International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 01, January-2017

Vigenere Cipher Algorithm with Grayscale Image Key Generator for Secure Text File

Imam Saputra[1]
Departement of Computer Engineering
STMIK Budi Darma
Medan, Indonesia
Jl. Sisingamangaraja XII No. 338, Siti Rejo I, Medan Kota,
Kota Medan, Sumatera Utara, 20216

Mesran[2]
Departement of Computer Engineering
STMIK Budi Darma
Medan, Indonesia
Jl. Sisingamangaraja XII No. 338, Siti Rejo I, Medan Kota,
Kota Medan, Sumatera Utara, 20216

Nelly Astuti Hasibuan[3]
Departement of Computer Engineering
STMIK Budi Darma
Medan, Indonesia

Jl. Sisingamangaraja XII No. 338, Siti Rejo I, Medan Kota,
Kota Medan, Sumatera Utara, 20216

Robbi Rahim[4]
Departement of Computer Engineering
Medan Institute of Technology
Medan, Indonesia
Jl. Gedung Arca No.52 Kota Medan, Sumatera Utara,

***Abstract* - With the changing of the times, information is crucial today especially for technological developments, especially in data security systems. In maintaining data security, there is a branch of science in its development, namely cryptography. Classical cryptography as vigenere cipher is a cryptographic algorithm implementation is very simple but quite powerful in his era. Having discovered methods kasiski, vigenere cipher algorithm is very easy to be analyzed by cryptanalyst to get a key. This is due to the relationship between the cipher, plaintext, and the key cryptography. The core used is usually composed of some characters arrangement either letters or numbers that are not too long, so it is easy to remember. So as to facilitate cryptanalyst to determine the key cryptography. To that end, the key must be an array of random characters long, so that the relationship between plaintext, ciphertext and key becomes very apparent that it would be difficult to solve by cryptanalyst. Which is the key arrangement of random characters that can obtain the pixel values of an image that being converted into ASCII characters? The pixel values of 8-bit grayscale images ranging from 0-255 equal the number of characters in the ASCII table. So that all pixel values in an 8-bit grayscale image can be converted into random characters and can be used as a key for the Vigenere Cipher Algorithm.**

Keywords*: *Vigenere Cipher, Key Generator, Grayscale Image 8 Bit

I. INTRODUCTION

Computer technology needed in human life. Almost every man needs computer assistance in their daily lives. Each person will have an important document that is confidential which can only be accessed by certain people. The problem of computer security is something crucial in this information age. There are several techniques for data security one of which is a disguise or cryptographic techniques. Cryptography is the art and science to protect the data by transforming it into a specific code and is intended only for people who have the key to change the code back to normal. In the field of cryptography, there are three crucial concepts that encryption, decryption, and key. Encryption is the process of transforming information (plaintext) into a code that is not recognizable (ciphertext) by using a key. Decryption is the process of converting code that is not identifiable (ciphertext) into information (plaintext) using a key, in this case, the encrypted files in text files.

One of the famous classic cryptographic algorithms is Vigenere Cipher Algorithm. Vigenere Cipher is a form polyalphabetic substitution like the idea expressed Caesar but by adding more secure locks are formed. Vigenere Cipher is well known because it is easily implemented. This method is strong enough to avoid a cryptanalyst who uses frequency analysis until. Finally, someone named Frederick Kasiski to find an efficient method to solve the Vigenere Cipher Algorithm keys. Vigenere Cipher Algorithms have abandon for quite easily analyzed by cryptanalyst. Especially with the technology that exists today and the discovery of Kasiski methods then if we want to use Vigenere Cipher Algorithms need to be modified. The manner in which this time is to generate a key from an 8-bit grayscale image pixel value has been converted into a row of characters with ASCII table. With a key which is an image, then the key can be longer and more random characters so that the relationship between the plaintext and ciphertext will be more apparent, so cryptanalyst does not easily analyze it. With long locks and randomly generated from the picture, it is not necessary to remember the order of the key characters, quite remember where the image is used as a key.

II. THEORY

A. Cryptography

Cryptography is a science that is used to maintain the confidentiality of the data, by using certain methods so that data can only read by a person who is entitled to such data, in the maintenance of the confidentiality of data, cryptography alters original data (plaintext) into data that is encrypted (ciphertext). This process is called encryption process. Cryptography can be classified into two categories, namely [1]:

1. Shared Key Cryptography
2. Public Key Cryptography

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 01, January-2017

Shared Key Cryptography is also often called symmetric key cryptography or cryptographic private key or secret key because of the key used in the encryption and decryption process at [2].

