Applications*, vol. 11, no. 2, pp. 59–68, Feb. 2017, doi: 10.14257/ijsia.2017.11.2.06.

[3] J. C. T. Arroyo, A. M. Sison, R. P. Medina, and A. J. P. Delima, "A Cryptographic Test ofRandomness, Entropy,and Brute Force Attack onthe Modified Playfair Algorithm with the Novel Dynamic Matrix," *International Journal of Emerging Technology and Advanced Engineering*, vol. 12, no. 6, pp. 73–83, 2022, doi: 10.46338/ijetae0622_11.

[4] "What is Data Security? Data Security Definition and Overview | IBM," 2021. https://www.ibm.com/topics/data-security (accessed Jan. 02, 2023).

[5] E. Sugiarto *et al.*, "Securing Text Messages using the Beaufort-Vigenere Hybrid Method," in *Journal of Physics: Conference Series*, Institute of Physics Publishing, Jul. 2020. doi: 10.1088/1742-6596/1577/1/012032.

[6] D. G. Pai and Y. Pai, "Analysis of the Beaufort Cipher Expansion Technique and Its Usage in Providing Data Security in Cloud," 2022, pp. 49–58. doi: 10.1007/978-981-16-4284-5_5.

[7] E. Ndruru and T. Zebua, "Pembangkitan Kunci Beaufort Cipher Dengan Teknik Blum-blum Shub pada Pengamanan Citra Digital," *Bulletin of Information Technology (BIT)*, vol. 3, no. 2, pp. 149–154, 2022, doi: 10.47065/bit.v3i1.302.

[8] J. P. G. Perez *et al.*, "A Modified Key Generation Scheme of Vigenère Cipher Algorithm using Pseudo-Random Number and Alphabet Extension," in *2021 7th International Conference on Computer and Communications, ICCC 2021*, Institute of Electrical and Electronics Engineers Inc., 2021, pp. 565–569. doi: 10.1109/ICCC54389.2021.9674565.

[9] R. N. Sari and R. S. Hayati, "Beaufort Cipher Algorithm Analysis Based on the Power Lock-Blum Blum Shub in Securing Data," 2018.

[10] T. Kaeding, "Quagmire ciphers and group theory: What is a Beaufort cipher?," 2022.

[11] M. Risnasari, M. A. Effindi, P. Dellia, L. Cahyani, N. Aini, and N. Aini, "Computer Based Test Using the Fisher-Yates Shuffle and Smith Waterman Algorithm," *KnE Social Sciences*, pp. 353–360, Jun. 2021, doi: 10.18502/kss.v5i6.9224.

[12] M. Yadav, P. R. Gautam, V. Shokeen, and P. K. Singhal, "Modern Fisher–Yates Shuffling Based Random Interleaver Design for SCFDMA-IDMA Systems," *Wirel Pers Commun*, vol. 97, no. 1, pp. 63–73, Nov. 2017, doi: 10.1007/s11277-017-4492-9.

[13] F. Panca Juniawan, H. Arie Pradana, Laurentinus, and D. Yuny Sylfania, "Performance comparison of linear congruent method and fisher-yates shuffle for data randomization," in *Journal of Physics: Conference Series*, Institute of Physics

Publishing, Apr. 2019. doi: 10.1088/1742-6596/1196/1/012035.

[14] B. Al-Shargabi, M. Abbas, and F. Al-Husainy, "A New DNA Based Encryption Algorithm for Internet of Things," 2021.

[15] F. Nurahmadi and S. D. Siregar, "HYBRID CRYPTOSYSTEM USING ELGAMAL ALGORITHM AND BEAUFORT CIPHER ALGORITHM FOR DATA SECURITY," *J Theor Appl Inf Technol*, vol. 15, no. 7, 2022, [Online]. Available: www.jatit.org

[16] M. Fadlan, Suprianto, Muhammad, and Y. Amaliah, "Double layered text encryption using beaufort and hill cipher techniques," in *2020 5th International Conference on Informatics and Computing, ICIC 2020*, Institute of Electrical and Electronics Engineers Inc., Nov. 2020. doi: 10.1109/ICIC50835.2020.9288538.

[17] A. L. Hananto, A. Solehudin, A. Susilo, Y. Irawan, and B. Priyatna, "Analyzing the Kasiski Method Against Vigenere Cipher," *International Journal of Computer Techniques*, vol. 6, 2019, [Online]. Available: http://www.ijctjournal.org

[18] R. M. Marzan and A. M. Sison, "An enhanced key security of playfair cipher algorithm," in *ACM International Conference Proceeding Series*, Association for Computing Machinery, 2019, pp. 457–461. doi: 10.1145/3316615.3316689.

[19] K. Muthavhine, M. Sumbwanyambe, International Conference on Information and Communications Technology 1 2018.03.06-07 Yogyakarta, and ICOIACT 1 2018.03.06-07 Yogyakarta, *An Analysis And A Comparative Study Of Cryptographic Algorithms Used On The Internet Of Things (IoT) Based On Avalanche Effect*. 2018.

[20] M. Levinskas and A. Mihalkovich, "Avalanche effect and bit independence criterion of perfectly secure Shannon cipher based on matrix power," *Mathematical Models in Engineering*, vol. 7, no. 3, pp. 50–53, Sep. 2021, doi: 10.21595/mme.2021.22234.