Double Encryption, Decryption Process Using Graph Labeling Through Enhanced Vigenere Cipher

Journal of Physics: Conference Series **1362** (2019) 012023 doi:10.1088/1742-6596/1362/1/012023

DOUBLE ENCRYPTION, DECRYPTION PROCESS USING GRAPH LABELING THROUGH ENHANCED VIGENERE CIPHER

JAYA SHRUTHY V. N[1], V.MAHESWARI[2]

[1]Department of Mathematics

Research Scholar, Vels Institute of Science, Technology & Advanced Studies Chennai - 600117, India.

E-mail: jayashruthy12@gmail.com

[2] Department of Mathematics Associate Professor, Vels Institute of Science, Technology & Advanced Studies Chennai – 600117, India.

E-mail: maheswari.sbs@velsuniv.ac.in

Abstract--In this paper, we promote Double encryption process of our secret text initially through Difference Labeling of Signed Graphs and then through the Vigenere Cipher technique. Thus we propose Double encryption and their corresponding decryption process thereby making prediction of secret text complicated.
Keywords: Signed Graph, Difference labeling, Encryption, Decryption, Plaintext, Ciphertext.
2010 Mathematical subject Classification number: 05C78

1. Introduction

We perform Encryption process I of our Plaintext through Difference labeling of Signed Graphs obtaining Ciphertext-I. We then further proceed to Encryption process II by processing the Ciphertext-I through Enhanced version of Vigenere Cipher which is quite similar to the one proposed by [5] but with a slight variation which will be discussed in the Encryption process II eventually obtaining Ciphertext-II. The main idea behind our work is that the Ciphertext-I gets reduced in character compared to the original Plaintext thereby leaving less clue for decryption .Thus we implement double filtering of our Plaintext making it extremely difficult for Cryptanalysis.

A. Definition

A Graph G in which each edge is assigned either positive or a negative sign is termed as Signed Graph.

B. Definition

Let G be a graph. A Difference Labeling of Signed graph G is an injection l_i from the vertex set to the collection of all integers (positive and negative) for every edge in G defined by $\mathbf{l_i = v_{i+1} - v_i}$ for i =1 to n.

C. Definition

The original secret text from the sender to the receiver which requires to be transformed into some version is called Plaintext.

D. Definition

The required version of our plaintext is called Ciphertext.

E. Definition

The process of transforming plaintext to Ciphertext is called Encryption.

F. Definition

The transformation of Ciphertext to Plaintext is termed as Decryption.

G. Definition

The essential tool that encodes the Plaintext and also decodes the Ciphertext is called Key.

2. Plan of Work

We explore a concept in which the Plaintext from the sender is depicted in the form of vertices of a Signed Graph for which the sender defines a Difference labeling constituting our Encryption process I. The labels thus obtained from the Graph is the Ciphertext I which undergoes yet another encryption process II yielding Ciphertext II before it reaches the receiver. On the other hand the receiver well in advance is provided with two keys namely a key for deciphering the Ciphertext II enabling Decryption process I and another key for Decryption process II thereby revealing the Plaintext from the sender.

We now give a detailed report of our double Encryption and Decryption process.

3. ENCRYPTION PROCESS I

In Encryption process I use the concept of Graph labeling for obtaining our Ciphertext I. Let original message be Plaintext – I. We prepare Table - A by allocating two different numeric values both positive and negative for each letter to produce a Signed Graph by taking the positive numeric values as vertices for our Signed Graph. We define a Difference labeling for our Signed Graph whose labels will act as our Ciphertext I. Negative values are also allocated since we use difference labelling.

