A Novel Approach by Using a New Algorithm: Wolf Algorithm as a New Technique in Cryptography

Basim Najim Al-din*
University of Diyala, Diyala, Iraq. E-mail: basim007@yahoo.com

Ahmad M. Manasrah
Yarmouk University, Irbid, Jordan.

Salam Abdulkhaleq Noaman
University of Diyala, Diyala, Iraq.

Received August 04, 2020; Accepted October 10, 2020
ISSN: 1735-188X
DOI: 10.14704/WEB/V17I2/WEB17069

Abstract

In order to develop the cryptographic systems, it must always find new techniques to construct the strong cryptosystem, the proposed method try to employ the nature and animals activates in their society to propose the new algorithm for new cryptosystem, depending completely on the behaver of the wolfs communications between each other's through howls to exchange the information between the wolf's group to determine the locations and for warning each other's against the dangers, in this paper propose a new algorithm through classify the characters of the message into groups and exchange the keys between the groups to be difficult on the cryptanalytics to follow the path of constructing the system, also using the different cryptanalysis techniques to evaluate the proposed algorithm.

Keywords

Wolfs Group, Howls, Cryptanalytics, Transposition Genetic Analysis.

Introduction

Wolf communication includes both elements of pre-programmed signals conveying information between strangers, and suitable signs learned during interactions with companies, information about individual identity is carried in howling and scent marking behavior of wolves. Howling provide information without revealing location, the wolves divide into groups each group communicate with other groups through cipher signals to communicate and warning each other against the dangers and risks [9,6,4,7].

In cryptography, there are two types of cryptosystem, namely the symmetric key cryptosystem and asymmetric key cryptosystem or the public key cryptosystem. The public key cryptosystems, in vogue today are the RSA, El-Gamal and the Elliptic curve cryptosystem. In this paper a new algorithm proposed which mimic the wolf's society, in order to make a strong cryptosystem to be more difficult against different types of attacks, and be complex to guess the original keys, that make process of cryptanalysis the secret message very hard and difficult [1].

Literature Review

Manasrah, A. M., & Al-Din, B. N.(2013) proposed an enhancement for the Caesar cipher method by using two private keys according to the character positions (even, odd), for the encryption and the decryption process. Then the private keys are mapped into one public key for send it to the recipient. The obtaining results are show that the new cryptosystem was inevitable to the cryptanalysis attack.[5]

Abed, B. N. A. D, & Noaman, S. A. (2019, September). proposed a new technique for developing the encryption process by using the mathematical term which is McLaurin series as a cryptosystem, then by using different cryptanalysis techniques, the results show that the proposed method was inevitable against the different attacks.[3]

Abed, B. N. A. D, et.al,(2013) proposed the new encryption technique to encrypt the text depending on the principle of indefinite integral, through using the constant of the integral and the order of the equation as a two keys, where the variable in the integration represent the character. The results show the cryptosystem is unbreakable through different types of cryptanalysis attack.[2]

Shaban, S. A., & Najim al-din, B. (2017) proposed a new technique to encrypt Arabic text through using the principle of integrals to produce high security to increasing the cipher complexity and make the process of f guessing the correct keys and correct plain text is difficult. [10]

Salam Abdulkhaleq Noaman, et. al (2013). proposed a method depending on the use of the complementary number that represent the key. The encrypted message is the series of numbers sent via the internet, then the receiver of the cipher text extract the plain text from the cipher through using the value of the complement.[8]

Abed, B. N. A. D., & Noaman, S. A. (2013) proposed a new method to encrypt data in an RGB color image format with the key and then send the secret message through internet.

The cipher text and the key are arranged in reverse mode every time there were a different arrangement depending on the agreement, that complicates the method [1]

Key Generation Technique

1- Choose a key for each wolf group, for example : k1 for group (A), k2 for group (B), … and so on, 26 keys for each wolf society

2- Choose a permutations for each m/n characters, where (m) is number of characters in the message, (n) number of wolf groups, at most 26 permutation in each wolf society.

3- Choose m/2 exchanges between wolf groups and keys where (m) is number of characters in the each wolf society.

