Analysis of the security level of modified CBC algorithm cryptography using avalanche effect

N R D P Astuti, I Arfiani and E Aribowo
Informatics Department, Faculty of Industrial Technology, Universitas Ahmad Dahlan, Prof Soepomo Street, Janturan, Umbulharjo, Yogyakarta, Indonesia
Email: rochmahdyah@tif.uad.ac.id, ika.arfiani@tif.uad.ac.id, ekoab@tif.uad.ac.id

Abstract. There have been many modifications of cryptographic algorithms aimed at increasing the security of the algorithm. One cryptographic algorithm that has been modified is CBC (Cipher Block Chaining) cryptography. CBC is a block-based modern cryptographic algorithm. The disadvantages that exist in CBC is the encryption process in each block plaintexts using the same key, resulting in if the cryptanalyst finds the key that is used it will be easy to decrypt the ciphertext. Modifications made to CBC aimed at increasing security is by combining the Vigenere algorithm in determining the key and block transposition on the final reading of the encryption process. Parameters for assessing the algorithm are good or not by looking at the value of avalanche effect. A cryptographic algorithm will be categorized as good if the value of avalanche effect ranges between 45% -60% and bernilia is very good if the value of avalanche effect is 50%. The results of this study indicate that the modified CBC cryptographic algorithm resulting from the encryption process of several plaintexts has Avalanche effect values in the range above 50% and below 60%, which means that the modified CBC algorithm is of good value.

Keywords: Modified CBC, modified performance algorithm, Avalanche effect.

1. Introduction
Cryptography is a mathematical technique related to information security aspects such as confidentiality, data integrity, user authentication, and data authenticity [1]. There have been many modifications made in cryptography aimed at increasing the security power of the algorithm. One of the cryptographic algorithms that have been modified is Cipher Block Chaining (CBC). In CBC mode, each block of plaintext is XORed with the previous ciphertext block before being encrypted. This way, each ciphertext block depends on all plaintext blocks processed up to that point. To make each message unique, the initialization vector must be used in the first block [2]. The CBC encryption process uses the same key on each block. This results in vulnerability, by finding the key and initial vector used, the kripanalis will very easily decrypt the encrypted ciphertext. To improve the security of the CBC, modification of the encryption process and the encryption result reading process is carried out. Modifications made to the CBC algorithm are by combining the Vigenere algorithm for determining keys and block transposition on the reading of the encryption process [3].

To determine the performance of the modified CBC algorithm, it is necessary to test the security level of the algorithm. Measurement of security level will be measured by the analysis of the avalanche effect. According to Webster, A. F.; Tavares, Stafford E. (1985), that a very well-known
The parameter used to analyze security (randomness) of encryption algorithms is with avalanche effect [4]. The test of avalanche effect measurement is done by changing the number of encrypted text bits (cipher) because a one-bit change in the key text or plaintext will produce significant changes to the ciphertext. The avalanche test is considered best if half of the ciphertext bits are changed according to the Strict Avalanche Criterion (SAC) [5].

Analysis with the value of the avalanche effect will prove the performance of the modified CBC algorithm. This paper will show how to measure the level of security of the modified CBC algorithm with the value of avalanche effect, the measurement is done by encrypting several plaintext forms and calculating the value of the avalanche effect from the encrypted ciphertext.

2. Method

2.1. CBC (Cipher Block Chaining)

Cipher Block Chaining Algorithm (CBC) is a cryptography method based on block. The series of plaintext bits are divided into bits of the same length, for example 64 bits. The same plaintext block will be encrypted into the same ciphertext block when the same key is used. This operation is applied to modern cryptography algorithms that are already operating at the bit level (0 or 1) or groups/block bits and not characters.

