Merging of Vigenére Cipher with XTEA Block Cipher to Encryption Digital Documents

Fathir Maruf
Universitas Islam Indonesia
Jln. Kaliurang km. 14.5,
Yogyakarta, Indonesia

Imam Riadi
Ahmad Dahlan University
Jln. Prof. Dr. Soepomo,
Yogyakarta, Indonesia

Yudi Prayudi
Universitas Islam Indonesia
Jln. Kaliurang. km 14.5,
Yogyakarta, Indonesia

ABSTRACT
Security and confidentiality of documents or information has become a very important concern, in this modern era of computing speed increases dramatically, certainly considered threatening for some algorithms that are used to secure documents or information, it spawned an option to increase the security of documents by combining two cryptographic algorithms are Vigenére cipher with XTEA. Selection Vigenére cipher because it is not so vulnerable to solving method code is called frequency analysis, but some cryptanalyst has found security flaws of this algorithm, for it Vigenére cipher in this research carried out modifications to operations of mathematics, the results of these modifications will be combined with the algorithm-based XTEA block cipher, because his strength has been proven to secure the document (text). Based on the results of research conducted, the merger of the two algorithms are (VixTEA) can improve the security of ciphertext, it is measured by various indicators, namely, a visual comparison of encryption (frequency analysis), entropy value analysis, and analysis of bruteforce attacks. The results also showed that the VixTEA concept does not change the performance of the algorithm and the integrity of the digital documents can secured.

General Terms
Security.

Keywords
Vigenére cipher, XTEA, Block cipher, VixTEA, Digital documents.

1. INTRODUCTION
For an organization or individual, the security of a document or information has to be something very important, delivery and acceptance in a network, either a local network or the Internet would lead to a risk of such documents would be threatened, both of theft and unauthorized access of unauthorized persons can be harm of the documents, the losses in question could be lost and the leaking of confidential information and material losses. The development of information technology has made storage and transmission of digital documents such as images, documents, videos, and others to be more easily and efficiently, Issues arising from the ease it is the presence of security gaps for people who are not responsible for theft of data, whether stored in a hard drive or transmitted [10].

Related to security and confidentiality of documents or information gives a choice of whether any individual or organization will secure document that they have or do not, of course, a risk that is received from each of these options will be different, techniques and activities theft of documents is often the case especially in the Internet network, these activities make everyone should secure documents or information to be stored or transmitted. For various reasons the security and confidentiality of information is needed in data communications, there are various ways to ensure the security and confidentiality in data communications, such as the art of scrambling data or cryptography, the science of cryptography has a very interesting history, this science has been used since 4000 years ago, introduced by the Egyptians to send a message to the military forces in the battlefield. The main purpose of encryption is to hide the data from unauthorized parties from viewing, altering the data [14], Cryptography concepts contained in the terms of encryption or scrambling the data, which aims to secure of digital documents [5].

According to [10] combining the two algorithms can improve security on a particular digital document security on the image, to improve the security of which is owned by Vigenére cipher algorithm in this study will be modified by adding mathematical functions on operations, ciphertext produced by Vigenére cipher algorithm that has been modified to be secured again by using XTEA 32 rounds, after the double encryption using two algorithms, can improve the security of the ciphertext, the concept of merging the proposed algorithm (VixTEA) will have 3 main security Vigenére key, integer Z, and XTEA key.

2. LITERATURE REVIEW
Cryptography is composed of two processes – encryption and decryption. Encryption is the process of converting the data to be communicated or plaintext into a form which is readable or understandable only by the authorized party, known as cipher text. On the other hand, the process of converting cipher text into plaintext is known as decryption. The objective of cryptography is to fulfill four basic objectives- authentication, privacy/confidentiality, integrity and non-repudiation [12]. Another important term in this context is cryptanalysis. Cryptanalysis is the process of deciphering encrypted communication without the knowledge of the key.

Vigenére cipher is a type of classical cryptography, including the cipher alphabet-compound (polyalpabetic cipher substitution) [1], while XTEA included in the cryptographic algorithm based on block ciphers, and is a derivative of the TEA, XTEA have a principle that stands out is small, secure, simple and fast, the reason that makes this algorithm is considered safe because implementation does not use a function of the s-box and permutation [8], so it is considered safe from frequency analysis, XTEA which uses 27 rounds have been solved, then the implementation of XTEA using 27 rounds is not recommended for is used because it has discovered a security hole [9].