4- Send keys, permutations and exchanges as a private keys to the receiver

5- Choose a public key (K) for all wolf groups

Encryption Process

1- Divide the message into wolf groups of characters WG(x)

2- Divide the message into wolf society WS(ch)

3- For each WS(ch) add the key into wolf groups [WG(x) + K]

4- Arrange the result from above step in the same order

5- Do the permutations for each WS(ch)

6- Exchange the keys between WG(x) as follows:

$$ch_a(WG(x_1)) \leftrightarrow ch_b(WG(x_2)) \rightarrow O[ch_a(WG(x_1))] \leftrightarrow O[ch_b(WG(x_2))]$$
$$\rightarrow k_b + O[ch_a(WG(x_1))] \leftrightarrow k_a + O[ch_b(WG(x_2))]$$

7- Exchange the characters positions in each WS(ch) as follows :

$$k_b + O[ch_a(WG(x_1))] \leftrightarrow k_a + O[ch_b(WG(x_2))] \rightarrow k_a + O[ch_b(WG(x_2))]$$
$$\leftrightarrow k_b + O[ch_a(WG(x_1))]$$

Add public key (K) to all wolf groups $k_m + \left[k_n + O\left(Ch(WG(x_n))\right)\right]$

8- The result is the wolf cipher text

Decryption Process

1- $k_m - k_m + \left[k_n + O\left(Ch(WG(x_n))\right)\right] mod\ 26$

2- Exchange the positions of characters for each WS(ch) as follows :

$k_b + O[ch_a(WG(x_1))] \leftrightarrow k_a + O[ch_b(WG(x_2))]$

$k_b - k_b + O[ch_a(WG(x_1))] \leftrightarrow k_a - k_a + O[ch_b(WG(x_2))] \rightarrow ch_a(WG(x_1)) \leftrightarrow$

3- $ch_b(WG(x_2))$

4- WG(x)+K-K=ch

5- Wolf plain text

Implementation

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

Key Generation

1- Keys= 1,2,3,4,5,6,7

2- Permutation=6,7,5,3,2,1,11,8,10,9,4,12

3- Exchange=1&6, 2&11, 3&4, 5&10, 7&12, 8&9

4- Public key=8

Encryption Process

1- Plain text = **GOOD MORNINGG**

2- **Wolf group (G)**= 6+1=7=H
Wolf group (O)=14+2=16=Q
Wolf group (D)=3+3=6=G
Wolf group (M)=12+4=16=Q
Wolf group (R)=17+5=22=W
Wolf group (N)=13+6=19=T
Wolf group (I)=8+7=15=P

3- **Result = HQQGQQWTPTHH**

4- **Permutations = QWQQQHHTTPGH**

5- **Exchange the keys inside wolf society as follows:**

$1\&6 \rightarrow Q \leftrightarrow H \rightarrow O \leftrightarrow G \rightarrow 14+1 \leftrightarrow 6+2 \rightarrow 15 \leftrightarrow 8 \rightarrow L \leftrightarrow I$

$2\&11 \rightarrow W \leftrightarrow G \rightarrow R \leftrightarrow D \rightarrow 17+3 \leftrightarrow 3+5 \rightarrow 20 \leftrightarrow 8 \rightarrow U \leftrightarrow I$

$3\&4 \rightarrow Q \leftrightarrow Q \rightarrow M \leftrightarrow O \rightarrow 12+2 \leftrightarrow 14+4 \rightarrow 14 \leftrightarrow 18 \rightarrow K \leftrightarrow S$

$5\&10 \rightarrow Q \leftrightarrow P \rightarrow O \leftrightarrow I \rightarrow 14+7 \leftrightarrow 8+2 \rightarrow 21 \leftrightarrow 10 \rightarrow V \leftrightarrow J$

$7\&12 \rightarrow H \leftrightarrow H \rightarrow G \leftrightarrow G \rightarrow 6+1 \leftrightarrow 6+1 \rightarrow 7 \leftrightarrow 7 \rightarrow H \leftrightarrow H$

$8\&9 \rightarrow T \leftrightarrow T \rightarrow N \leftrightarrow N \rightarrow 13+6 \leftrightarrow 13+6 \rightarrow 19 \leftrightarrow 19 \rightarrow T \leftrightarrow T$

