Int. J. Nonlinear Anal. Appl. 12 (2021) No. 2, 447-454
ISSN: 2008-6822 (electronic)
http://dx.doi.org/10.22075/ijnaa.2021.5071

A robust encryption technique using enhanced Vigenère cipher

Hazim Noman Abed[a], Zainab Mohammed Ali[a,*], Ahmed Luay Ahmed[b]

[a]*Computer Science Department, College of Science, University of Diyala, Diyala, Iraq.*
[b]*Supervision and Scientific Education Apparatus, International Accreditation Department, Ministry of Higher Education.*

(Communicated by Madjid Eshaghi Gordji)

Abstract

A lot of data in this world are very important and no matter how simple it can be. Hence the number of data conveyed through the internet still increasing due to the rapid development of computer technology. In order to save the data over the internet, cryptography is a technique for conveying information securely between two parties without interference from outside elements. The Vigenère cipher is a technique of encrypting alphabetic text via using a sequence of different Caesar ciphers depend on the letters of a keyword. It is a simple form of polyalphabetic replacement. In this paper, the traditional way for the Vigenère method is enhanced by using two keys for text encryption. The first key is used to format the table of the alphabet (26 characters) and second keys are used to encrypt the plain text like the original Vigenère cipher. The result shows the proposed method is efficient and stronger against the kasiski and Friedman attack to find the length of the key.

Keywords: Cryptography, Vigenère cipher, polyalphabetic, encryption and decryption

1. Introduction

A lot of data in this world are very important and no matter how simple it can be. Hence the number of data conveyed through the internet still increasing due to the fast development of computer technology. As a result, the transmission of secret data through public channels in a safe way has become a shared interest in both research and academic fields [12]. Many ways to security and applications, from safe commerce and payments to private communications and password protection. Cryptography is a necessary aspect of protecting communications [3, 10].

*Corresponding author
Email addresses: Hazim_ numan@sciences.uodiyala.edu.iq (Hazim Noman Abed), zainab_ ml@yahoo.com (Zainab Mohammed Ali), ahmed.qacc@gmail.com (Ahmed Luay Ahmed)

Received: March 2021 *Accepted:* April 2021

internet cryptography is a technique for conveying information securely between two parties without interference from outside elements. Cryptography contains an algorithm and a key-value to change the information into a format that is incomprehensible to anybody excluding the participants. Whenever we need to share some information with somebody the same algorithm can use with different key values because is difficult to create a new algorithm in every communication process. As a result, if the algorithm was known to the outside elements, they would not be able to get the message without any information related to the key [8].

2. Vigenère Cipher

Vigenère cipher is a technique for encoding alphabetical text using a sequence of different Caesar ciphers based on the letters of the keyword. It is an easy form of multi-alphabetic replacement [2, 6]. The Cipher spoils the statistics of a simple Caesar cipher by using several Caesar ciphers. The method is named referring to its inventor, Blaise de Vigenère from France in the 16th century, and it was considered a significant and unbreakable method for 300 years. In 1854 Charles Babbage have broken some variables in Vigenère Cipher and did not publish his work, but 1863 Friedrich Kasiski published a full account of how to broke down the Vigenère Cipher, without any knowledge of either the key or the plain text[5, 12].
The cipher step achieved by a Caesar cipher is often combined as part of complex schemes, such as the Vigenère cipher, and still has a recent implementation in the ROT13 system which is a particular case of the Caesar cipher. In the alphabet, it is a simple letter replacement cipher that replaces a letter with the 13th letter after it. As with all alternate ciphers for the single alphabet, the Caesar cipher is easily broken and in modern practice, it does not fundamentally provide a secure connection. There is one major weakness in Vigenère Cipher's security. And this is the fact that the key is being duplicated. In the nineteenth century, kasiski broke down Vigenère's cipher is based on the number of iterations. In ciphertext, the number of iterations means the number of times that the trigrams occurred [5].

3. Related Works

Aized et al. [1] proposed a technique to overcome Vigenère cipher problems against Kasiski and Friedman attacks. In this proposed approach, eight tables are used. In each table, each alphanumeric character represents a different numeric value. While the traditional style alphabet has a fixed numeric value. In the traditional method, plain text is considered as alphabetical sequences without any spaces between them. It may make a problem for the receiver to read the message by entering spaces between the words and the receiver needs to guess the correct place to insert a space in plain text that has been decrypted. This paper enhanced this problem by introducing a dissimilar numeric value for space in all tables.