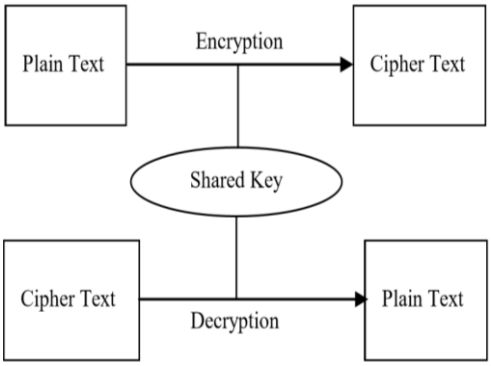


Fig 1. Shared Key Cryptography

Public Key Cryptography is also often called asymmetric key cryptography uses different keys in the encryption and decryption process. Only the private key used for encryption. Moreover, the public key used during the decryption process.

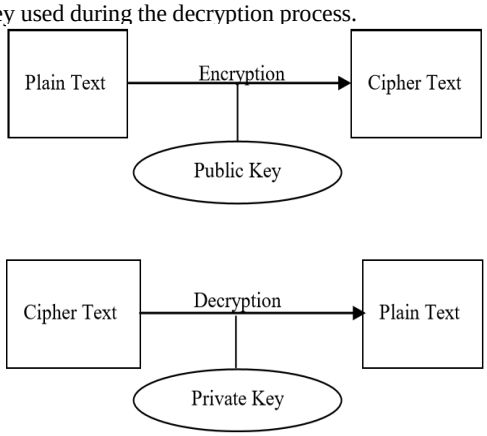


Fig 2. Public Key Cryptography

B. *Vigenere Cipher Algorithm*

Vigenere Cipher Algorithm is a classical cryptographic technique are more secure than a Caesar cipher. Vigenere Cipher cipher alphabet included in the compound (Polyalphabetic Substitution Cipher) with a 26 x 26 matrix with Caesar shift cipher [3]. Vigenere Cipher is a method of encrypting text with rows cipher based on keywords. Vigenere cipher algorithm using a square table vigenere to perform the encryption process. Each row in the table squares states ciphertext letters were obtained by the caesarian cipher. Here is a square table vigenere [4].

TABLE I. Vigenere Cipher Square Table

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	D
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	C
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	B
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Encryption and decryption process vigenere cipher algorithm can be represented mathematically [4]:

Encryption : Ci = (Pi + Ki) mod 26

Decryption : Pi¬ = (Ci + Ki) mod 26

Where C0....Cn is ciphertext, P0....Pn is plaintext and K0...Kn is key

If vigenere cipher applied in computer application, the code used by the ASCII table as many as 256 characters, so if represented mathematically be:

Encryption : Ci = (Pi + Ki) mod 256

Decryption : Pi¬ = (Ci + Ki) mod 256

C. *Digital Image*

The image of the other terms of the picture as a multimedia component that plays a crucial form of visual information. The image has characteristics that are not owned by text data, i.e., information-rich image. The image is a two-dimensional function that represents some features such as brightness or color of a scene and can be defined as a two-dimensional function f (x, y) where (x, y) position of the projected and f (x, y) defines the brightness at that point [5].

Digital image composed of elements called picture elements, image elements, and pixels. Pixel is the smallest part of an image [6]. Digital image is divided into several types based on the depth of color a binary image, grayscale image (8 bits), a color image (24-bit) and color images (32 bit). For a grayscale image (8 bits) then the value of a pixel is represented by an 8-bit binary number with a minimum value of 0 and a maximum value of 255.

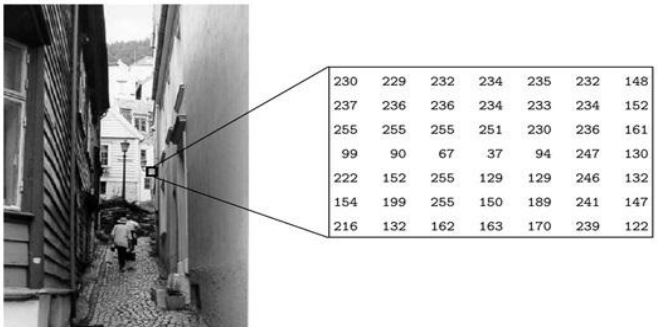


Fig 3. Grayscale Image 8 bit

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 01, January-2017

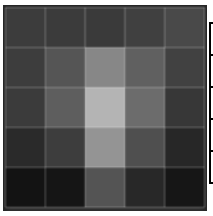
D. ASCII

ASCII (American Standard Code for Information Interchange) is an international standard in the code of letters and symbols is always used by computers and other communication tools to show the text. ASCII code has a composition of as much as 8-bit binary number. ASCII characters are divided into five groups according to their use, namely consistent communication, device control, information separator, code extension and real communication [7].

