Enhancing Security of Vigenere Cipher by Stream Cipher

Fairouz Mushtaq Sher Ali
Department of Computer Science/
College of Education for Girls/
University of Kufa
Najaf/ Iraq

Falah Hassan Sarhan
Department of Mathematics/
College of Education for Girls/
University of Kufa
Najaf/ Iraq

ABSTRACT
Cryptography is a science of converting clear message into secret message "nonreadable message", where message was encrypted at sender side then decrypted at receiver side. Vigenere is an example of substitution cipher, it has various limitations, in this paper we propose an advanced encryption algorithm which improves the security of Vigenere method by combining it with modern cipher method like Stream cipher, Stream cipher relatively regards as unbreakable method, and it uses binary form (instead of characters) where the Plaintext, Ciphertext and the Key are strings of bits.
When applying the proposed algorithm, we see that the mentioned above combination cipher has a high degree of security, where cipher based on just Vigenere method is not secure. Also, the proposed algorithm makes the cryptanalysis, using frequency attack, more difficult.

General Terms
Information security, cryptography

Keywords
Plaintext, Ciphertext, Key, Cipher, Substitution, Vigenere, Stream cipher

1. INTRODUCTION
There are many aspects to security and many applications, ranging from secure commerce and payments to private communications and protecting passwords. One essential aspect for secure communications is that of cryptography[1].

Cryptography is a Greek word which means secret writing. Today this term refers to the science and art of transforming message to make them secure and immune to attacks[2]. For the purpose of security and privacy, we need to encrypt the message at the sender side and decrypt it at the receiver side. In cryptography the term Plaintext is used for the original message that is to be transformed. The message which has been transformed is called Cipher text. An encryption algorithm is a function that works with a key to transform the Plaintext into cipher text. Decryption algorithm works in the reverse order and convert the Ciphertext into Plaintext[1].

Symmetric and Asymmetric are the two types of encryption. In symmetric encryption techniques we use the same key for both encryption and decryption purpose[3].

Asymmetric-key encryption using public and private keys, the public key is announced to all members while the private key is kept secure by the user. The sender uses the public key of the receiver to encrypt the message. The receiver uses his own private key to decrypt the message[3].

In symmetric method, there are two techniques (substitution and transposition) are used as a classical methods. Substitution technique maps the Plaintext elements into cipher text elements. Substitution has further two types, Monoalphabetic and polyalphabetic cipher. In monoalphabetic the character in the Plaintext is changed to the same character in the Ciphertext. In polyalphabetic cipher a single character in the Plaintext is changed to many characters in the Ciphertext[2].

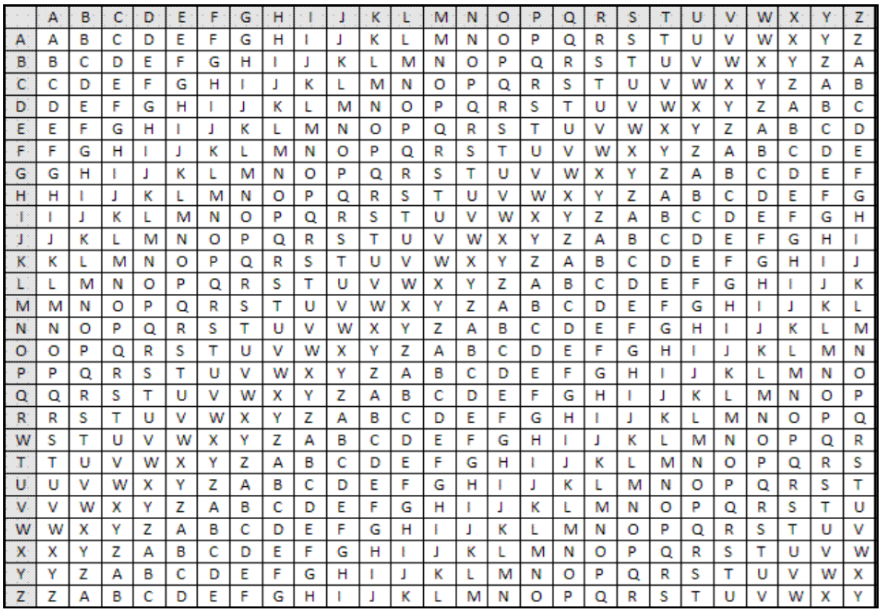
Permutation technique is one in which the Plaintext remains the same, but the order of characters is shuffled around to get the Ciphertext[1].
Also the symmetric ciphers can be divided into Stream ciphers and block ciphers, as a modern ciphers[3].