Senthil et al. [9] some new additions technique of Vigenère and Caser cipher were introduced using some rigorous mathematical tools that employ a key factor, their primitive roots, and their generators. Changes and modifications made in both cryptographic methods are not uniform and track a specific scientific process.

Gerhana et al. [4] Design digital image applications using the Vigenère chipper algorithm. In this research paper, it showed good results with dissimilar digital image data capabilities. Using Vigenère encryption is successful in securing data in the form of digital image data, therefore cryptographic encryption methods can be used for oral digital data acquisition, although many encryption methods can be used to secure digital image data such as Vigenère methods is one of them. Everybody can

use this digital image for security applications well.
Saraswat et al [8] comprised the many encryption methods available. It mainly emphasizes the polyalphabetic encoding methods and the Vigenère table. In this research paper, authors extend the Vigenère table by including the numbers in the table so that digital data can also be encrypted using the new proposed table. It also decreases the size of plain text, if there are numbers in plain text and also makes cryptographic analysis a hard task

4. Proposed technique

The Vigenère method is simple and unfortunately still often used. This is why it is a good and interesting candidate for discussing a few problems in cryptanalysis. for that, it must find another way to use this method to make it more secure than before. In this paper, the traditional way for the Vigenère method is enhanced by using two keys for text encryption.

4.1. Encryption Method

In this cipher, two keys make substitution rules. The first key is used to format the table of the alphabet (26 characters) and second keys are used to encrypt the plain text like the original Vigenère cipher. A second keyword is repeated so that the total length is equal to that of the plaintext. The first and second keys are used to create a set of a grid of Vigenère table letters.
Steps for encryption process are:

1. In the first row, the keyword (cipher) is used as the first key and then followed it by the remaining letters without repeating. For example (key1: cipher) which is written as following c, i, p, h, e, r, and then a, b, (don't write c because we write it before), d, (don't write e because we write it before),f,g and so on until we finish all 26 letters
2. The next step is to set the "cryptography" as the second key in the first column. Illustrated in figure1.
3. In the second row, as shown in figure 1, we start with the first letter in the second key and continue with the same order as the first row. In our example: the first letter in key1 = the first letter in key2, therefore row1 = row2.
4. In row3, the first letter is r, and in the first row after r is a,b, d, f, g, j,. . . .,z because in row two after r letter is a letter, therefore we will write all and add c, I, p, h and e to complete 26 letters.
5. We will continue until complete all rows depending on the length of the second key.

For example, suppose the plaintext is COMPUTER SCIENCE DEPARTMENT and the key 1 is CIPHER and key 2 is CRYPTOGRAPHY. Then, the key 2 must be repeated as follows:
P.T: COMPUTER SCIENCE DEPARTMENT. . . . . (25 LETTERS)
K2: CRYPTOGRAPHY CRYPTOGRAPHY C . . . . . .(25 LETTERS)
Now removing all spaces and punctuation, and dividing the plaintext according to the size of the second key. As a result, the above plaintext and second key become as follow:

P.T	C	O	M	P	U	T	E	R	S	C	I	E	N	C	E	D	E	P	A	R	t	M	E	N	T
K2	C	R	Y	P	T	O	G	R	A	P	H	Y	C	R	Y	P	T	O	G	R	A	P	H	Y	C

Now for encryption, take the 1st letter in the plaintext and 1st corresponding letter in the second key, use the plaintext letter as the row index, and the second key letter as a column index. And take the 2nd letter in the plaintext with 2nd corresponding letter in the second key, respectively, and