2.1 Vigenére cipher
In a study conducted by [1] states that the classical algorithm Vigenére cipher included within the compound alphabetical (polyalphabetic cipher substitution) issued by a diplomat as well kriptologis coming from France, Blaise de Vigenère in the 16th century (1586), researchers has implemented a

concept inspired by nature to classical cryptography and cryptanalysis claim success, using genetic algorithms can be done to cryptanalysis simple substitution cipher [13], Kasiski is a method used to find weaknesses found in Vigenére cipher [15]. This method takes advantage of that ciphertext encrypted cipher Vigenére there is repetition of characters, encryption and decryption that has been solved by a method Kasiki based on the following formula [12]:

Encryption:

Ci = (Pi + Ki) mod 26 - (Equation 1) (1)

Decryption:

Pi = (Ci – Ki) mod 26 - (Equation 2) (2)

Where C = C0….Cn is the Ciphertext, P = P0….Pn is the Plaintext and K = K0….Kn is the key.

Example: encryption plaintext "CRYPTOGRAPHY" with key "KLASIK".

Plaintext	: C R Y P T O G R A P H Y
Key	: K L A S I K
Ciphertext	: L C A H B Y Q C A H P I

In Vigenére cipher each letter in the plaintext has some letters corresponding ciphertext, making cryptanalysis can guess the frequency distribution and key [13], Formula encryption and decryption presented above is the basic formula of the algorithm Vigenére cipher that uses modulo 26 (Total alphabet), but in this study will make modifications to the formula by adding a parameter Z and use the ASCII code 256 was adopted from the source code based on polyalphabetic cipher algorithm:

Encryption

Ci = (Pi + Ki – Z) mod 256 – (Equation 1) (3)

Decryption

Pi = (Ci – Ki – Z) mod 256 – (Equation 2) (4)

Example: encryption plaintext "CRYPTOGRAPHY" with key "KLASIK".

Plaintext	: C R Y P T O G R A P H Y
Key	: K L A S I K
Z	: 29
Ciphertext	: V f n f k g ` l \ l [m

The encryption process aimed at securing a document, by tampering with the document that is not known by others, and the decryption process aims to restore documents that have been damaged [15]. Modification results show that, the range of characters be broadly in line with the ASCII code, security not only in the key, also located at integer value Z, flowchart encryption / decryption Vigenére cipher that has been modified can be seen in Figure 1 below:

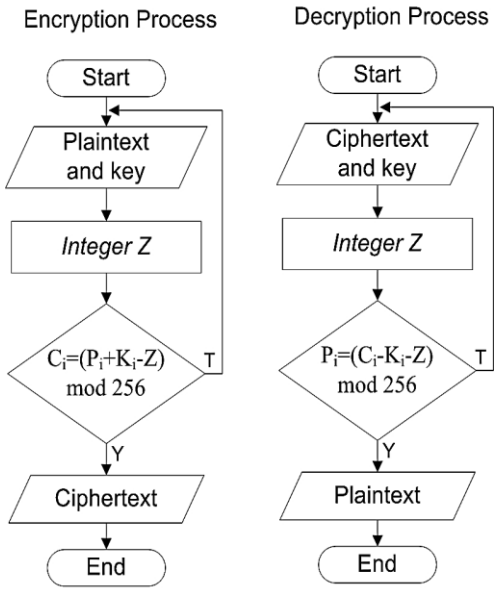


Fig 1: Encryption and decryption Process of Vigenére cipher

Description:

Pi = Plaintext

Ci = Ciphertext

K = Key

Z = Positive integer value

Mod 256 = ASCII code number that is used

Based on the flow of encryption in Figure 1 describes the stages in changing a document (plaintext) into a ciphertext which starts from the input plaintext and key, and then determine the value of Z is given to sub-keys, then apply the formula Ci= (Pi+Ki-Z) mod 256, where the results obtained from implement of the formula such is the ciphertext. While the decryption process performed by the ciphertext input, the initial key, and the value of Z, the next step is to restore the ciphertext into its original form, using a decryption formula Pi= (Ci-Ki-Z) mod 256.

