Journal of Computing and Applied Informatics (JoCAI) Vol. 4, No.2, 2020 | 89 – 99

DATA SCIENCE
Journal of Computing and Applied Informatics

A Hybrid Cryptosystem Using Vigenère Cipher and Rabin-*p* Algorithm in Securing BMP Files

Mohammad Andri Budiman*, Muhammad Yogi Saputra, Handrizal

Departemen Ilmu Komputer, Fakultas Ilmu Komputer dan Teknologi Informasi, Universitas Sumatera Utara, Jl. Universitas No. 9-A, Kampus USU, Medan 20155, Indonesia

Abstract. Vigenère cipher is a classical cryptography algorithm and similar to other classical algorithms, it produces smaller but less secure ciphertexts than a public key cryptography algorithm. Meanwhile, Rabin-*p* is a public key cryptography algorithm with a stronger encryption than Vigenère cipher. Nevertheless, as a public key algorithm, Rabin-*p* is inefficient to encrypt vast amounts of messages such as BMP image files, since the size of the cipherimages will increase manyfold and this would lead to a problem in storing and sending the cipherimages. To overcome these problems, in this study, we combined the Vigenère cipher and the Rabin-*p* algorithm in a hybrid cryptosystem scheme. In the experiment, the Vigenère cipher was used to encrypt the BMP files and the Rabin-*p* algorithm was used to encrypt the Vigenère keys. The result showed that the size of the cipherimages did not increase and the decryption procedure could recover the original BMP files while maintaining their integrity.

Keyword: Vigenère cipher, Rabin-*p*, hybrid cryptosystem, BMP file.

Received 3 June 2020 | Revised 26 June 2020 | Accepted 31 July 2020

1 Introduction

A confidential message must be encrypted in such a way so that only intended parties can recover it back and read it. To ensure confidentiality, in the past, people secured data using classical cryptographic algorithms which all belong to the class of symmetric algorithms. Symmetric algorithms are cryptography algorithms that use a single key for both encryption and decryption procedures [1][2]. Their security depends solely on the secrecy of the key; if the key used can be tracked down or guessed methodically by unwanted parties, then the whole message can easily be decrypted by them. This results in messages being vulnerable to theft. Then came the modern time, public key cryptography algorithms are now used everywhere. Public key cryptography algorithm has two distinct keys: private key and public key. The public key is used to encrypt messages into obfuscated form and the private key is used to decrypt the

*Corresponding author at: Departemen Ilmu Komputer, Fakultas Ilmu Komputer dan Teknologi Informasi, Universitas Sumatera Utara, Jl. Universitas No. 9-A, Kampus USU, Medan 20155, Indonesia

E-mail address: mandrib@usu.ac.id

ISSN: 2580-6769 | e-ISSN: 2580-829X | DOI: https://doi.org/10.32734/jocai.v4.i2-4173
Journal Homepage: https://jocai.usu.ac.id

obfuscated messages back into the original massages [3]. In the public key encryption scheme, both public key and private key are generated by the recipient of the message. The public key should be known to everyone and the private key should be known only to the recipient [4]. The security of the public key encryption algorithm depends on the size of the key: the longer the key, the securer the algorithm. But the size of key also has its consequence: the longer the key, the longer the time to encrypt and decrypt, and the longer the resulting ciphertext. Thus, encrypting vast amount of data with public key encryption scheme is deemed to be ineficient.

Vigenère cipher is a classical polyalphabetical substitution cipher, *i.e.*, a cipher that utilizes multiple substitution characters. Similar to other classical ciphers, Vigenère cipher produces small ciphertexts: the size of its ciphertext is always equal to the size of its plaintext. The drawback of Vigenère cipher is that it is easy nowadays to attack it by some analytical methods, such as the Kasiski method, Friedman test, and the twist algorithm [5].

Rabin algorithm [6] is a public key cryptography algorithm that uses Blum integer n as its modulus. Recall that if n is a Blum integer, then $n = p \times q$, $p, q \in PRIMES$, $p \neq q$, and $p \equiv q \equiv 3 \ (mod\ 4)$. Rabin algorithm has an advantage over the well-used public key algorithm, the RSA, i.e. the encryption procedure of the Rabin algorithm is faster than that of RSA algorithm, since Rabin only uses exponent 2 while RSA uses exponent e which is much greater than 2. However, the decryption procedure in Rabin algorithm results in four results, and only one of them is the original message [7]; thus, this may lead to confusion on the side of the recipient.