2. RELATED WORKS
This paper discusses the combination cipher related to cipher methods like Substitution and Stream cipher. Different computer and data security related researches search in different combination methods.
S.G.Srikantaswamy and H. D. Phaneendra (2011) attempt in their paper to identify that using different key values for encrypting consecutive characters of Plaintext hides the relationship between the Ciphertext and Plaintext, and makes the cryptanalysis still more complex[4].
Sonia Dhull and Vinod Saroha (2013) applied a double columnar transposition method on One Time Pad in order to overcome limitations of One time Pad cipher and provide much more secure and strong cipher[5].
Fauzan Saeed and Mustafa Rashid(2010) propose a new technique that emphasizes on improving classical encryption techniques by integrating modern cipher like DES and SDES with classical methods like Playfair and Vigenere cipher[6].

Next sections will explain Vigenere method and Stream cipher, after that we will discuss our proposed combination method.

3. VIGENERE CIPHER
Vigenere cipher, being poly-alphabetic cipher was one of the most popular ciphers in the past because of its simplicity and resistance to the frequency analysis test of letters that can crack simple ciphers like Caesar cipher[7]. The Vigenere cipher consists of several Caesar ciphers in sequence with different shift values. In Caesar cipher each letter is shifted along some places. For example for a shift of 5 A will become F, B will map to G and so on.

3.1 Vigenere square
The Vigenere square cipher uses sequence of different shift values and uses a table called tabula recta, Vigenere square, or Vigenere table. The table is a 26 * 26 matrix in which the English alphabets are written 26 times in different rows representing the different possible shifts. The table is used and substitution is made according to the varying shift values derived from the key [8,9].



	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
W	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	V
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	W
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	X
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

Fig 1: The Vigenere table [10,11].

Vigenere can also be viewed algebraically. If the letters A–Z are taken to be the numbers 0–25 then Vigenere encryption E using the key K can be written as[2]:
Ci = EK(Pi) = (Pi + Ki) mod26
and decryption D using the key K,
Pi = DK(Ci) = (Ci - Ki) mod26
where
P = P_0…P_n is the message,
C = C_0….C_n is the ciphertext and
K= K_0.....K_m is the used key.

3.2 Cryptanalysis of Vigenere Cipher

With the increase in the cryptanalytic skills, Vigenere cipher is no longer taken as secure cipher and is not popularly used. The most weak point of Vigenere cipher is the use of repeated words as key-streams that causes repetition of certain patterns in cipher texts at intervals equal to the length of the keyword used[7].

Kasiski's method provides a general technique for cryptanalyzing Vigenere ciphers with repeated keywords, based on the following observation: repeated portions of plaintext encrypted with the same portion of the keyword result in identical ciphertext segments. Consequently one expects the number of characters between the beginning of repeated ciphertext segments to be a multiple of the keyword length. Ideally, it suffices to compute the greatest common divisor of the various distances between such repeated segments, but coincidental repeated ciphertext segments may also occur. Nonetheless, an analysis (Kasiski examination) of the common factors among all such distances is possible; the largest factor which occurs most commonly is the most likely keyword length. Repeated ciphertext segments of length 4 or longer are most useful, as coincidental repetitions are then less probable[2].

4. MODERN ENCRYPTION

The symmetric ciphers can be divided into Stream ciphers and Block ciphers.

1) Stream ciphers encrypt bits individually. This is achieved by adding a bit from a key stream to a Plaintext bit. There are synchronous Stream ciphers where the key stream depends only on the key, and asynchronous ones where the key stream also depends on the Ciphertext[3].
2) Block cipher is much more than just an encryption algorithm. It can be used as a versatile building block with which a diverse set of cryptographic mechanisms can be realized. For instance, we can use them for building different types of block based encryption schemes, and we can even use block ciphers for realizing Stream ciphers. The different ways of encryption are called *modes of operation*. Block ciphers can also be used for constructing hash functions, message authentication codes which are also known as MACs, or key establishment protocols. There are also other uses for block ciphers, e.g., as pseudo-random generators. In addition to modes of operation[3].