2.2 Extended Tiny Encryption Algorithm (XTEA)

XTEA is a symmetric block cipher algorithm that is designed to correct deficiencies found in TEA, this algorithm operates in a block size of 64 bits and a key length of 128 bits [16], in implementation XTEA will divide the plaintext into two blocks of plaintext early each with a value of 32 bits, block z and block y, while the key-value 128 bits would be divided into 4 blocks sub key K[0] = 32 bits, K[1] = 32 bits, K[2] = 32 bits and K[3] = 32 bit [11], XTEA has a very simple key schedule: the 128-bit master key K is split into four 32-bit blocks K0, K1, K2, K3. Then, for r = 1,…, 64, the round keys Kr are derived from the following equation the rules operate on the terms odd rounds and even rounds, as described in the following formula [9]:

$$K_r = \begin{cases} K_{\left(\frac{r-1}{2}\cdot\delta \gg 11\right)\&3} & \text{if } r \text{ is odd} \\ K_{\left(\frac{r}{2}\cdot\delta \gg 11\right)\&3} & \text{if } r \text{ is even} \end{cases} \quad (5)$$

Feistel network belongs to XTEA is almost the same as the Feistel network owned TEA, according to [6] which differentiates between XTEA with TEA was Feistel and key scheduling function is used. use the odd round of K [sum & 3], while the even-numbered rounds used K [sum >> 11 & 3], as shown in the following Figure 2 [4]:

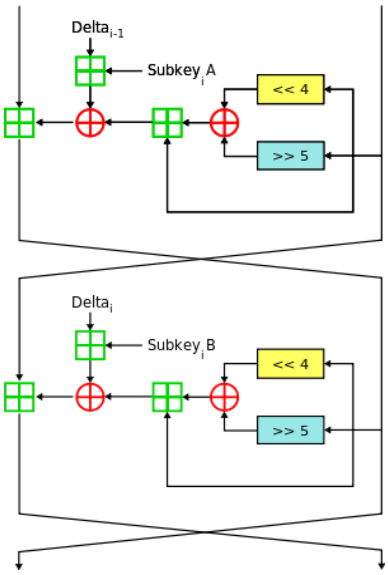


Fig 2: One round Feistel network encryption in XTEA

Explanation of the flowchart in Figure 2 above is shown in Table 1 below [11]:

Table 1. Notation of XTEA

Symbol	Meaning
⊞	Addition modulo 2^{32}
⊕	Exclusive-OR
≪	Left shift
≫	Right shift

In the implementation of XTEA using delta value (√5 - 1) 232 with the constant value of delta is the change to the value Hexadecimal 9E3779B9, the following is a mathematical operation on the encryption process XTEA [12]:

Round 0:

y+= (z << 4 ^ z >> 5) + z ^ sum + k[sum & 3]; (6)

sum += delta;

Round I:

z+= (y << 4 ^ y >> 5) + y ^ sum + k[sum >> 11 & 3]; (7)

Measures used in decrypting the ciphertext using the same steps with the encryption process on the provisions of 32 rounds or 64 rounds, using the following operations:

Round 0:

z-= (y << 4 ^ y >> 5) + y ^ sum + k[sum >> 11 & 3]; (8)

sum -= delta;

Round I:

y-= (z << 4 ^ z >> 5) + z ^ sum + k[sum & 3]; (9)

Recommendations for the use of round XTEA is 32 cycles or 64 rounds, because the cryptanalyst has found security flaws XTEA use with round bottom 32 cycles, We presented related key differential attacks on XTEA and GOST. In the case of XTEA, we use 121 structures to attack 27 rounds of XTEA with an expected success rate of 96.9%; this attack requires about 220.5 chosen-plaintexts and 2115.15 27-round XTEA encryptions [9].

3. METHODOLOGY

Importance in securing digital documents is when the document that is personal or confidential, person or institution does not want the document is known by others or unauthorized parties, both in storage and transmission can provide security at the document with encryption method. A general description of the concept of the double encryption (VixTEA) on documents in the real world scenario can be seen in the use of encryption in Figure 3:

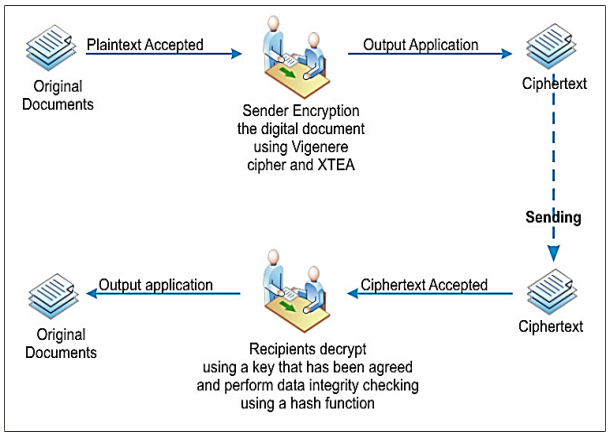


Fig 3: Scenario double encryption (VixTEA)

In Figure 3 above is given an example, a user wants to send a digital document that has important information to his friend through a public network that is certainly vulnerable to interception or access by others. To maintain the confidentiality and security of documents sent, it is necessary to double encryption on the document so that a digital document that is sent is not recognized as an important information but a ciphertext that has no meaning, The document will not be recognized anymore, because it was done randomization codes that include odd contained in ASCII code 256 characters and of course the information contained in the digital documents that are sent will be safe from being accessed by unauthorized parties. The design of double encryption using Vigenére cipher algorithms and XTEA to be constructed in this research are generally described in following Figure 4:

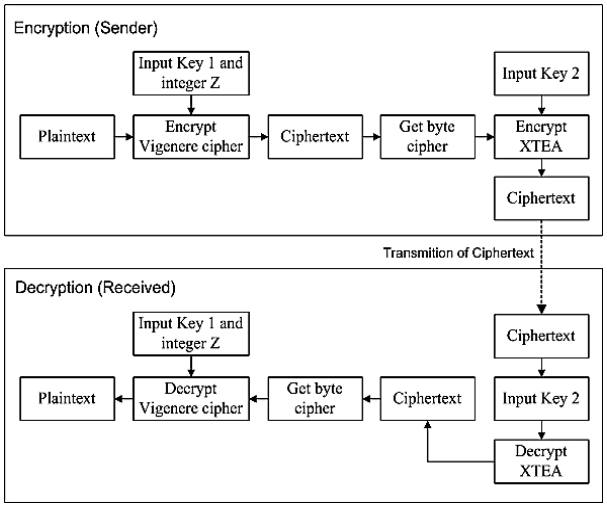


Fig 4: Design encryption and decryption VixTEA

The design of the above will be implemented in an application encryption / decryption, or in a new concept named VixTEA and specifically of design scheme encryption and decryption VixTEA will be described in Figure 5 and 6 following:

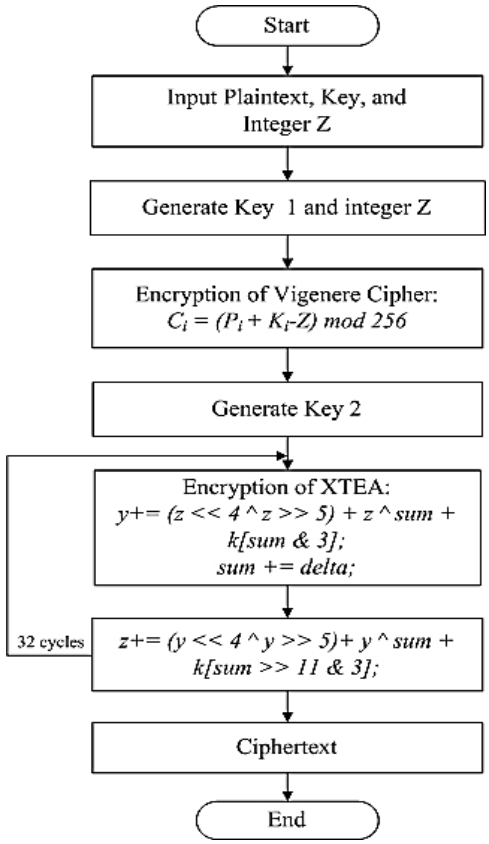


Fig 5: Design of the encryption scheme VixTEA

Explanation of the encryption process in Figure 5 above:

1. Input plaintext (documents), Key 1 (Key Vigenére) of length n <256, key 2 (Key XTEA) with a length of 16 characters, or 128 bits, and the value of Z.
2. Generate key 1 dan value of Z.
3. Encryption Vigenére ciher using equation Ci =(Pi+Ki–Z) mod 256.
4. Generate key 2.
5. Before performing encryption with XTEA, first dividing the ciphertext early into 2 blocks, namely block y and block z, which is worth 32 bits, and divides the key into the 4 key block that K[0], K[1], K[2], K[3], which is well worth the 32 bit.
6. Encryption XTEA using equation: y+= (z << 4 ^ z >> 5) + z ^ sum + k[sum & 3]; sum += delta; for each even-numbered rounds, and using the equation: z+= (y << 4 ^ y >> 5) + y ^ sum + k[sum >> 11 & 3]; for each odd round.
7. Phase number 5 and 6 be repeated 32 rounds, to get the ciphertext.