Suppose that block plaintext \( P \) which is \( m \)-bit in size is expressed as a vector \( P = (p_1, p_2, \ldots, p_m) \) which in this case \( p_i = 0 \) or \( 1 \) for \( i = 1, 2, \ldots, m \), and block ciphertext \( C \) is \( C = (c_1, c_2, \ldots, c_m) \) which in this case \( c_i = 0 \) or \( 1 \) for \( i = 1, 2, \ldots, m \). If the plaintext is divided into \( n \) blocks, the plaintext blocks are expressed as \( (P_1, P_2, \ldots, P_n) \). For each plaintext \( P_i \) block, the constituent bits can be expressed as \( P_i = (p_{i1}, p_{i2}, \ldots, p_{im}) \) vectors. Encryption and decryption with key \( K \) are expressed in succession with the equation.

\[
E_K (P) = C \tag{1}
\]

for decryption, and

\[
D_K (C) = P \tag{2}
\]

The \( E \) function must be a one-to-one correspondent function, so

\[
E^{-1} = D \tag{3}
\]

The CBC mode scheme is shown in Figure 1 and Figure 2.

![Figure 1](image-url)
Figure 2. Scheme of the CBC method decryption process (Bruce 2013)

Mathematically, encryption with CBC mode is declared as
\[ C_i = E_K (P_i \oplus C_{i-1}) \] (4)
and decryption as
\[ P_i = D_K (C_i \oplus C_{i-1}) \] (5)

For the first plaintext block encryption process, use \( C_0 \) as the initial vector (initialization vector or IV). Vector Initialization (IV) does not need to be kept secret. Initialization Vector (IV) which is a random data as the first block. Initialization Vector (IV) has no meaning, it is only used to create each unique ciphertext block. Identical plaintext blocks encrypted into ciphertext blocks differ only if the previous plaintext block is different. If the previous plaintext block is the same, it is possible that the ciphertext is the same, to prevent this, Initialization Vector (IV) is used.

2.2. Modified CBC
The result of improvisation in the modified CBC method is that there are two encryption processes in the modified CBC technique. The first modification encryption \((E1)\) is in the key placement process. The key to the CBC method which is initially fixed in value for each block, by combining the Vigenere cipher method the key will always change following the key length in each block. Changing each key on each block will make it difficult for the cryptanalysis to estimate the connectedness of each plaintext block which ultimately leads to the entire message.

The second modification encryption \((E2)\) is a continuation of the first process, the modification is found in the first encryption ciphertext reading process \((E1)\) done by the block transposition method, this modification is intended to reduce the weakness of CBC, namely the ciphertext reading using the monotonous block concept so that it is easily kripanalis to find out the message sent, by changing the reading position of the encryption result by using block transposition, the kripanalis will find it difficult to estimate.

The modified CBC method scheme for the encryption process can be seen in Figure 3. Description of the modified CBC scheme as follows, on encryption 1 \((E1)\) will be used Vigenere cipher. . The first plaintext block will be XORed with the value IV (Initialization Vector), the XOR result will be encrypted using the key from the vinegere cipher and generate an intermediate ciphertext. The encrypted ciphertext will be the initial vector on the next plaintext block. And the encryption process will end until the last plaintext block.
Encryption process 2 ($E2$), the final ciphertext reading is done in Block Transposition. The intermediate output from $C_i$ to $C_n$ will be read in the Block Transposition or transposition column, the output of the process is the final Ciphertext ($C$) which will be converted into hexadecimal. In CBC modification with block transposition the ciphertext reading process will be sequential according to the column. Whereas for the modified CBC decryption process scheme is shown in Figure 4.

![Figure 3: The modified CBC algorithm scheme for the encryption process (Astuti 2012)](image)

**Figure 3.** The modified CBC algorithm scheme for the encryption process (Astuti 2012)

The decryption process is the opposite of the encryption process, Decryption Process 1 ($D1$), is the process of reading ciphertext done in Block Transposition. The ciphertext will be made per block according to the block key from $C_i$ to $C_n$. Result $D1$ is an intermediate plaintext. In decryption 2 ($D2$) intermediate plaintext, Vigenere cipher will be used. The current ciphertext block is XORed with the plaintext block that was decrypted before, the result will be XORed with the key. Determination of key index $K$ in the modified CBC technique, it is stated successively by the equation:

$$K_i = K_{[i \mod t]}$$

the $i$ key is obtained from the value of $i$ modulus with $t$, where $t$ is the key length and $i$ is the index with values from 1 to $n$. For the second plaintext and so on the key index becomes $K_s$ where $s$ is the plaintext index with a value of 1 to $n$, the $K_s$ equation becomes