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	C	I	P	H	E	R	A	B	D	F	G	J	K	L	M	N	O	Q	S	T	U	V	W	X	Y	Z
1	C	I	P	H	E	R	A	B	D	F	G	J	K	L	M	N	O	Q	S	T	U	V	W	X	Y	Z
2	R	A	B	D	F	G	J	K	L	M	N	O	Q	S	T	U	V	W	X	Y	Z	C	I	P	H	E
3	Y	Z	C	I	P	H	E	R	A	B	D	F	G	J	K	L	M	N	O	Q	S	T	U	V	W	X
4	p	H	E	R	A	B	D	F	G	J	K	L	M	N	O	Q	S	T	U	V	W	X	Y	Z	C	I
5	T	U	V	W	X	Y	Z	C	I	P	H	E	R	A	B	D	F	G	J	K	L	M	N	O	Q	S
6	O	Q	S	T	U	V	W	X	Y	Z	C	I	P	H	E	R	A	B	D	F	G	J	K	L	M	N
7	G	J	K	L	M	N	O	Q	S	T	U	V	W	X	Y	Z	C	I	P	H	E	R	A	B	D	F
8	R	A	B	D	F	G	J	K	L	M	N	O	Q	S	T	U	V	W	X	Y	Z	C	I	P	H	E
9	A	B	D	F	G	J	K	L	M	N	O	Q	S	T	U	V	W	X	Y	Z	C	I	P	H	E	R
10	P	H	E	R	A	B	D	F	G	J	K	L	M	N	O	Q	S	T	U	V	W	X	Y	Z	C	I
11	H	E	R	A	B	D	F	G	J	K	L	M	N	O	Q	S	T	U	V	W	X	Y	Z	C	I	P
12	y	Z	C	I	P	H	E	R	A	B	D	F	G	J	K	L	M	N	O	Q	S	T	U	V	W	X

Figure 1: Proposed technique

the entry at the row-column intersection is the letter in the ciphertext. When the first block was completed, pick the next plain text letter with the second key letter in the second block because we divided the size of blocks according to the second key size.
As shown in figure 2 the 1st letter in the plaintext is C and its corresponding letter in the second key is C. This means that the row of C and the column of C are used, and the entry C at the intersection is the encrypted result. And the 2nd letter in the plaintext is O and its corresponding letter in the second key is R, this means that the encryption result is V.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	C	I	P	H	E	R	A	B	D	F	G	J	K	L	M	N	O	Q	S	T	U	V	W	X	Y	Z
1	C	I	P	H	E	R	A	B	D	F	G	J	K	L	M	N	O	Q	S	T	U	V	W	X	Y	Z
2	R	A	B	D	F	G	J	K	L	M	N	O	Q	S	T	U	V	W	X	Y	Z	C	I	P	H	E
3	Y	Z	C	I	P	H	E	R	A	B	D	F	G	J	K	L	M	N	O	Q	S	T	U	V	W	X
4	p	H	E	R	A	B	D	F	G	J	K	L	M	N	O	Q	S	T	U	V	W	X	Y	Z	C	I
5	T	U	V	W	X	Y	Z	C	I	P	H	E	R	A	B	D	F	G	J	K	L	M	N	O	Q	S
6	O	Q	S	T	U	V	W	X	Y	Z	C	I	P	H	E	R	A	B	D	F	G	J	K	L	M	N
7	G	J	K	L	M	N	O	Q	S	T	U	V	W	X	Y	Z	C	I	P	H	E	R	A	B	D	F
8	R	A	B	D	F	G	J	K	L	M	N	O	Q	S	T	U	V	W	X	Y	Z	C	I	P	H	E
9	A	B	D	F	G	J	K	L	M	N	O	Q	S	T	U	V	W	X	Y	Z	C	I	P	H	E	R
10	P	H	E	R	A	B	D	F	G	J	K	L	M	N	O	Q	S	T	U	V	W	X	Y	Z	C	I
11	H	E	R	A	B	D	F	G	J	K	L	M	N	O	Q	S	T	U	V	W	X	Y	Z	C	I	P
12	y	Z	C	I	P	H	E	R	A	B	D	F	G	J	K	L	M	N	O	Q	S	T	U	V	W	X

Figure 2: Proposed technique example

Repeating this process until all plaintext letters are processed table 1, the ciphertext is :

Table 1: Ciphertext for proposed technique example

P.T	C	O	M	P	U	T	E	R	S	C	I	E	N	C	E	D	E	P	A	R	t	M	E	N	T
K2	C	R	Y	P	T	O	G	R	A	P	H	Y	C	R	Y	P	T	O	G	R	A	P	H	Y	C
C.T	C	V	K	E	L	F	M	G	Y	P	E	P	N	R	P	G	X	S	O	G	Z	O	B	L	T

4.1.1. Encryption Using Algebraic Description

Vigenère can also view algebraically. If the 26 letters are taken to be the numbers 0–25, and addition perform modulo 26, then Vigenère encryption using the key K can be written [7].
$Ci = (Pi + Ki)$ mod 26.
Table 2 below is to understand a mathematical method.