6- **Exchange1=LUKSVIHTTJIH**

7- **Exchange2=IISKJLHTTVUH**

8- **Add public key=8 as follows :**

9- **Wolf group (I)**= 8+8=16 mod 25=16=Q
Wolf group (S)=18+8=26 mod 25=1=B
Wolf group (K)=14+8=22 mod 25=22=W
Wolf group (J)=21+8=29 mod 25=4=E
Wolf group (L)=15+8=23 mod 25=23=X
Wolf group (H)=7+8=15 mod 25=15=P
Wolf group (T)=19+8=27 mod 25=2=C

Wolf group (V)=21+8=29 mod 25=4=E
Wolf group (U)=20+8=28 mod 25=3=D

10- **Cipher wolf=QQBWEXPCCEDP**

Decryption Process

1- For the first character Q in the cipher wolf
Q=16-8=8 mod 25=8=I

2- Apply previous step for all characters in the cipher wolf, so the result will be **IISKJLHTTVUH**

3- Exchange the characters positions, the result will be **LUKSVIHTTJIH**

4- exchange the characters keys, the result will be **QWQQQHHTTPGH**

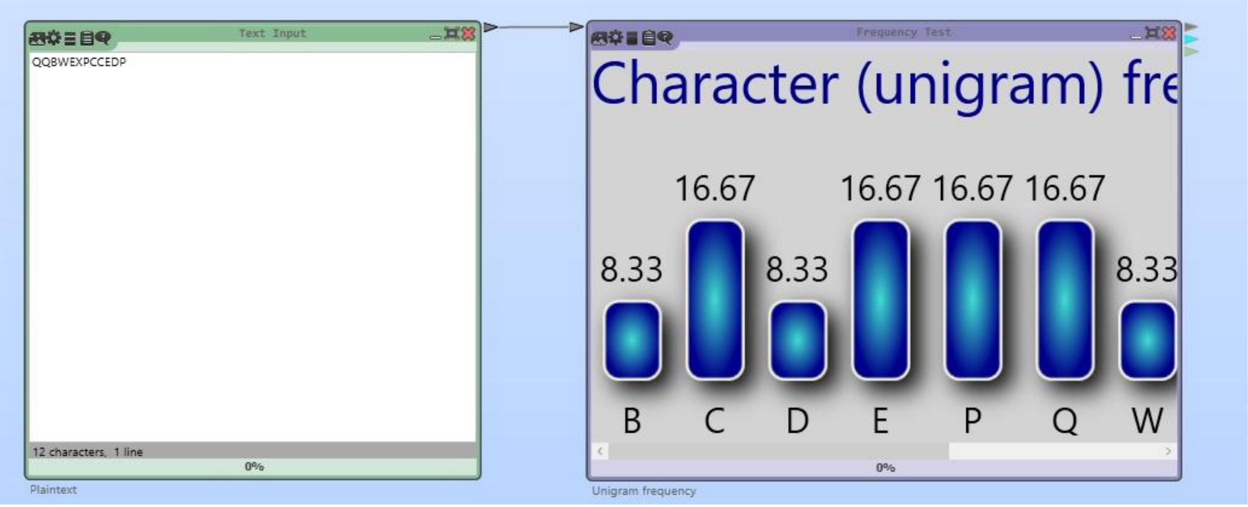
5- apply permutations for the characters, the result will be **HQQGQQWTPTHH**

6- for the first character H :- $WG(H) = 7 \rightarrow 7 - 1 = 6 = WG(G)$

7- apply for all characters in the same way, the result will be
The plain wolf= GOOD MORNINGG

Result and Discussion

In this paper many attacks were applied on the proposed algorithm to evaluate the strength and complexity of the new cryptosystem, all the results show that the cryptosystem was very hard to break and know the plain text from given cipher text, also the difficulty of cracking the secret keys. The results declared the strength of the new cryptosystem.