5. PROPOSED TECHNIQUE:

Modern ciphers normally use a combination of (substitution with transposition) and some other complex transformations to create a Ciphertext from a Plaintext.
In our paper we put emphasis on proposing a new combination method (Vigenere with Stream cipher), because cipher based on just Vigenere method is not secure.

5.1 Structure of encryption algorithm

Below the briefly steps of this algorithm:
Step1: Start**.**
Step2: Read the plaintext ***P***.
Step3: Read Keyword for Vigenere cipher ***K***.
Step4: Read a random binary key for stream cipher K_{bin} that can be generated by any method of keystream generators.
Step5: Apply Vigenere equation $C = P + K$ or Vigenere square to encipher the characters in even locations.
Step6: Apply stream cipher to encipher each character in the odd locations as follows:

i. Converting the characters to ASCII value then to equivalent binary form.
ii. Enciphering these characters using stream cipher equation $C = P \oplus K_{bin}$.
iii. Converting the resulted binary numbers to equivalent ASCII value then to characters to obtain the Cipher characters.

Step7: end

5.2 Example

To clarify the proposed encryption algorithm, we will consider the following:

- **Plaintext:** cowards die many times before their death.
- **Keyword(K):** *file.*
- **Proposed Binary key (K_{Bin}):**

01100100011110000111011100 01

The Encryption results produced by the above Algorithm are explained in the following tables**:**

Table 1. Encryption results using Vigener Cipher C = P + K

Even Locations	0	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34
P →	C	W	R	S	I	M	N	T	M	S	E	O	E	H	I	D	A	H
+																		
K →	F	I	L	E	F	I	L	E	F	I	L	E	F	I	L	E	F	I
C →	**H**	**E**	**C**	**W**	**N**	**U**	**Y**	**X**	**R**	**A**	**P**	**S**	**J**	**P**	**T**	**H**	**F**	**P**

Table 2. Encryption results using Stream Cipher $C=P_{Bin} \oplus K_{Bin}$

Odd Locations	1	3	5	7	9	11	c13	15
Plaintext →	**O**	**A**	**D**	**D**	**E**	**A**	**Y**	**I**
Ascii equivalent	**79**	**65**	**68**	**68**	**69**	**65**	**89**	**73**
P_{Bin} →	1001111	1000001	1000100	1000100	1000101	1000001	1011001	1001001
⊕								
K_{Bin} →	0110010	0011110	0001110	1110001	0110010	0011110	0001110	1110001
C_{Bin} →	1111101	1011111	1001010	0110101	1110111	1011111	1010111	0111000
Ascii equivalent	125	95	74	53	119	95	87	56
Ciphertext→	**}**	**_**	**J**	**5**	**W**	**_**	**W**	**8**

Odd Locations	17	19	21	23	25	27	29	31	33
Plaintext →	**E**	**B**	**F**	**R**	**T**	**E**	**R**	**E**	**T**
Ascii equivalent	**69**	**66**	**70**	**82**	**84**	**69**	**82**	**69**	**84**
P_{Bin} →	1000101	1000010	1000110	1010010	1010100	1000101	1010010	1000101	1010100
⊕									
K_{Bin} →	1001001	1001001	0001110	1110001	1001001	1001001	0001110	1110001	1001001
C_{Bin} →	0001100	0001011	1001000	0100011	0011101	0001100	1011100	0110100	0011101
Ascii equivalent	12	11	72	34	29	12	92	52	29
Ciphertext→	♀	♂	**H**	**#**	**↔**	♀	\	**4**	**↔**

Ciphertext:	**H**	**}**	**E**	**_**	**C**	**J**	**W**	**5**	**N**	**w**	**U**	**_**	**Y**	**W**	**X**	**8**	**R**	♀
	A	♂	**P**	**H**	**S**	**#**	**J**	**↔**	**P**	♀	**T**	\	**H**	**4**	**F**	**↔**	**P**	

In this example, the repeated random binary numbers 1001001 occurred to fall the places of repeated characters, accounting for the repeated ciphertext character ♀ and such repeating is highly unlikely.