Table 2: Vigenère Cipher mathematical method

plaintext	C	O	M	P	U	T	E	R	S	C	I	E	N	C	E	D	E	P	A	R	T	M	E	N	T
Numerical plaintext	0	16	14	2	20	19	4	5	18	0	1	4	15	0	4	8	4	2	6	5	19	14	4	15	19
2^{nd} key	C	R	Y	P	T	O	G	R	A	P	H	Y	C	R	Y	P	T	O	G	R	A	P	H	Y	C
Numerical 2^{nd} key	0	5	24	2	19	16	10	5	6	2	3	24	0	5	24	2	19	16	10	5	6	2	3	24	0
Numerical ciphertext using Algebraic	0	21	12	4	13	9	14	10	24	2	4	2	15	5	2	10	23	18	16	10	25	16	7	13	19
Ciphertext	C	V	K	E	L	F	M	G	Y	P	E	P	N	R	P	G	X	S	O	G	Z	O	B	L	T

As shown in table 1 first row is the plaintext "COMPUTER SCIENCE DEPARTMENT", the second row is the numerical representation of the plaintext as we created before. The third row is the keyword "cryptography" which is repeated to fill all columns; the fourth row is the numerical representation of 2nd key. The fifth row is the result of the mathematical equation:
$Ci = (Pi + Ki)$ mod 26
According to our arrangement, $C1 = (P1 + K1)$ mod 26
$C1 = (0 + 0)$ mod 26
$C1 = 0$, which represents letter C.
$C2 = (P2 + K2)$ mod 26
$C2 = (16 + 5)$ mod 26
$C2 = 21$, which represents letter V. and so on.
Figure 3 explain proposed technique example using encryption mathematical equation.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
	C	I	P	H	E	R	A	B	D	F	G	J	K	L	M	N	O	Q	S	T	U	V	W	X	Y	Z
1	C	I	P	H	E	R	A	B	D	F	G	J	K	L	M	N	O	Q	S	T	U	V	W	X	Y	Z
2	R	A	B	D	F	G	J	K	L	M	N	O	Q	S	T	U	V	W	X	Y	Z	C	I	P	H	E
3	Y	Z	C	I	P	H	E	R	A	B	D	F	G	J	K	L	M	N	O	Q	S	T	U	V	W	X
4	p	H	E	R	A	B	D	F	G	J	K	L	M	N	O	Q	S	T	U	V	W	X	Y	Z	C	I
5	T	U	V	W	X	Y	Z	C	I	P	H	E	R	A	B	D	F	G	J	K	L	M	N	O	Q	S
6	O	Q	S	T	U	V	W	X	Y	Z	C	I	P	H	E	R	A	B	D	F	G	J	K	L	M	N
7	G	J	K	L	M	N	O	Q	S	T	U	V	W	X	Y	Z	C	I	P	H	E	R	A	B	D	F
8	R	A	B	D	F	G	J	K	L	M	N	O	Q	S	T	U	V	W	X	Y	Z	C	I	P	H	E
9	A	B	D	F	G	J	K	L	M	N	O	Q	S	T	U	V	W	X	Y	Z	C	I	P	H	E	R
10	P	H	E	R	A	B	D	F	G	J	K	L	M	N	O	Q	S	T	U	V	W	X	Y	Z	C	I
11	H	E	R	A	B	D	F	G	J	K	L	M	N	O	Q	S	T	U	V	W	X	Y	Z	C	I	P
12	y	Z	C	I	P	H	E	R	A	B	D	F	G	J	K	L	M	N	O	Q	S	T	U	V	W	X

Figure 3: Proposed technique example using encryption mathematical equation

This is the same Equation in the original Vigenère cipher. But it's stronger because the numerical letters are different from the standard form. For example. In standard form as shown in table 2, the first cipher letter C equivalent 2 but in this example, it's equivalent 0. As well as for third cipher letter K which is equivalent 10 in standard form, but in this example, it's equivalent 12. Note that

the second cipher letter is V it equivalent 21 in this example, which is the same in standard form in table 3.

Table 3: Standard form

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
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

Creation of Vigenère table using two key are different with differ these keys from one example to another. These keys depend on the sender and receiver.