Text Input

QQBWEXPCCEDP

12 characters, 1 line

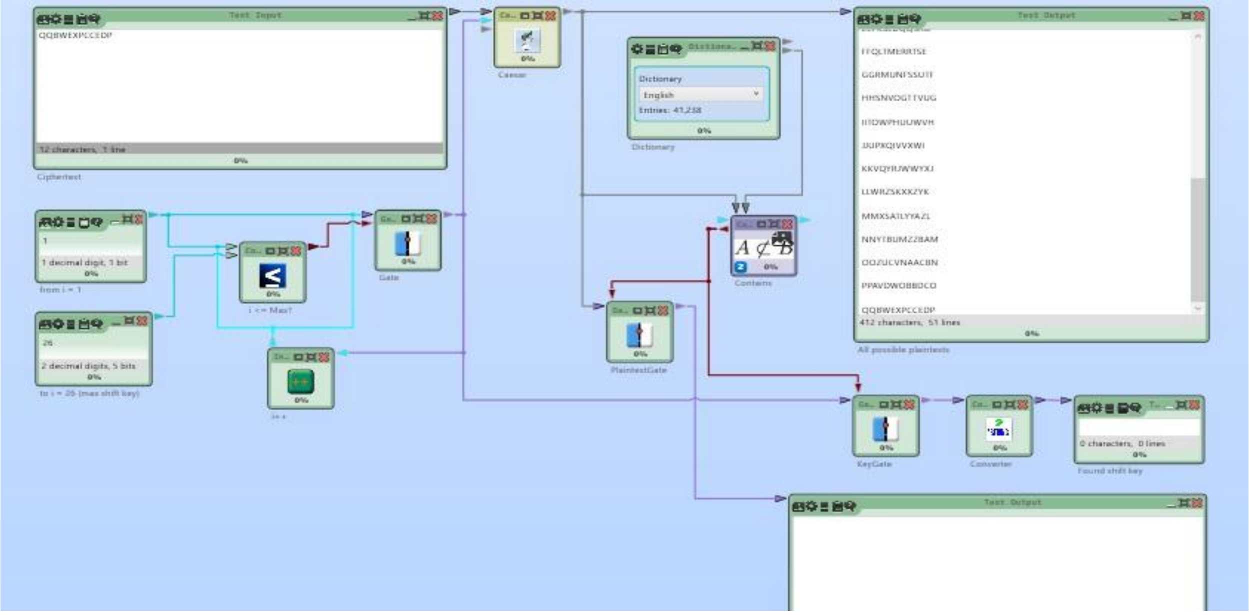
0%

Plaintext

Frequency Test

Figure 1 Frequency attack

The frequency attack applied on the proposed cryptosystem to extract the frequency of the characters in the message, but from the result of this attack it show that the cryptanalysis method doesn't succeeded as it showed in the figure (1).



```
QQBWEXPCCEDP
12 characters, 1 line
```

```
Dictionary
English
Entries: 41,238
```

```
1
1 decimal digit, 1 bit
```