Rabin-p algorithm is a variant of Rabin algorithm which was designed by M. A. Asbullah and M. R. K. Ariffin [8]. One obvious advantage of this algorithm is that the decryption procedure of the Rabin-p algorithm only results in one result, *i.e.*, the original message; and, therefore, there is no more confusion on the side of the recipient about finding out the original message out of four decryption results as in the Rabin algorithm. The other advantages of the Rabin-p algorithm are that this algorithm does not need to use Jacobi symbol [9] and since it also does not need to use Chinese Remainder Theorem computation, this cryptosystem cannot be compromized by Novak's attack [8] [10].

Earlier, it has been mentioned that public key cryptography is inefficient to encrypt large messages, such as BMP files, since the size of the cipherimages will increase manyfold and this would lead to a problem in storing and sending the cipherimages. It is also been mentioned that classical cryptography such as Vigenère cipher is prone to various kinds of attacks. In this study, we combined the Rabin-p algorithm and Vigenère cipher in a hybrid scheme in order to solve these problems. In this scheme, the key of the Vigenère cipher is encrypted with Rabin-p algorithm while the BMP file is encrypted with Vigenère cipher.

2 Methods

In this section, we explain the Vigenère cipher, the Rabin-*p* algorithm, and the proposed hybrid cryptosystem along with the example of encryption and decryption procedures.

2.1 The Vigenère cipher

The Vigenère cipher was developed by Blaise de Vigenère in 1583. The Vigenère cipher uses a defined square matrix termed as tabula recta (which is also known as Vigenère square or Vigenère table) and a series of keys to encrypt a plaintext. Since during the encryption procedure every character of the plaintext is substituted with different key, the Vigenère cipher belongs to the class of polyalphabetic cipher. By far, the most widely known polyalphabetic substitution cipher is, arguably, the Vigenère cipher [11]. Compared to a monoalphabetic substitution cipher such as Caesar cipher and Affine cipher, the Vigenère cipher is considered securer since it is harder to be compromized by a method called frequency analysis [2]. The formula for encryption and decryption of the Vigenère cipher are as follows.

Encryption:

$$C_i \equiv (P_i + K_i) \text{ (mod N)}$$

Decryption:

$$P_i \equiv (C_i - K_i) \text{ (mod N)}$$

Where:

C_i = The decimal value of the ith ciphertext character
P_i = The decimal value of the ith plaintext character
K_i = The decimal value of the it^{h} key character
N = The length of the *tabula recta*

We shall now show below how to encrypt and decrypt one pixel of a BMP file.

A. The Vigenère Cipher Encryption (Example)

An example of using Vigenère cipher to encrypt a pixel of a BMP file is as follows:

1. Suppose that the pixel of the BMP file has these RGB values:

   $red = 185; green = 255; blue = 125.$

2. In Vigenère cipher, these values become:

   $P_1 = 185; P_2 = 255; P_3 = 125$

3. We choose some Vigenère keys:

$K_1 = 85; K_2 = 91; K_3 = 155$

4. Using the encryption formula $C_i \equiv (P_i + K_i)$ (mod N), we compute:

$C_1 = (P_1 + K_1) \bmod 256 = (185 + 85) \bmod 256 = 270 \bmod 256 = 14$

$C_2 = (P_2 + K_2) \bmod 256 = (255 + 91) \bmod 256 = 310 \bmod 256 = 90$

$C_3 = (P_3 + K_3) \bmod 256 = (125 + 155) \bmod 256 = 220 \bmod 256 = 24$

The ciphertext C = (14, 90, 24) is the corresponding RGB value in the cipherimage. Note that modulo 256 was used in the computation since we encrypted a pixel of 8-bit BMP where every R, G, and B can have 2^8 = 256 different values.

B. The Vigenère Cipher Decryption (Example)

The decryption procedure of the cipherimage is as follows:

1. In the cipherimage, we have a pixel with these values:

$C_1 = 14; C_2 = 90; C_3 = 24$

2. From secured channel, we have the corresponding keys:

$K_1 = 85; K_2 = 91; K_3 = 155$

3. Using the decryption formula $P_i \equiv (C_i - K_i)$ *(mod N)*, we compute:

$P_1 = (C_1 - K_1) \bmod 256 = (14 - 85) \bmod 256 = 185$

$P_2 = (C_2 - K_2) \bmod 256 = (90 - 91) \bmod 256 = 255$

$P_3 = (C_3 - K_3) \bmod 256 = (24 - 155) \bmod 256 = 125$

Thus, $P = (185, 255, 125)$ is the corresponding pixel value of the decrypted image.