![Figure 4: Schematic of the modified CBC algorithm decryption process. (Astuti 2012)](image)

**Figure 4.** Schematic of the modified CBC algorithm decryption process. (Astuti 2012)


\[ K_s = K_{[i+1 \mod t]} \]  

while for the \( n \)-th plaintext, key \( K_j \) determination using the equation

\[ K_j = K_{[n \cdot l \mod t]} \]

\( j \) is the key index with values from 1 to \( t \), the key index will be \( t \) if the modulus is 0. So that the encryption and decryption equation of the CBC modification are respectively

\[
\begin{align*}
C_i &= E_{K_i}(P_i \oplus C_{i-1}) \\
C_{i+1} &= E_{K_s}(P_{i+1} \oplus C_{i-1}) \\
&\quad \ldots \\
C_n &= E_{K_j}(P_n \oplus C_{i-1})
\end{align*}
\]

and decryption is

\[
\begin{align*}
P_i &= D_{K_i}(C_i \oplus C_{i-1}) \\
P_{i+1} &= D_{K_s}(C_{i+1} \oplus C_{i-1}) \\
&\quad \ldots \\
P_n &= D_{K_j}(C_n \oplus C_{i-1})
\end{align*}
\]

2.3. Avalanche Effect

One characteristic to determine whether or not a cryptographic algorithm is by looking at the avalanche effect. Changes in one bit from plaintext or one key bit must produce changes in many bits of the password text. This property is known as the Avalanche Effect [6]. The key will produce changes to many bits in the ciphertext. An avalanche effect is said to be good if the changes in the bits produced range from 45-60\% (50\% is a very good result). This is because these changes mean making a difference that is quite difficult for cryptanalysts to carry out attacks. The value of the avalanche effect is formulated with [7]:

\[
\text{Avalanche effect (AE)} = \frac{\sum \text{bit\_change}}{\sum \text{total\_bit}} \times 100 \%
\]

2.4. Research Flow

The process of this research is planned with the following lines:

1) The course of the study begins with reviewing the theory of the process of measuring avalanche effects from existing literature, books, and journals.

2) The results of the theoretical study are made in the business process in the form of a flowchart avalanche effect analysis process.

3) Development of applications as tools for measurement using specific program languages.

4) Testing CBC algorithm performance Modified with plaintext with extension .txt and .doc.

5) The results of the application are data from the measurement of plaintext and ciphertext.

6) Measurement data are analyzed to produce conclusions on the performance of the algorithm.

The research flow is shown in Figure 5.
3. Results and Discussion

One characteristic to determine whether or not a cryptographic algorithm is by looking at the avalanche effect. Changing bits in plaintext and key will cause significant changes to the resulting ciphertext [8]. Testing the modified CBC cryptographic algorithm performance with the value of the Avalanche effect is done by giving the same plaintext using capital letters and plaintext using lowercase letters. The key is given the same. The results of measuring the value of avalanche effect can be seen in table 1 and table 2.

**Plaintext:** "Ahmad Dahlan University informatics engineering"

**Key:** uad produces 8 bits in hex.

| Number of Ciphertext Key bits | The original plaintext and in hex values | CipherText | AE(%) | Analysis of AE |
|-------------------------------|----------------------------------------|------------|-------|----------------|
| 8                             | “informatics” = 696E666F726D6174696373 | 32ACAF2B51AEFAB1D048CA | 50% | very good |
| 8                             | “informatics engineering” = 696E666F726D617469637320656E67 | 32A02ACAC0AF2B02BD1A99BEFA D74B1E3F904BB58CA80A | 56% | good |
| 8                             | “informatics engineering ahmad” = 696E666F726D617469637320656E67 | 32A02AFB2B02BF82B02BF846A66 DEEDFA752AC78FEB54BB5B32A02AF | 52% | good |
| 8                             | “informatics engineering ahmad dahlan” = 696E666F726D617469637320656E67 | 32A02AE1656057F42CAC0AF8E5A 35336F42EFA475295F8F1FD6AF412 ED6D5C950157F0 | 51% | good |
| 8                             | “informatics engineering ahmad dahlan university” = 696E666F726D617469637320656E67 | 32B0FC184000CA3F0610032B0FC18 | 56% | good |
Table 2. Results of testing plaintext using capital letters.