III. RESULT & DISCUSSION

A. Key Generator

To generate a series of random keys, resulting the relationship between plaintext and ciphertext are false, then used an 8-bit grayscale image with a size of 5 x 5 pixels. The pixel values of the grayscale image converted to use an ASCII table in the form of symbols or characters that will be used to perform the encryption and decryption process.



48	41	39	42	48
46	58	134	74	44
46	37	142	88	45
26	42	152	72	20
15	20	44	26	14

Fig 4. Key Generator With Grayscale Image 8 bit

If the pixel values are converted using the ASCII table

Table II
Conversion Values of Pixel Become Character

Decimal	Character
48	0
41	)
39	‘
42	*
48	0
46	.
58	:
134	å
74	J
44	,
46	.
37	%
142	Ä
88	X
45	-
26	SUB
42	*
152	Ÿ
72	H
20	DC4
15	SI
20	DC4
44	,
26	SUB
14	SO

So after being converted into a character, then the key to 0) '* 0 .: AJ.% AX-SUB * ŸHDC4SIDC4, SUBSO key that will be used for encryption and decryption process is the result of the conversion of the pixel values of the 8-bit grayscale image size of 5 x 5 pixels.

B. Encryption Process

Text data to be encrypted is NEVER underestimate YOURSELF and keys to be used in the encryption process is 0) '* 0 .: AJ.% AX-SUB * ŸHDC4SIDC4, SUBSO. If the plaintext is longer than the key, the key will be automatically restarted from the beginning so that all the characters in the encryption of plaintext completed, if the plaintext is shorter than lock the remaining locks will not be used.

C_0=(78+48) mod 256 = 126 character t
C_1=(69+41) mod 256 = 110 character n
C_2=(86+39) mod 256 = 125 character }
C_3=(69+42) mod 256 = 111 character o
C_4=(82+48) mod 256 = 130 character é
C_5=(32+46) mod 256 = 78 character N
C_6=(85+58) mod 256 = 143 character Å
C_7=(78+134) mod 256 = 212 character È
C_8=(68+74) mod 256 = 142 character Ä
C_9=(69+44) mod 256 = 113 character q
C_{10}=(82+46) mod 256 = 128 character Ç
C_{11}=(69+37) mod 256 = 106 character j
C_{12}=(83+142) mod 256 = 225 character ß
C_{13}=(84+88) mod 256 = 170 character ¬
C_{14}=(73+45) mod 256 = 118 character v
C_{15}=(77+26) mod 256 = 103 character g
C_{16}=(65+42) mod 256 = 109 character m
C_{17}=(84+152) mod 256 = 236 character ẏ
C_{18}=(69+72) mod 256 = 141 character Í
C_{19}=(32+20) mod 256 = 52 character 4
C_{20}=(89+15) mod 256 = 104 character h
C_{21}=(79+20) mod 256 = 99 character c
C_{22}=(85+44) mod 256 = 129 character ù
C_{23}=(82+26) mod 256 = 108 character l
C_{24}=(83+14) mod 256 = 97 character a
C_{25}=(69+48) mod 256 = 117 character u
C_{26}=(76+41) mod 256 = 117 character u
C_{27}=(70+39) mod 256 = 109 character m

After performing the encryption process ciphertеksnya be tn} oéNÅÈÄqÇjß¬vgmẏÍ4hcülauum

C. Decryption Process

After the plaintext is converted into ciphertext in the encryption process, the next step is to change ciperteks back into plaintext with the same key used during the encryption process. Which will decrypt ciphertext is tn} oéNÅÈÄqÇjß¬vgmẏÍ4hcülauum using keys 0) '* 0 .: AJ.% AX-SUB * ŸHDC4SIDC4, SUBSO.