We define a Difference labelling $\mathbf{l_i = v_{i+1} - v_i}$ for the vertices i = 1, 2, 3,…..,n

TABLE 1: ENCRYPTION PROCESS I

0	1	2	3	4	5	6	7	8	9	10	11	12	13
a	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**
-26	-25	-24	-23	-22	-21	-20	-19	-18	-17	-16	-15	-14	-13

14	15	16	17	18	19	20	21	22	23	24	25	26
o	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**	**&**
-12	-11	-10	-9	-8	-7	-6	-5	-4	-3	-2	-1	

Let our **plaintext I** be: **caty&dogie**

Their corresponding positive numeric values are **2,0,19,24,26,3,14,6,8,4**

(we use commas to differentiate the numbers)

We construct a Signed graph with the above numeric values as vertices $v_1, v_{2,\ldots\ldots} v_i, v_{i+1\ldots..} v_n$.

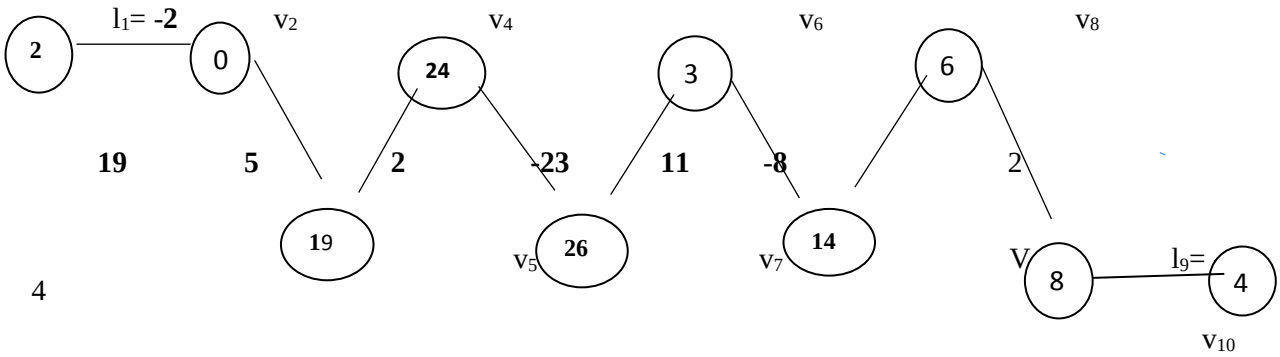

Fig. 1: Difference Labeling of Signed Graph

For the **difference labeling $l_i = v_{i+1} - v_i$** for vertices **i = 1 to 9** we obtain the following labels

$l_1 = v_2 - v_1$ gives 0 -2 = -2; $l_2 = v_3 - v_2$ gives 19 - 0 = 19 ; $l_3 = v_4 - v_3$ gives 24 -19 = 5

$l_4 = v_5 - v_4$ gives 26 - 24 = 2; $l_5 = v_6 - v_5$ gives 3 - 26 = -23 ; $l_6 = v_7 - v_6$ gives 14 - 3 = 11

$l_7 = v_8 - v_7$ gives 6 -14 = -8; $l_8 = v_9 - v_8$ gives 8 - 6 = 2 and $l_9 = v_{10} - v_9$ gives 4 - 8 = -4.

Hence for the labels received the corresponding letters from our TABLE I are as follows:

Labels	**-2**	**19**	**5**	**2**	**-23**	**11**	**-8**	**2**	**-4**
Ciphertext-I	**y**	**t**	**f**	**c**	**d**	**l**	**s**	**c**	**w**

This **Ciphertext-I** : **ytfcdlscw** becomes our **Plaintext II** for our **Encryption process II .** The beauty behind this concept is that our **Ciphertext I** characters are **reduced** in numbers when compared to **Plaintext I** characters by using This definitely plays a significant role in efficient encryption**.** Thus the mediator does not get clear clue regarding the actual plaintext I as the ciphertext I is reduced.