For the design of xTEA decryption scheme will be built, specifically illustrated in the following Figure:

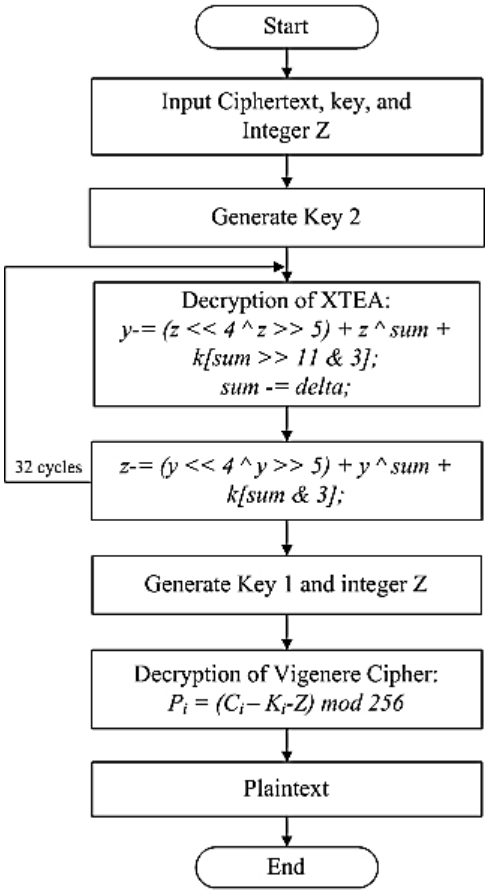


Fig 6: Design of the decryption scheme VixTEA

Explanation of the encryption process in Figure 6 above:

1. Input ciphertext (documents), Key 1 (Key Vigenére) of length n <256, key 2 (Key XTEA) with a length of 16 characters, or 128 bits, and the value of Z.
2. Generate key 2.
3. Before performing encryption with XTEA, first dividing the ciphertext early into 2 blocks, namely block y and block z, which is worth 32 bits, and divides the key into the 4 key block that K[0], K[1], K[2], K[3], which is well worth the 32 bit.
4. Decryption XTEA using equation: *z-= (y << 4 ^ y >> 5) + y ^ sum + k[sum >> 11 & 3]; sum -= delta;* for each even-numbered rounds, and using the equation: *y-= (z << 4 ^ z >> 5) + z ^ sum + k[sum & 3];* for each odd round.
5. Phase number 5 and 6 be repeated 32 rounds.
6. Generate key 1 dan value of Z.

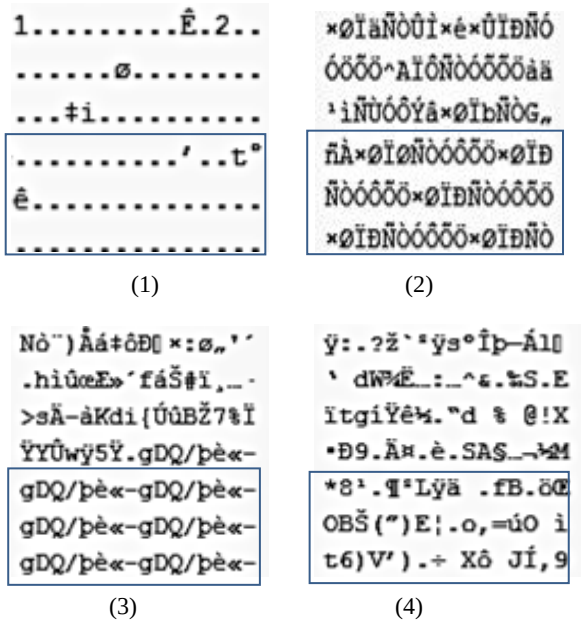
7. Decryption Vigenére cipher using equation: $P_i = (C_i – K_i - Z) \bmod 256$.