P_0=(126-48) mod 256 = 78 character N
P_1=(110-41) mod 256 = 69 character E
P_2=(125-39) mod 256 = 86 character V
P_3=(111-42) mod 256 = 69 character E
P_4=(130-48) mod 256 = 82 character R
P_5=(78-46) mod 256 = 32 character
P_6=(143-58) mod 256 = 85 character U
P_7=(212-134) mod 256 = 78 character N
P_8=(142-74) mod 256 = 68 character D
P_9=(113-44) mod 256 = 69 character E
P_{10}=(128-46) mod 256 = 82 character R
P_{11}=(106-37) mod 256 = 69 character E
P_{12}=(225-142) mod 256 = 83 character S
P_{13}=(170-88) mod 256 = 84 character T

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 01, January-2017

P_{14}=(118-45) mod 256 = 73 character I
P_{15}=(103-26) mod 256 = 77 character M
P_{16}=(109-42) mod 256 = 65 character A
P_{17}=(236-152) mod 256 = 84 character T
P_{18}=(141-72) mod 256 = 69 character E
P_{19}=(52-20) mod 256 = 32 character
P_{20}=(104-15) mod 256 = 89 character Y
P_{21}=(99-20) mod 256 = 79 character O
P_{22}=(129-44) mod 256 = 85 character U
P_{23}=(108-26) mod 256 = 82 character R
P_{24}=(97-14) mod 256 = 83 character S
P_{25}=(117-48) mod 256 = 69 character E
P_{26}=(117-41) mod 256 = 76 character L
P_{27}=(109-39) mod 256 = 70 character F

After performing the decryption process tn} oéNÅÈÄqÇjß¯vgmýÍ4hcùlauum with key 0) '* 0 .: AJ.% AX-SUB * ŸHDC4SIDC4, SUBSO then back into plaintext NEVER underestimate YOURSELF. To be more concise can be seen in the following table:

Table III
Result Vigenere Cipher Encryption and Decryption

Process	Result
Plainteks	NEVER UNDERESTIMATE YOURSELF
Kunci	0)'*0.: åJ,.% ÄX-SUB* ŸHDC4SIDC4,SUBSO
Cipherteks	tn}oéNÅÈÄqÇjß¯vgmýÍ4hcùlauum

Can be seen in the relationship between plaintext to ciphertext is very apparent that would make it harder to find a cryptanalyst of cryptographic Vigenere Cipher Algorithms keys such as a row of keys generated from a very random image and key length depends on the dimensions of the picture that is used as a key. No need to remember the key because the key consists of random characters that are tough to remember, just remember the image employed in the encryption process so that the picture can also be utilized in the decryption process as long as there are changes to the pixel values of the image. Vigenere Cipher Algorithm key generation is quite practical and generated keys are also very random, so it will be difficult if analyzed by either method kasiski cryptanalyst and the brute force method.

III. CONCLUSION

This study discusses the formation of a row of keys vigenere cipher algorithm that is very random to secure a text file, so it will be difficult to analyze by cryptanalyst. By using a key generated from the 8-bit grayscale image that has been converted into a character pixel value using ASCII table it will produce a series of the main characters were very random and the length determined by the size or dimensions of the image are used as the key. In Vigenere Cipher Algorithm, there is no limit on the duration of the key utilized so it matches the key generation through the 8-bit grayscale image. So it is not difficult to find images that can be used as a key generator. The length and randomness of the key do not need to remember, to keep in mind is the image that is used as the key. Because if the imagery used at the time of encryption, there are differences with the image pixel value used at the time decryption of the ciphertext will not go back into the original plaintext.

IV. REFERENCES

[1] G. C. Kessler, An Overview of Cryptography, 2013.
[2] Y. Rajput, D. Naik dan C. Mane, "An Improve Cryptography Technique to Encrypt Text Using Double Encryption," *International Journal of Computer Application*, vol. 86, no. 6, pp. 24-28, 2014.
[3] W. Stallings, Cryptography and Network Security – Principles and Practice (Fifth Edition), Pearson Education, Inc, 2011.
[4] A.-A. M. Aliyu and A. Olaniyan, "Vigenere Cipher: Trends, Review and Possible Modifications," *Internasional Journal of Computer Application*, vol. 135, no. 11, pp. 46-50, 2016.
[5] S. Jayaraman, S. Esakkirajan dan T. Veerakumar, Digital Image Processing, New Delhi: Tata McGraw-Hill Education Private Limited, 2009.
[6] R. C. Gonzales dan R. E. Woods, Digital Image Processing (Third Edition), Pearson Education, Inc, 2009.
[7] H. Randal, Understanding the Machine, No Stark Press, Inc, 2004.