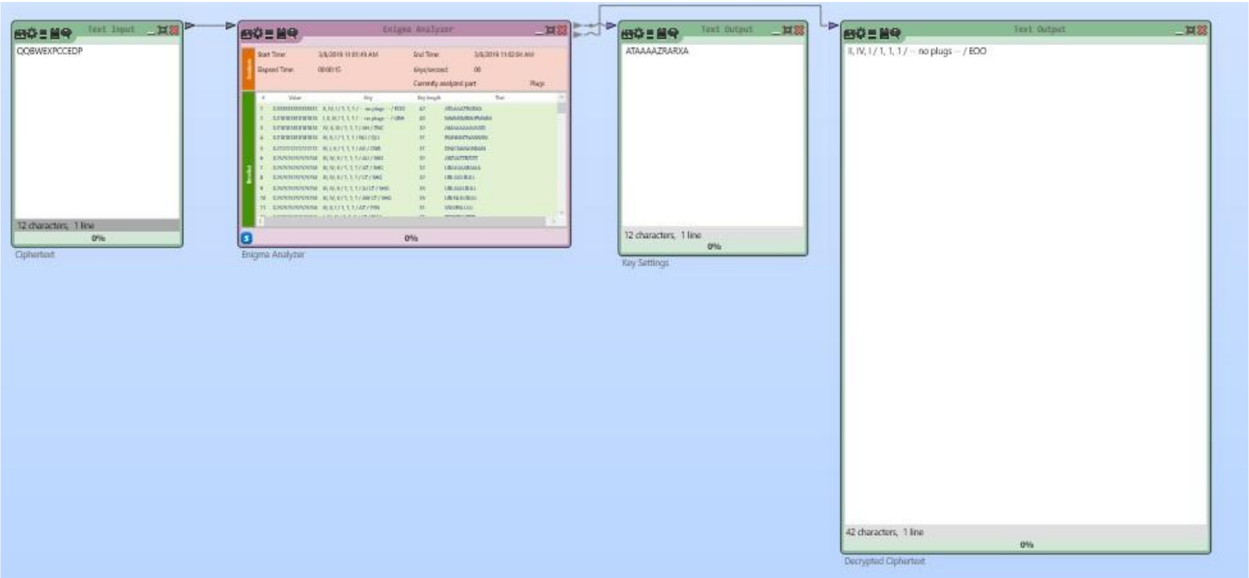
```
26
2 decimal digits, 5 bits
```

```
FFQLTMERRTSE
GGRMUNFSSUTF
HHSNVOGTTVUG
IITOWPHUUWVH
JJUPXQIVVXWI
KKVQYRJWWYXJ
LLWRZSKXXZYK
MMXSATLYYAZL
NNYTBUMZZBAM
OOZUCVNAACBN
PPAVDWOBBDCO
QQBWEXPCCEDP
412 characters, 51 lines
```

```
0 characters, 0 lines
```

Figure 2 Brute force attack

The second attack applied on the cipher text was the most powerful attack which I the brute force attack, in this attack all possible results will appear and then guess the correct one from these selections, but it fail in doing that in this cryptosystem as showing in figure (2).



```
QQBWEXPCCEDP
12 characters, 1 line
```

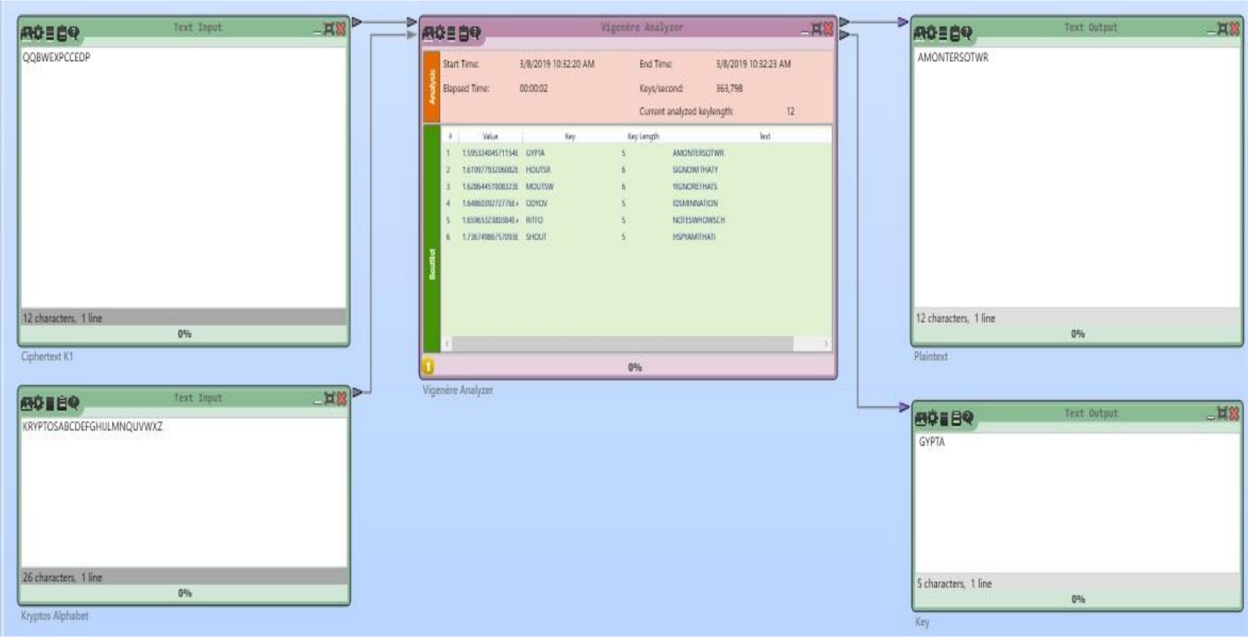
```
Start Time    3/8/2019 11:01:49 AM    End Time    3/8/2019 11:02:04 AM
Elapsed Time  00:00:15                Keys/second  00
                                      Currently analyzed part    Plugs
#   Value   Key   Key length   Text
```

```
ATAAAAZRARXA
12 characters, 1 line
```

```
II, IV, I / 1, 1, 1 / -- no plugs -- / EOO
42 characters, 1 line
```