4. ENCRYPTION PROCESS II

ENHANCED VIGENERE CIPHER FOLLOWING CYCLIC PATTERN

The Historical Vigenere Cipher has one decided numeral or value corresponding to each alphabet. In [5] Enhanced Vigenere technique with eight reference tables were followed and the first letter followed their corresponding P_i ,C_i, K_i from table I and second letter from table II and so on. But we have adopted only Six Reference Tables as shown in Table B. We follow a cyclic pattern where P_i and C_i values for first letter is from Ref. Table I and K_i is from Ref. Table II , P_i and C_i values for second letter is from Ref. Table II and K_i is from Ref. Table III and each letter proceeds so on.

TABLE 2: ENCRYPTION PROCESS II

Ref. Tab. No	**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**	**26**
t_1	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

t_2	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
t_3	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
t_4	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
t_5	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
t_6	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

In Table - B the rows specifies Ref. Table number and columns denote the value for the alphabet.

For our encryption process – II six tables are sufficient in which every alphabet is assigned different numeric value in different tables. We use the same keys for both encryption and decryption process using Vigenere technique. We now discuss the encryption and decryption process by this technique.

5. ENCRYPTION PROCESS –II

Encryption Formula for Encryption process - II is as follows:

$C_i [t_i] = (P_i [t_i] + K_i [t_{i+1}]) \pmod{27}$ where i ranges from 1 to 6

Where **P_i** represents the plaintext to be encrypted

K_i represents the encryption key and **C_i** represents the ciphertext obtained.

In our proposed method we have length of alphabet 27 (ranging from 0 to 26), hence m = 27

Procedure for Encryption Process-II:

1. We repeat the key letters till it equals the plaintext if the former is shorter when compared to the latter.

2. For the first plaintext letter (P_1) the value will be from Ref. Table I (t_1) and the first keyletter (K_1) to be added will be from Ref. Table II (t_2).

3.The first ciphertext letter (C_1) follows a cyclic pattern by jumping back to Ref. Table I (t_1) which is obtained from the resultant (modulo 27) of $P_1 [t_1]$ and $K_1 [t_2]$.

4. Similarly the value of second ciphertext letter (C_2) follows Ref. Table II (t_2) calculated from (mod 27) of the resultant of $P_2 [t_2]$ and $K_2 [t_3]$.

5. We continue this process till our plaintext reaches Ref. Table VI (t_6). After which for the upcoming plaintext letters, key letters and ciphertext letters once again follows the same cyclic pattern starting from Ref. table I to VI.

Mathematically our cyclic **encryption process -II** can be expressed as:

$C_1 [t_1] = (P_1 [t_1] + K_1[t_2]) \pmod{27}$, $C_2 [t_2] = (P_2 [t_2] + K_2[t_3]) \pmod{27}$,

$C_3[t_3] = (P_3 [t_3] + K_3[t_4]) \pmod{27}$, $C_4 [t_4] = (P_4 [t_4] + K_4[t_5]) \pmod{27}$,

$C_5 [t_5] = (P_5 [t_5] + K_5[t_6]) \pmod{27}$, $C_6 [t_6] = (P_6 [t_6] + K_6[t_1]) \pmod{27}$

Where t_i indicates the Ref. Table number i =1 to 6.

Thus each P_i follows Ref. Table i, K_i follows Ref. Table i +1, C_i jumps back to Ref.Table i

Example

So for our **plaintext II**: **ytfcdlscw** let the key be **folk**

Table 3: Encryption process -II

Plain text II (P_i)	**y (23)**	**t (16)**	**f (0)**	**c (22)**	**d (21)**	**l (0)**	**s (17)**	**c (26)**	**w (17)**
Key (K_i)	**f (2)**	**o (9)**	**l (4)**	**k (1)**	**f (21)**	**o (13)**	**l (8)**	**k (5)**	**f (25)**
$P_i + K_i$(mod 27) (Ref .Table)	$t_1 + t_2 = 25$ (mod27)	$t_2 + t_3 = 25$ (mod 27)	$t_3 + t_4 = 4$ (mod 27)	$t_4 + t_5 = 23$ (mod 27)	$t_5 + t_6 = 42$ (mod 27)	$t_6 + t_1 = 13$ (mod 27)	$t_1 + t_2 = 25$ (mod 27)	$t_2 + t_3 = 31$ (mod 27)	$t_3 + t_4 = 42$ (mod 27)
C_i (Ref. Table)	**t_1**	**t_2**	**t_3**	**t_4**	**t_5**	**t_6**	**t_1**	**t_2**	**t_3**
Cipher text II	**&**	**b**	**j**	**d**	**y**	**y**	**&**	**h**	**u**

At the end of **encryption process II** the **ciphertext II** is **&bjdyy&hu** .