2.2 The Rabin-*p* Algorithm

The Rabin-*p* algorithm was invented in Malaysia by M. A. Asbullah and M. R. K. Ariffin [8] as a variant of Rabin algorithm. The Rabin algorithm has four decryption results; thus, without additional information, it would be confusing for a recipient to decide which one of these four is the original message. The Rabin-*p* algorithm solves this problem since its decryption procedure only results in one result, *i.e.*, the original message. The Rabin-*p* algorithm has other properties: it does not rely on Jacobi symbol [9] and it does not utilize Chinese Remainder Theorem (CRT) computation. Since CRT is avoided, the Rabin-*p* algorithm cannot be compromized by Novak's

attack [8] [10]. In the following, we will describe the procedures for key generation, encryption, and decryption of the Rabin-*p* algorithm.

The Rabin-*p* key generation procedure is as follows [9]:

1. Choose *k*, the security parameter.
2. Generate two random and different prime numbers, p and q, such that $2^k < p, q < 2^{k+1}$, and $p \equiv q \equiv 3 \pmod 4$.
3. Calculate $N = p^2 q$.
4. Keep the value of p as private key. (Although the authors [9] suggest to only keep the value of p as private key, we recommend to also keep the value of q as secret).
5. Publish N as public key.

The Rabin-*p* encryption procedure is as follows [9]:

1. Obtain the public key, N.
2. Take a message m such that $0 < m < 2^{2k-1}$ and $GCD(m, N) = 1$.

   In the proposed hybrid cryptosystem, m is the key of the Vigenère cipher.
3. Calculate $c \equiv m^2 \pmod N$.
4. Send c to the recipient

The Rabin-*p* decryption procedure is as follows [9]:

1. Obtain the value of c.
2. Calculate $w \equiv c \pmod p$.
3. Calculate $m_p \equiv w^{\frac{p+1}{4}} \pmod p$.
4. Calculate $i = \frac{c - {m_p}^2}{p}$
5. Calculate $j \equiv \frac{i}{2m_p} \pmod p$
6. Calculate $m_1 = m_p + jp$
7. If $m_1 < 2^{2k-1}$ then return $m = m_1$
8. Else, return $m = p^2 - m_1$

A. The Rabin-p Key Generation (Example)

1. The recipient chooses $k = 7$ as the security parameter. (For real-world usage, we recommend choosing much bigger security parameter, *e.g.*, $k > 512$).
2. The recipient generates $p = 131$, $q = 43$, which satisfy $2^k < p, q < 2^{k+1}$, and $p \equiv q \equiv 3 \pmod 4$.

3. The recipient calculates $N = p^2q = 131^2 \times 43 = 737923$.
4. The recipient keeps p as private key. In addition, the recipient also keeps the value of q as per recommendation.
5. The recipient publishes the value of N.

B. The Rabin-p Encryption (Example)

1. The sender obtains the value of $N = 737923$.
2. The sender chooses a message m. In the proposed hybrid cryptosystem, m is the key of Vigenère cipher. Let say that $m = K_1 = 85$, which satisfies $0 < m < 2^{2k-1}$ and $GCD(m, N) = 1$.
3. The sender calculates the cipherkey, $c = m^2 \bmod N = 85^2 \bmod 737923 = 7225$.
4. The sender sends the value of c to the recipient.

C. The Rabin-p Decryption (Example)

1. The recipient receives the value of $c = 7225$.
2. The recipient calculates $w = c \bmod p = 7225 \bmod 131 = 20$.
3. The recipient calculates $m_p = w^{\frac{p+1}{4}} \bmod p = 20^{\frac{131+1}{4}} \bmod 131 = 46$.
4. The recipient calculates $i = \frac{c - m_p{}^2}{p} = \frac{7225 - 46^2}{131} = \frac{5109}{131} = 39$
5. The recipient calculates $j = \frac{i}{2m_p} \bmod p = \frac{39}{92} \bmod 131 = 39.92^{-1} \bmod 131 = 39.47 \bmod 131 = 130$.
6. The recipient calculates $m_1 = m_p + jp = 46 + 130.13 = 17076$.
7. Since $m_1 > 2^{2k-1}$ then $m = p^2 - m_1 = 131^2 - 17076 = 85$.