4.1.2. Result assessment

To prove the efficiency of the proposed method, the results were evaluated as show in figure 4, and using two keys proven that our proposed technique is stronger against the kasiski and Friedman attack to find the length of the key. The plain text used 13 letters, 7 letters repeated and 6 letters unique.

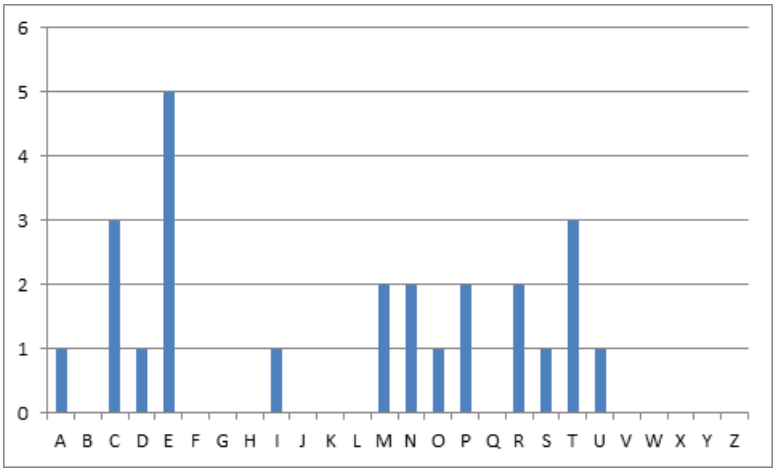

Figure 4: plain text ("COMPUTER SCIENCE DEPARTMENT")

In figure 5, after using K1, the result text using 17 letters, 8 letters repeated, and 9 letters are unique.

Finally, in figure 6 when using k2, the result text using 18 letters, only 5 letters repeated and 13 letters are unique.

4.2. Decryption Method

To decrypt the ciphertext the mathematical equation below is used [7].

$Pi = ((Ci - Ki) + 26) \bmod 26$

To applied this equation on example above the result shows the effectiveness of this equation in dealing with the results to reach the desired result, as shown in figure 7 :