Figure 3 Enigma analyzer

Through applying Enigma analyzer the results showed all attempted to obtain the plain text from cipher text but without any success in this type of encryption process as in Figure (3).

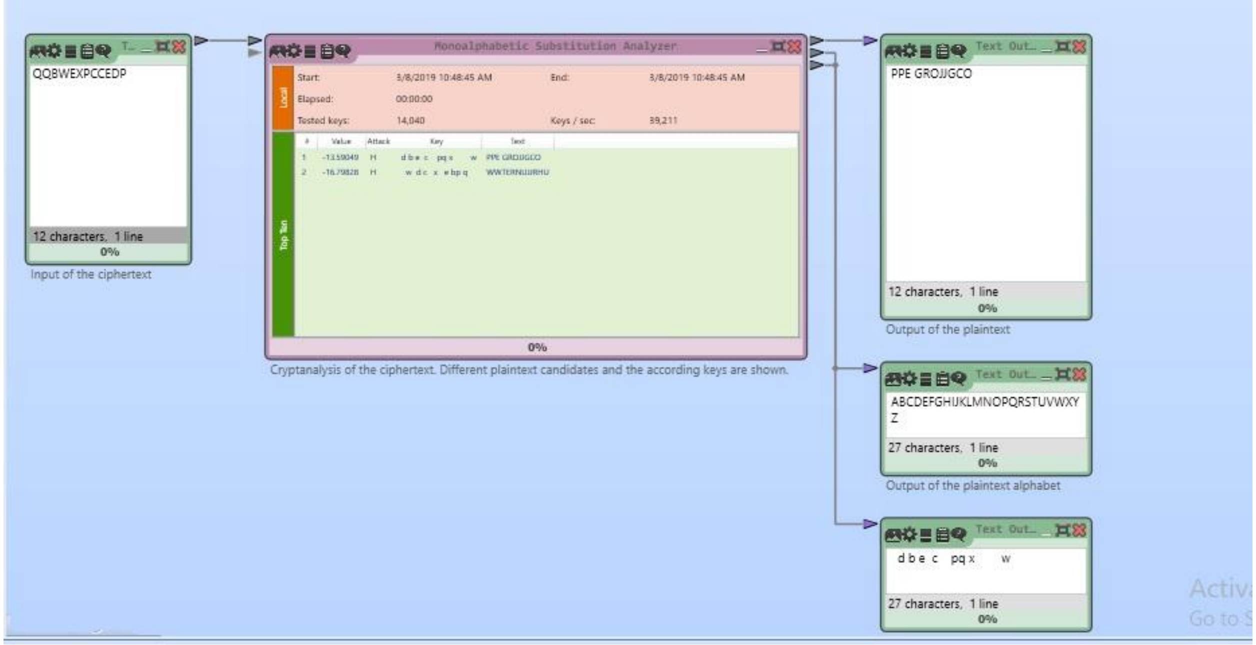


Start Time: 3/8/2019 10:32:20 AM
End Time: 3/8/2019 10:32:23 AM
Elapsed Time: 00:00:02
Keys/second: 363,798
Current analyzed keylength: 12

#	Value	Key	Key Length	Text
1	1.59532404571154E	GYPTA	5	AMONTERSOTWR
2	1.61097793206082E	HOUTSR	6	SIGNOWITHATY
3	1.62864451908323E	MOUTSW	6	YIGNORETHATS
4	1.64860092727766E+	ODYOV	5	IDSMINNATION
5	1.65965523803084E+	RITTO	5	NOTESWHOWSCH
6	1.73674986757093E	SHOUT	5	HSPYAMITHATI

Figure 4 Crypto K1 attack

Figure (4) show the crypto K1 attack on the cipher text of the proposed algorithm, the result of this type doesn't guess the plain text and the correct keys as showing.