We have shown that the Rabin-p decryption procedure has recovered back the value of the Vigenère cipher's key, $K_1 = 85$.

3 Result and Discussions

In this section, we will show the result of using the Vigenère cipher and the Rabin-p algorithm in a hybrid scheme to secure some BMP files. The Vigenère cipher's keys of each BMP file were encrypted and decrypted using the Rabin-p algorithm, while the BMP files were encrypted and decrypted using the Vigenère cipher.

Table 1 BMP Encryption Result

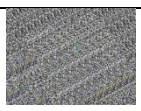
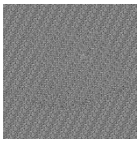
Plainimage	Cipherimage	Encryption Time (ms)
		
image5.bmp	cipherimage5.bmp	0.3421
259 x 194 pixel	259 x 194 pixel	
147 KB	147 KB	

 image3.bmp 236 x 236 pixel 163 KB	 cipherimage3.bmp 236 x 236 pixel 163 KB	0.5613
 image2.bmp 355 x 245 pixel 255 KB	 cipherimage2.bmp 355 x 245 pixel 255 KB	0.8533
 image6.bmp 500 x 300 pixel 439 KB	 cipherimage6.bmp 500 x 300 pixel 439 KB	2.1755
 image4.bmp 488 x 488 pixel 697 KB	 cipherimage4.bmp 488 x 488 pixel 697 KB	2.5886
 image1.bmp 439 x 600 pixel 773 KB	 cipherimage1.bmp 439 x 600 pixel 773 KB	3.4664

From Table 1, it can be seen that all cipherimages cannot be comprehend by normal eyes and the size of each cipherimage is the same as the size of its corresponding plainimage. Since the size did not increase, there would be an efficiency in storing and sending the cipherimages, and, therefore, one research problem is solved.

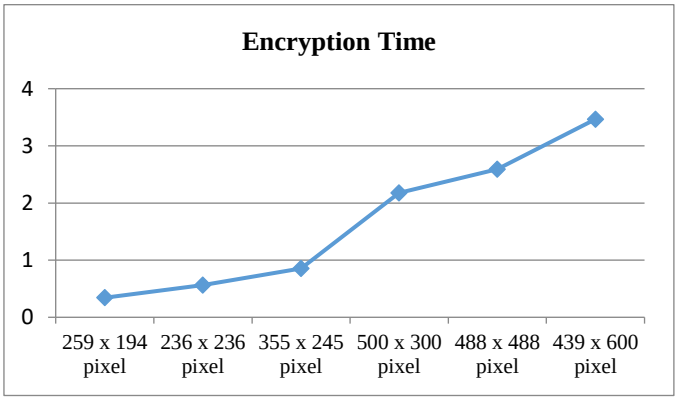
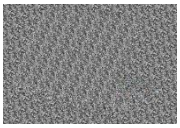
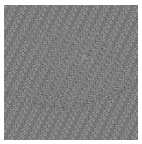


Figure 1 Encryption time (in milliseconds) of various sizes of BMP files

From Figure 1, it can be deduced that the correlation between the size of BMP file and encryption time is directly porportional as might be expected.

Table 2 BMP Decryption Result

Cipherimage	***Plainimage***	**Decryption Time (ms)**
 cipherimage5.bmp 259 x 194 pixel 147 KB	 plainimage5.bmp 259 x 194 pixel 147 KB	10.3747
 cipherimage3.bmp 236 x 236 pixel 163 KB	 plainimage 3.bmp 236 x 236 pixel 163 KB	10.8662
 cipherimage2.bmp 355 x 245 pixel 255 KB	 plainimage 2.bmp 355 x 245 pixel 255 KB	11.0448
 cipherimage6.bmp	 plainimage	13.0079

500 x 300 pixel 439 KB	6.bmp 500 x 300 pixel 439 KB	
 cipherimage4.bmp 488 x 488 pixel 697 KB	 plainimage 4.bmp 488 x 488 pixel 697 KB	15.3301
 cipherimage1.bmp 439 x 600 pixel 773 KB	 plainimage 1.bmp 439 x 600 pixel 773 KB	15.7224

From Table 2, it can be seen that each cipherimage which cannot be comprehend by normal eyes can be recovered back to its corresponding plainimage. The image integrity has been maintained, and, thus, another research problem is solved. Comparing Table 1 and Table 2, we may deduce that encryption takes less time than decryption.