4. RESULTS AND DISCUSSION

The experiments were performed using the concept of merging algorithm (VixTEA), digital document file types used are files with various extensions, including .pdf, .mp4, .docx, .pptx, .jpeg, and .txt. This stage will be carried out tests and analysis on each algorithm, before and after the merger:

1. Provide visual comparison between the results of the encryption from each concept.
2. Encrypt a file documents that have been provided by using an application that adopts the concept of Vigenére cipher algorithm, XTEA and VixTEA to determine the value of Entropy analysis, analysis of bruteforce attacks, performance the algorithms, and integrity testing of results document decryption.

To provide the difference between the results of visual encryption of any concept of encryption (the algorithm) before and after combined are presented in the following Figure 7:



(1) (2)

(3) (4)

Fig 7: (1) Plaintext; (2) Encrypt of Vigenére cipher; (3) Encrypt of XTEA; (3) Encrypt of VixTEA

Figure 7 above shows a comparison of the results of visual encryption of every concept, from experiments carried out above using a file with a .txt extension, the document which is used as an example in this experiment is a document that contains many of the same characters, the characters (plaintext) in question, namely period (.), the test results showed that the ciphertext is generated by an algorithm Vigenére cipher and XTEA looks to repeat some of the same character in (last three lines), while the encrypted ciphertext of the concept VixTEA no repetition of the same character in each line, this show that the level of randomization performed by the concept of merging (VixTEA) is better than the ciphertext resulting from Vigenére cipher and XTEA. To view the security level and performance of each encryption concept, it will be analyzed as follows:

4.1 Entropy Analysis

Ideal entropy value if an information is encrypted and randomized in perfect condition is 7.99902 (~8), based on that, the designed system is considered safe from attack entropy. However, if the value of entropy is smaller than 8, it can be said encryption system is still unpredictable [7], entropy of ciphertext can be calculated using the following formula [3]:

$$H_e = -\sum_{k=0}^{G-1} P(k) \log_2\big(P(k)\big) \qquad (10)$$

Description:
H_e : Entropy value
G : Total characters used (ASCII code)
P(k) : Symbol-*k*

Table 2. Entropy analysis from algorithms

No	File	Size	Vigenére	XTEA	VixTEA
1	Be.pdf	31.6 Mb	7.99045	7.99981	7.99995
2	Du.mp4	33.6 Mb	7.99999	7.99999	7.99999
3	Mt.docx	17.8 Mb	7.97496	7.99927	7.99993
4	Mo.pptx	23.5 Mb	7.99944	7.99999	7.99999
5	Mo.jpeg	1.90 Mb	7.99344	7.99915	7.99984
6	Co.txt	3.59 Kb	6.01011	7.94875	7.94946
Average			**7.66140**	**7.99116**	**7.99153**

Table 2 shows that the value of the entropy before and after the incorporation of algorithms, an increase in the value of entropy, average entropy value of Vigenére cipher encryption result is 7.66140, XTEA 7.99116 and 7.99153 VixTEA value of entropy, entropy value contained in Table 3 above is described in the graph in Figure 8 below:

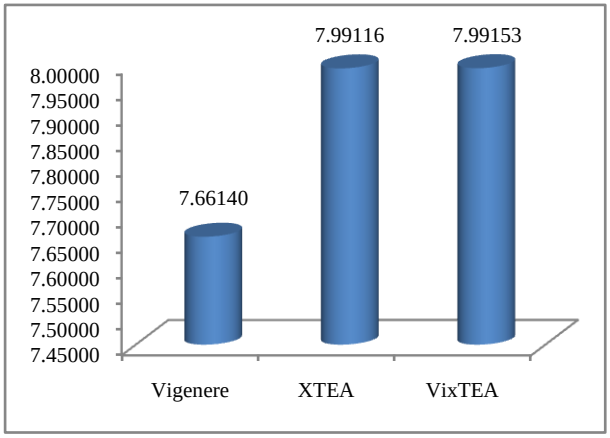


Fig 8: Graph Entropy analysis

The graph shown in Figure 8, seen the value of entropy results Vigenére cipher encryption algorithm is so low, while the value of entropy from encryption of XTEA almost has in common with VixTEA entropy, but between both of them have different values, although not significantly increased, from the data presented above can be picked conclusion, after the merger of these two algorithms can improve the value of the entropy of the resulting ciphertext, and of course it is considered to be the result of merging more ready to fight attack of entropy, based on the theory presented by [7] if the entropy value of 7.99902 (~ 8) it is considered to be safe from attack entropy, the conclusions obtained by the VixTEA

encryption concept can increase the value of entropy and can be free from attack cryptanalyst.