This **ciphertext II** undergoes decryption process I and II.

6. Decryption Process I

We first decrypt our **Ciphertext II** thus obtained using Enhanced Vigenere technique thereby arriving at **Plaintext II** which is our **Ciphertext I** for the next Decryption process - I using Graph Labeling.

Decrytion process – I is the exact opposite of our encryption process – II. We reach our plaintext II by subtracting the Ciphertext II from the same key used in Encryption process – I and applying mod 27 for the value thus obtained.

The formula is as follows:

$P_i[t_i] = (C_i [t_i] - K_i [t_{i+1}])$ (mod 27) where i ranges from 1 to 6

Mathematically our decryption process is as follows

$P_1 [t_1] = (C_1[t_1] - K_1 [t_2])$(mod 27), $P_2 [t_2] = (C_2 [t_2] - K_2 [t_3])$ (mod 27),

$P_3 [t_3] = (C_3 [t_3] - K_3 [t_4])$ (mod 27), $P_4 [t_4] = (C_4 [t_4] - K_4 [t_5])$ (mod 27),

$P_5 [t_5] = (C_5 [t_5] - K_5 [t_6])$(mod 27), $P_6 [t_6] = (C_6 [t_6] - K_6 [t_1])$ (mod 27)

Where t_i refers the table number i =1 to 6.

Table 4: Decryption Process -I

Cipher text II (C_i)	& (25)	b (25)	j (4)	d (23)	y (42)	y (13)	& (25)	h (31)	u (42)
Key(K_i)	f (2)	o (9)	l (4)	k (1)	f (23)	o (13)	l (8)	k (5)	f (25)
C_i - K_i (mod27)	t_1 -t_2 25-2 =23 (mod 27)	t_2 -t_3 25-9 =16 (mod 27)	t_3- t_4 4-4 = 0 (mod 27)	t_4- t_5 23-1 =22 (mod 27)	t_5 - t_6 15-23=8 (mod 27)	t_6 - t_1 13-13=0 (mod 27)	t_1 - t_2 2-58=17 (mod 27)	t_2 - t_3 31-5=26 (mod 27)	t_3 - t_4 42 - 25 =17 (mod 27)
P_i (Ref .Tab)	**t_1**	**t_2**	**t_3**	**t_4**	**t_5**	**t_6**	**t_1**	**t_2**	**t_3**
Plain text II	**y**	**t**	**f**	**c**	**d**	**l**	**s**	**c**	**w**

After **Decryption process I** our required **plaintext II** is **ytfcdlscw** from which **plaintext I** will be retrieved.

7. Decryption Process II

The **plaintext I** is percieved by the receiver by making use of the concept of Difference labeling $\mathbf{l_i = v_{i+1} - v_i}$ of Signed graph **for i = 1 to 9.**

The receiver is provided with Table A from which the labels for the **plaintext II** are obtained as enlisted below.

Plaintext II is **ytfcdlscw**

Corresponding plaintext II Labels: **-2, 19, 5, 2, -23, 11, -8, 2, -4.**

To find the corresponding vertices the receiver is handed over **Key II** .The Key II may be any of the vertices $v_1, v_2, \ldots\ldots, v_n$.

Let it be $\mathbf{v_1 = 2}$

Using $l_i = v_{i+1} - v_i$ for i = 1 we get $v_2 - v_1 = l_1 \rightarrow v_2 - 2 = -2 \rightarrow v_2 = -2+2 = 0$.