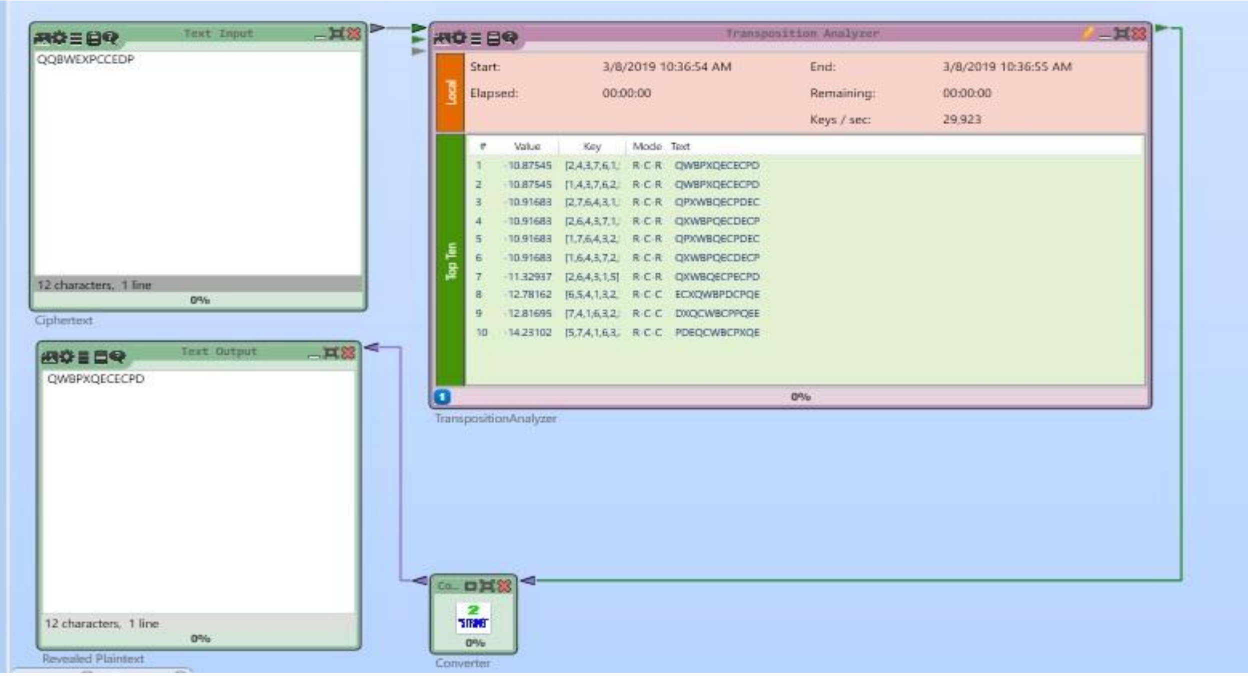


Start: 3/8/2019 10:48:45 AM
End: 3/8/2019 10:48:45 AM
Elapsed: 00:00:00
Tested keys: 14,040
Keys / sec: 39,211

#	Value	Attack	Key	Text
1	-13.59049	H	d b e c pq x w	PPE GROJJGCO
2	-16.79828	H	w d c x e bp q	WWTERNUJJRHU

Figure 5 Monoalphabitic substitution analysis

monoalphabitic substitution analysis applied on the proposed method in order to break the cipher text and extract the orginal text from the secret message, but the result showed the revers of that as in the figuer (5).