4.2 Performance Anaysis

To view the performance of each concept before and after combined encryption, performance associated with the time described in Table 3 below:

Table 3. Time encryption analysis (performance)

No	File	Size	Encrypt time (in seconds)		
			Vigenére	XTEA	VixTEA
1	Be.pdf	31.6 Mb	0.610179	3.992444	4.845577
2	Du.mp4	33.6 Mb	0.640530	4.331984	4.720395
3	Mt.docx	17.8 Mb	0.550764	2.378419	2.708127
4	Mo.pptx	23.5 Mb	0.708328	2.954658	3.355831
5	Mo.jpeg	1.90 Mb	0.084031	0.245188	0.304957
6	Co.txt	3.59 Kb	0.000346	0.000687	0.000708
Average			**0.432363**	**2.317230**	**2.655932**

Table 3 above explains that the average time required to perform encryption using Vigenére cipher algorithm takes 0.432363 seconds, and XTEA 2.317230 seconds, while time encryption of VixTEA is 2.655932 seconds, the information in Table 3 are described again in the graph in Figure 9 below:

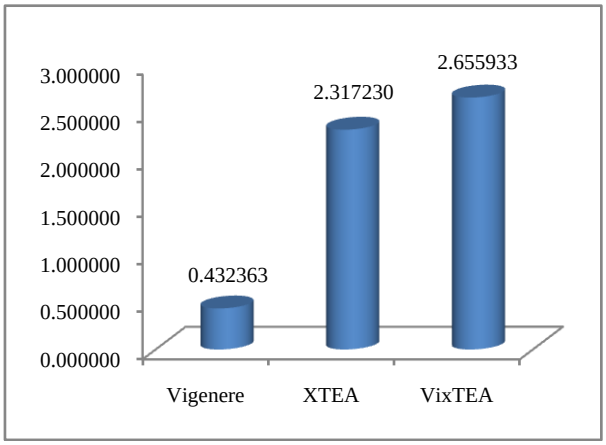


Fig 9: Graph comparison time encryption

If you created a scenario, the user performs encryption each uses algorithms and different applications, with the first encryption that uses Vigenére cipher and then, encrypting both use XTEA, means the time of encryption obtained will be slower that is 2.749593 seconds (the sum of the time of encryption Vigenére and XTEA), and based on the results of the analysis, it can be concluded that VixTEA, does not change the performance of the algorithm to be slower in doing encryption, is evident from the above test results obtained from time encryption VixTEA only takes 2.52517 seconds.

4.3 Bruteforce Attack Analysis

In conducting experiments bruteforce attack, using the following formula [10]:

$$P = r \wedge n \quad (11)$$

Description:

P: Number of keys

r: Amount of possible keys

n: Total Characters used

To perform a bruteforce attack on the ciphertext encryption result the Vigenére cipher, the key parameters used to perform the encryption has a value of n (unknown), all key characters that are used in the form of letters and numbers in accordance with the code of ASCII 256 characters, then the details of the formula above, namely:

r = (Possible keys = 12 characters (example))

n = (Total characters used = 256)

key combinations = 25612

P = 25.106.405.242 years

After modifying the Vigenére cipher algorithm, in implementation, the strength of this algorithm not only on the length of the key-value 256n, but also on an integer value for each key, with possibility of Z = 103, whereas for a bruteforce attack on XTEA, the value of the key parameters used are 128 bits, all the key characters that are used in the form of letters and numbers corresponding to the ASCII code 256 characters, then the details of the formula above, namely:

r = (Possible keys = 16 characters (128 bit))

n = (Number of characters used = 256)

Key combinations = 25616

P = 1.078.311.894.384 years

After combining these two algorithms, cryptanalyst who perform a bruteforce attack must first penetrate the three (3) defense contained in the ciphertext, as described in the Figure 10 following:

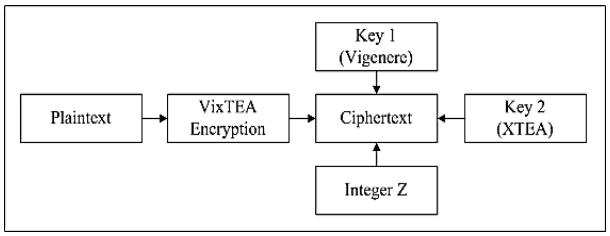


Fig 10: Ciphertext security of VixTEA

Security described in the Figure 10 above, refer to the following formula:

Amount of possibilities: 256n + 103 + 25616 (12)

Length time required: 26,2 x 1012

Based on these calculations, it is known that the decryption experiment using a bruteforce method requires a very long time or is not possible to do. So it can be concluded that the application of double encryption on digital documents (plaintext) can produce a ciphertext that is safe from attack bruteforce.

4.4 Integrity Data Test

Examination the integrity of document has the aim to determine whether there is a change from a file decryption results or not, by matching the hash value of document, the results showed that the encryption by VixTEA can restore files into original form without any changes.

5. CONCLUSION

The proposed concept is to combine two algorithms, XTEA with Vigenére cipher for encrypting the document (VixTEA).

This concept is implemented in C# programming language. This concept can improve the security of digital documents to be better, seen from the entropy analysis, and analysis of bruteforce attacks. This concept also does not change the performance of the algorithm, and does not alter the integrity of the data. The concept of encryption VixTEA is the concept of the algorithm symmetry using only public key, this is the main weakness of VixTEA, for it needs to be developed further by adding algorithms asymmetry which uses a public key and a private key, for example, the algorithm El-Gamal so that the distribution of security and key can be safer, VixTEA also further developed using multiplatform programming languages like python.

6. REFERENCES

[1] Bhateja. A. K., Bhateja. A., Chaudhury. S., and Saxena. P. K. 2015. "Cryptanalysis of Vigenére cipher using Cuckoo Search". Applied Soft Computing, vol. 26. 315-324.

[2] Denis. T. S. Extended TEA Algorithms. 1999. vol. 1. 2-6 Unpublished.

[3] El-latif. A. A. A., Li. L, Zhang, T. Wang. N, Song, X, and X. Niu. 2012. "Digital Image Encryption Scheme Based on Multiple". 67–88.

[4] Gaba. S., Aggarwal. I., and Pandey. S. 2012. "Design of Efficient XTEA Using Verilog". International Journal of Scientific and Research Publications. vol. 2. (6). 1-5.

[5] Hatipoglu. B. 2008. A Wireless Entryphone System Implementation With MSP430 and CC1100. Faculty of Engineering and Architecture Department of Komputer Engineering. Yetipede University. Unpublished.

[6] JaydebBhaumi. N .D. 2012. "A Modified XTEA". International Journal of Soft Computing and Engineering. vol. 2. (2). 461-464.

[7] Jolfaei. A. A., and Mirghadri. A. 2011. Image Encryption Using Chaos and Block Cipher. Computer and Information Science. 4:1.

[8] Kaminsky. A., Sparlin. R., Meresca. P., and Kelly. J. 2013. XTEA Block Cipher. Unpublished.

[9] Ko. Y., Hong. S., Lee. W., and Kang. J. Related Key Differential Attacks on 27 rounds of XTEA anf Full-round GOST. Unpublished.

[10] Pahrul, I., Yudi, P., and Imam. R. 2015. "Image Encryption using Combination of Chaotic System and Rivers Shamir Adleman (RSA)". International Journal of Computer Applications. vol. 123. (6), 11-16.

[11] Sekar. G., Mouha. N., Velichkov. V., and Preneel. B. Meet-in-the-Middle Attacks on Reduce-Round XTEA. Unpublished.

[12] Sinha, S. 2014. "Improving Security of Vigenère Cipher by Double Columnar Transposition". International Journal of Computer Applications. vol. 100, (14), 6–10

[13] Spillman. R., Janssen. M., Nelson. B., and Kepner. M. 1993. "Use of a genetic algorithm in the cryptanalysis of simple substitution ciphers". Cryptologia. vol. 17. (1). 31–44.

[14] Stallings. W. 1999. Cryptography and Network Security, 2nd edition, Prentice Hall.

[15] Stallings. W. 2006. Cryptography and Network Security : Principles and Practices, Prentice-Hall, Upper Saddle River. New Jersey.

[16] Wheeler. D. J., and Needham. R, TEA, a tiny encryption algorithm. Unpublished.