Similarly $v_3 - 0 = 19 \rightarrow v_3 = 19 + 0 = 19$; $v_4 - 19 = 5 \rightarrow v_4 = 5 + 19 = 24$

$v_5 - 24 = 2 \rightarrow v_5 = 24 + 2 = 26$; $v_6 - 26 = -23 \rightarrow v_6 = -23 + 26 = 3$

$v_7 - 3 = 11 \rightarrow v_7 = 11 + 3 = 14$; $v_8 - 14 = -8 \rightarrow v_8 = 14 - 8 = 6$

$v_9 - 6 = 2 \rightarrow v_9 = 2 + 6 = 8$; $v_{10} - 8 = -4 \rightarrow v_{10} = -4 + 8 = 4$

Thus we get the corresponding vertices for our labels as **2,0,19,24,26,3,14,6,8,4.**

These vertices values from the Table A is given by **caty&doggie** which is our original **Plaintext I** to the receiver.

8. Conclusion

In this paper we investigated a very secured method of double encryption and double decryption by combining the concepts of Graph labeling with Vigenere Cipher which is extremely difficult to perceive. Different types of Graph labeling techniques with other Cryptographic methods can be adopted for future studies to obtain even better encryption and decryption pattern.

9. References

[1]. J.A.Gallian,"A Dynamic Survey Of Graph labelings" The Electronic Journal Of Combinatorics, 2017.
[2]. J.BaskarBabujee,V.Vishnupriya "Encypting Numbers using Pair Labeling in path Graph", International Journal of Pure and Applied Mathematics ,Vol 114, No.2,2017,249 - 205.
[3]. S.Somasundaram and V. Ponraj ," Mean labeling of Graphs" National Academy of Science Letters, 26(2003), 210-213.
[4]. Rosa ,"On Certain Valuations of the vertices of a Graph", Theory of Graph, Gordon and Breach.N and Dunod Paris(1967),349-355.
[5]. Aized Amin Soofi, IrfanRiyaz, Umair Rasheed," An Enhanced Vigenere Cipher For Data Security" International Journal of scientific & Research Volume 5, Issue 03,March 2016 ISSN 2277-8616.
[6]. V.M.Chandrasekaran, B.Praba, A.Manimaran "Data Transfer using Complete Bipartite Graphs" IOP Conference Series: Material Science and Engineering,Volume 263, Computation And Information Technology.
[7]. M.Yamuna ,K.Karthika "Data Transfer Using Bipartite Graphs" International Journal Of Advance Research And Engineering" IJARSE,Vol. No. 4 February 2015.
[8]. Al- Amin Mohammed Aliyu, AbdulrahmanOlaniyan "VigenereCipher : Trends, Reviews and Possible Modifications" International Journal Of Computer Applications (0975-8887) Vol.135 – No.11 Feb 2016.
[9]. SaritaKumari, "A research Paper on Data on Cryptography Encryption and compression Techniques" International Journal Of Engineering and Computer Science ISSN :2319-7242 Vol 6, April 2017 .
[10]. RavindraBabuKallam, Dr. S, Udaiyakumar, Dr. A.VinayaBabu ,Md Abdul Razul, "An Enhanced Polyalphabetic Cipher using Extended Vigenere Cipher" International Journal of Advanced research in Computer Science,Vol 2,No.2, 2011,ISSN No.0976-5697.
[11]. KamilKulesza, ZbigniewKotulski "On Secret Sharing Of Graphs".
[12]. Shubam Agarwal, Anand Singh Uniyal " Prime Weighted Graph in cryptographic System For Secure Communication"International Journal of Pure and Applied Mathematics ,Vol 105, No.3,2015.
[13]. P.Amudha, A.C.CharlesSagayaraj, A.C.ShanthaSheela "An Application Of Cryptography In Graph Theory" International Journal of Pure and Applied Mathematics ,Vol 119, No.13, 2018, 375-383.