| Number of Chiphertexts Key bits | The original plaintext and in hex values | Chiphertext | AE(%) | Analysis of AE |
|---------------------------------|-----------------------------------------|-------------|-------|----------------|
| 8                               | “INFORMATICS” = 494E464F524D4154494353 | 32995CAE8DEF96341065 | 54%   | good |
| 8                               | “INFORMATICS ENGINEERING” = 494E464F524D415449435320454E4 | 32A822CAE08F2B023D1A9BBEFA | 51%   | good |
| 8                               | “INFORMATICS ENGINEERING AHMAD” = 494E464F524D415449435320454E4 | 32A822732B823732B023F346A6ED | 52%   | good |
| 8                               | “INFORMATICS ENGINEERING AHMAD DAHLAN” = 494E464F524D415449435320454E4 | 32A822749657046E13CAC08FCA7 | 53%   | good |
| 8                               | “INFORMATICS ENGINEERING AHMAD DAHLAN UNIVERSITY” = 494E464F524D415449435320454E4 | 32A8227490F8CAE08DC263E72B0 | 52%   | good |

From the results of testing two different types of paints, the results of the avalanche effect test for both plaintexts are between 50% - 56%, which means that the modified cryptographic algorithm has proven safety because it is in a good category from the avalanche effect.

4. Conclusion
Based on the results of this research, it can be concluded as 1) The modified CBC algorithm in terms of security is classified as good, so it can be used to improve the security of data from irresponsible people; 2) Modified CBC algorithm is said to be good according to the test results with the value of avalanche effect which is in the range of 50% is very good and a maximum of 56% in the good category; 3) The test uses the same key and plaintext whose contents are the same as letters, namely capital and lowercase; and 4) The testing process by breaking sentences into words and combining each word from the existing plaintext.

5. Sustainability of Research
Some suggestions that can be submitted and can be advanced research are: a) testing with other variables such as the complexity of the modification algorithm, and b) testing is done on data types other than text.

References
[1] Menezes, A.J., Oorschot, P.C. van & Vanstone, S.A., 1996. *Handbook of Applied Cryptography* 1st ed., New York: CRC Press Inc.
[2] William F. Ehrsam, Carl H. W. Meyer, John L. Smith, Walter L. Tuchman, "Message verification and transmission error detection by block chaining", US Patent 4074066, 1976
[3] Astuti, N.R.D.P., 2012. *Modifikasi Metode Kriptografi Modern Cipher Block Chaining (CBC) Dengan Algoritma Vigenere Cipher Dan Block Transposition*. Universitas Diponegoro,
Semarang.

[4] Webster, A. F.; Tavares, Stafford E. (1985). "On the design of S-boxes". Advances in Cryptology - Crypto '85. Lecture Notes in Computer Science. 218. New York, NY,: Springer-Verlag New York, Inc. pp. 523–534. ISBN 0-387-16463-4.

[5] Ibrahim, M.S., Security Analysis of Secure Force Algorithm for Wireless Sensor Networks., pp.1–7

[6] Ramanujam, S. & Karuppiah, M., 2011. Designing an algorithm with high Avalanche Effect., 11(1), pp.106–111

[7] Sidorenko, A. V & Mulyarchik, K.S., The Analysis Of The Avalanche Effect In Discrete Chaotic Maps For Block Ciphers., pp.32–35.

[8] Bruce, S., 2013. Applied cryptography. Journal of Chemical Information and Modeling, 53, pp.1689–1699

Acknowledgments
This research was supported by KEMENRISTEKDIKTI and LPMP of Ahmad Dahlan University in the research scheme of the beginner lecturer research number: PDP-094 / SKPP / III / 2018.