$Pi = ((Ci - Ki) + 26) \bmod 26$

$P1 = ((C1 - K1) + 26) \bmod 26$

$P1 = ((0 - 0) + 26) \bmod 26$

$P1 = 0$

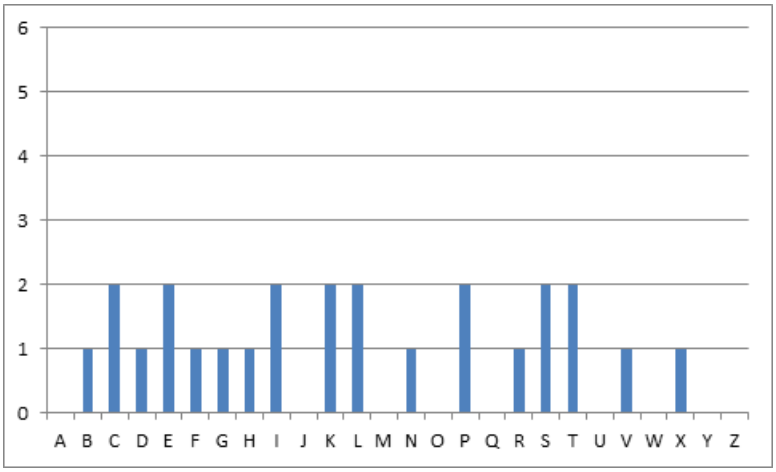

Figure 5: Vigenère cipher by one keyword

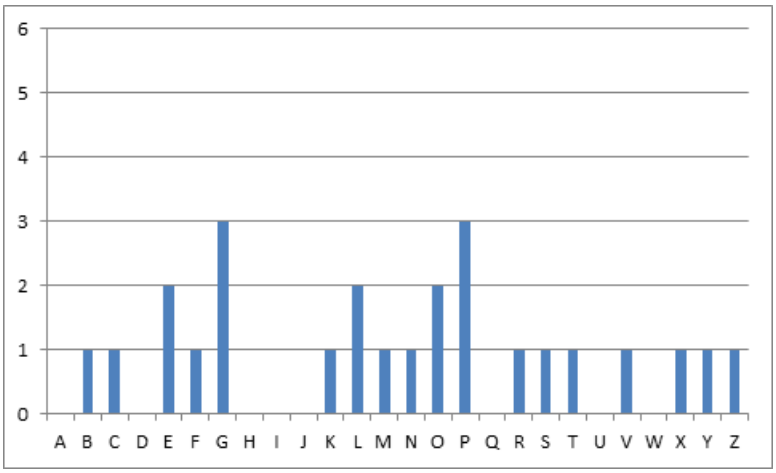

Figure 6: Vigenère cipher by two keywords

$P2 = ((C2 - K2) + 26) \bmod 26$
$P2 = ((21 - 5) + 26) \bmod 26$
$P2 = 16$
$P3 = ((C3 - K3) + 26) \bmod 26$
$P3 = ((12 - 24) + 26) \bmod 26$
$P3 = 14$

Plaintext	C	O	M	P	U	T	E	R	S	C	I	E	N	C	E	D	E	P	A	R	T	M	E	N	T
Numerical plaintext	0	16	14	2	20	19	4	5	18	0	1	4	15	0	4	5	4	2	6	5	19	14	4	15	19
2nd keyword	C	R	Y	P	T	O	G	R	A	P	H	Y	C	R	Y	P	T	O	G	R	A	P	H	Y	C
Numerical keyword	0	5	24	2	19	16	10	5	6	2	3	24	0	5	24	2	19	16	10	5	6	2	3	24	0
Numerical ciphertext using	0	21	12	4	13	9	14	10	24	2	4	2	15	5	2	10	23	18	16	10	25	16	7	15	19
Ciphertext	C	V	K	E	L	F	M	G	Y	P	E	P	N	R	P	G	X	S	O	G	Z	O	B	L	T

Figure 7: decryption method of Proposed technique

5. Conclusion

To overcome the limitations of Vigenere cipher we proposed an enhanced version of Vigenere cipher that is much secure against Kasiski and Friedman attacks. In this proposed technique, two keys make substitution rules. The first key is used to format the table of the alphabet (26 characters) and second keys are used to encrypt the plain text like the original Vigenère cipher. A second keyword is repeated so that the total length is equal to the plaintext. The first and second keys are used to create a set of a grid of Vigenère table letters. Results have been evaluated and proven to be effective against Cryptanalysis.

References

[1] A. Amin and U. Rasheed, *An enhanced Vigenère cipher for data security*, Int. J. Sci. Tech. Rese. 5(03) (2016).
[2] A. Bruen and M. Forcinito, *Cryptography, Information Theory, and Error-Correction: a Handbook for the 21st Century*, John Wiley & Sons, 2011.
[3] B. Forouzan, *Cryptography and network security*, McGraw-Hill, Inc, 2007.
[4] Y. Gerhana, E. Insanudin, U. Syarifudin and M. Zulmi, *Design of digital image application using Vigenère cipher algorithm*, In 2016 4th International Conference on Cyber and IT Service Management. IEEE. (2016) 1–5.
[5] Q. Kester, *A cryptosystem based on Vigenère cipher with varying key*, Int. J. Ad. Res. Comput. Engin. Tech. 1(10) (2012) 108–113.
[6] K. Martin, *Everyday cryptography*, The Australian Mathematical Society, 231(6) ((2012.
[7] S. Nasution, L. Ginting, M. Syahrizal and R. Rahim, *Data security using Vigenère cipher and Goldbach codes algorithm*, Int. J. Eng. Res. Technol, 6(1) (2017) 360–363.
[8] A. Saraswat, C. Khatri, P. Thakral and P. Biswas, *An extended hybridization of Vigenère and Caesar cipher techniques for secure communication*, Procedia Computer Sci. 92 (2016) 355–360.
[9] K. Senthil, K. Prasanthi and R. Rajaram, *A modern avatar of Julius Ceasar and Vigenère cipher*, IEEE International Conference on Computational Intelligence and Computing Research (2013) 1–3.
[10] A. Soofi, I. Riaz and U. Rasheed, *An enhanced Vigenère cipher for data security*, Int. J. Sci. Technol. Res, 5(3) (2016) 141–145.
[11] Z. Wang, S. Zhang, H. Liu and Y. Qin, *Single-intensity-recording optical encryption technique based on phase retrieval algorithm and QR code*, Optics Comm. 332 (2014) 36–41.
[12] R. Wobst, *Cryptology unlocked*, John Wiley & Sons.