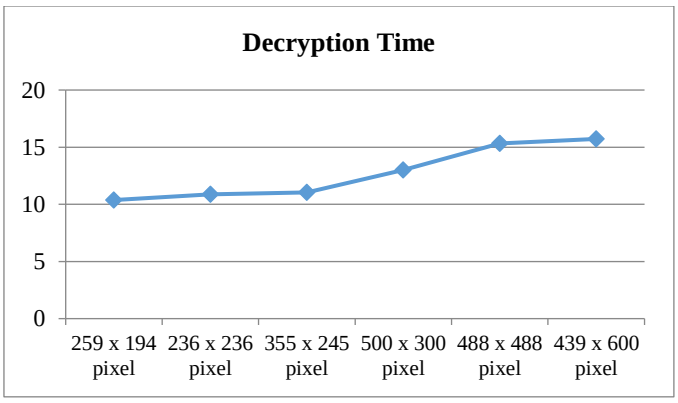


Figure 2 Decryption time (in milliseconds) of various sizes of cipherimages

From Figure 2, one may deduce that the correlation between the size of cipherimages and decryption time is directly porportional.

4 Conclusion

From the experiment results, we may conclude that:

1. A hybrid cryptosystem using Vigenère cipher and Rabin-p algorithm in securing BMP files has been implemented. In this cryptosystem, the key of the Vigenère cipher is encrypted with Rabin-p algorithm while the BMP file is encrypted with Vigenère cipher.

2. The size of the cipherimage file is the same as the size of its corresponding BMP file. Because there is no increase in the size, there would be an efficiency in storing and transmitting the cipherimages.

3. The correlation between the size of BMP file and its encryption time is directly porportional.

4. The decryption procedure can recover the cipherimage to its corresponding plainimage without loss of integrity.

5. The correlation between the size of cipherimage and its decryption time is directly porportional.

6. The encryption time takes less time than decryption time. This is due to the fact that there are more steps and complexities of computation in the encryption procedure than in the decryption procedure.

REFERENCES

[1] S. Chandra, S. Paira, S. S. Alam, and G. Sanyal, "A comparative survey of Symmetric and Asymmetric Key Cryptography", in *2014 International Conference on Electronics, Communication and Computational Engineering (ICECCE)*, 2014.

[2] Q. A. Kester, "A cryptosystem based on Vigenère cipher with varying key", *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, pp. 108-113, 2012.

[3] E. Ramaraj, S. Karthikeyan, and M. Hemalatha, "A design of security protocol using hybrid encryption technique (AES-Rijndael and RSA)", *International Journal of The Computer, the Internet and Management*, vol. 17, no. 1, pp. 78-86, 2009.

[4] V. Gampala, S. Inuganti, and S. Muppidi, "Data security in cloud computing with elliptic curve cryptography", *International Journal of Soft Computing and Engineering (IJSCE)*, vol. 2, no. 3, pp. 138-141, 2012.

[5] S. Park, J. Kim, K. Cho, and D. H. Yum. "Finding the key length of a Vigenère cipher: How to improve the twist algorithm", *Cryptologia*, vol. 44, no. 3, pp. 197–204, Jan. 2019.

[6] M. O. Rabin, Digitalized Signatures and Public-Key Functions as Intractable as Factorization, No. MIT/LCS/TR-212, Massachusetts Inst. of Tech. Cambridge Lab. for Computer Science, 1979.

[7] H. R. Hashim, "H-Rabin Cryptosystem", *Journal of Mathematics and Statistics*, vol. 10, no. 3, pp. 304–308, Jan. 2014.

[8] M. A. Asbullah and M. R. K. Ariffin, "Design of Rabin-like cryptosystem without decryption failure", *Malaysian Journal of Mathematical Sciences*, vol. 10, pp. 1-18, 2016.

[9] M. A. Asbullah, M. R. K. Ariffin, and Z. Mahad, "Analysis on the Rabin-*p* cryptosystem", in *AIP Conference Proceedings*, vol. 1787, no. 1, p. 080012, AIP Publishing LLC, Nov. 2016.

[10] R. Novak, "SPA-Based Adaptive Chosen-Ciphertext Attack on RSA Implementation," *Public Key Cryptography Lecture Notes in Computer Science*, pp. 252–262, 2002.

[11] B. Carter and T. Magoc, *Introduction Classical Ciphers and Cryptanalysis*, 2007.