6. COMPARISON WITH THE CONVENTIONAL COMBINATION METHODS

Most traditional combination ciphers combine substitution ciphers with transposition cipher. In this section we will give a brief comparison between traditional combination ciphers and our proposed technique.

The existing combination cipher is based on with use of classical ciphers only, i.e., combining Caesar cipher with rail fence cipher[12,13]. This type of cipher makes the detection and decryption processes are very easy cipher. Also, it is a very weak cipher to Cryptanalyze using frequency attack. Furthermore, in the classical cipher there is no using to random binary key. While in our proposed work we combined classical ciphers, i.e., Vigenere method, with moderns ones, i.e., Stream cipher, makes the encryption and decryption processes very difficult in absence of a secret binary random key which improve the security of data.

7. CONCLUSION

Vigenere cipher regard as simplest and weakest method, that mean it is very easy to detect by intruder or attacker. To overcome the limitations of this method, we propose a new algorithms which includes combining Vigenere substitution cipher with Stream cipher. We notice that repeated portions of plaintext always encrypted with the different portion of the keyword or binary key, because we encipher the letters in odd location with stream cipher and the letters in even locations with Vigenere cipher, result in different ciphertext segments, that mean proposed algorithm hides the relationship between

the Ciphertext and Plaintext, and makes the cryptanalysis more difficult. On the other side, when we encipher capital and small letters, the final Ciphertext may be contains different characters not only letters. Furthermore, the proposed combination method enhance the security of Vigenere method and make the detection process not easy, because the Stream cipher relatively regards as unbreakable cipher**.**

8. FUTURE STEPS

The binary key value consider as an essential part in encryption process. In our work we use random binary numbers of key with different letters of Plaintext but the best thing is using different binary key values with long period for Encrypting and Decryption process which help in hiding the correlation between the Ciphertext and plaintext, this make Ciphertext breaking process more complex and the above algorithm more efficient.

9. REFERENCES

[1] Stalling W. "Network Security Essentials (Applications and Standards)", Pearson Education, 2004.

[2] Menezes A. J., Oorschot P. C. and Vanstone S. A. handbook of applied cryptography, CRC Press, 1996.

[3] Paar C. and Pelzl J. 2010, Understanding Cryptography, Springer-Verlag Berlin Heidelberg.

[4] Phaneendra H. D. and Srikantaswamy S.G. "A Cipher Design using the Combined Effect of Arithmetic and Logic Operations with Substitutions and Transposition Techniques", International Journal of Computer Applications,2011, Vol. 29, No.8, pp 34-36.

[5] Saroha V. and Dhull S. " Enhancing Security of One Time Pad Cipher by Double Columnar Transposition Method", International Journal of Advanced Research in Computer Science and Software Engineering, 2013, Vol. 3, Issue 3, pp 692-694.

[6] Saeed F. and Rashid M. "Integrating Classical Encryption with Modern Technique", IJCSNS International Journal of Computer 280 Science and Network Security, 2010, Vol.10, No.5, pp 280-285.

[7] http://www.simonsingh.net/The_BlackChamber/cracking_ to`ol.

[8] http://www.simonsingh.net/The_Black_Chamber/vigenere_cipher.html.

[9] Albrecht Beutelspacher: "Cryptology: an introduction to the art and science of enciphering".

[10] http://illuminations.nctm.org/LessonDetail.aspx?ID=L6-18.

[11] http://www.counton.org/explorer/codebreaking/vigenere-cipher.php.

[12] Singh A., Nandal A. and Malik S. "Implementation of Caesar Cipher with Rail Fence for Enhancing Data Security", International Journal of Advanced Research in Computer Science and Software Engineering, 2012, Vol. 2, Issue 12.

[13] Mishra A. "ENHANCING SECURITY OF CAESAR CIPHER USING DIFFERENT METHODS", International Journal of Research in Engineering and Technology, 2013, Vol. 02 Issue 09.