Text Input

QQBWEXPCCEDP

12 characters, 1 line

0%

Ciphertext

Transposition Analyzer

Start:	3/8/2019 10:36:54 AM	End:	3/8/2019 10:36:55 AM
Elapsed:	00:00:00	Remaining:	00:00:00
		Keys / sec:	29,923

#	Value	Key	Mode	Text
1	-10.87545	[2,4,3,7,6,1,	R-C-R	QWBPXQECECPD
2	-10.87545	[1,4,3,7,6,2,	R-C-R	QWBPXQECECPD
3	-10.91683	[2,7,6,4,3,1,	R-C-R	QPXWBQECPDEC
4	-10.91683	[2,6,4,3,7,1,	R-C-R	QXWBPQECDECP
5	-10.91683	[1,7,6,4,3,2,	R-C-R	QPXWBQECPDEC
6	-10.91683	[1,6,4,3,7,2,	R-C-R	QXWBPQECDECP
7	-11.32937	[2,6,4,3,1,5]	R-C-R	QXWBQECPECPD
8	-12.78162	[6,5,4,1,3,2,	R-C-C	ECXQWBPDCPQE
9	-12.81695	[7,4,1,6,3,2,	R-C-C	DXQCWBCPPQEE
10	-14.23102	[5,7,4,1,6,3,	R-C-C	PDEQCWBCPXQE

0%

TranspositionAnalyzer

Text Output

QWBPXQECECPD

12 characters, 1 line

0%

Revealed Plaintext

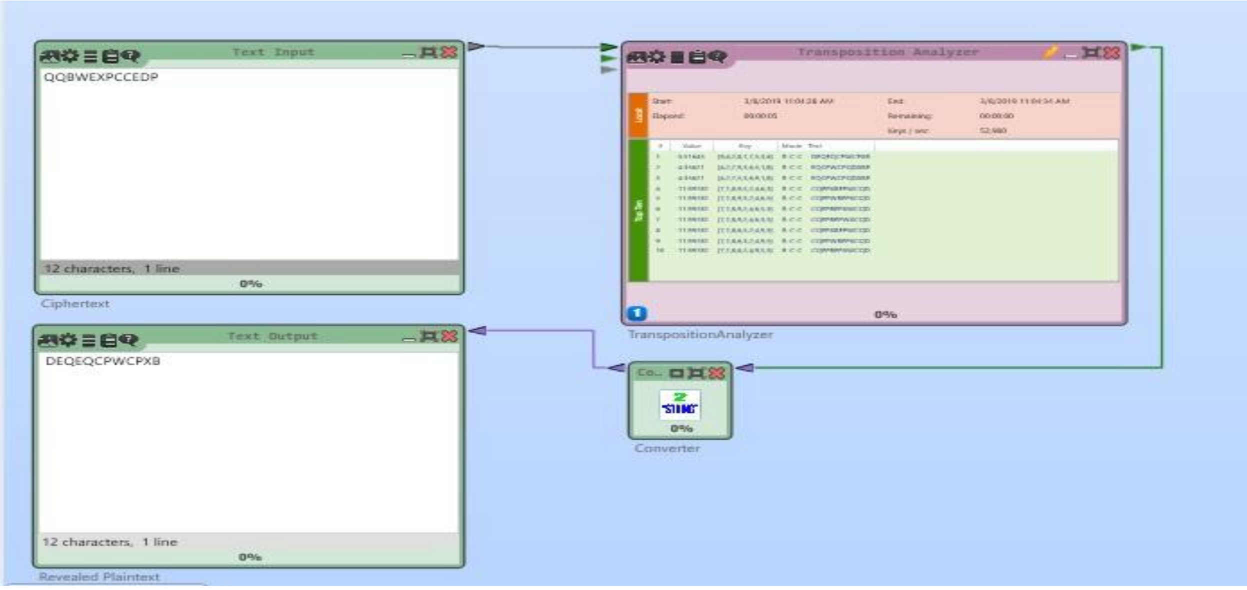
Co...

0%

Converter

Figure 6 Transposition brute- force analysis

Figure (6) showed the transposition brute-force analysis result to decrypt the cipher text, then through all possible results in this method no one of these results match the correct plain text.



Text Input

QQBWEXPCCEDP

12 characters, 1 line

0%

Ciphertext

Transposition Analyzer

Start:	3/8/2019 11:04:28 AM	End:	3/8/2019 11:04:34 AM
Elapsed:	00:00:05	Remaining:	00:00:00
		Keys / sec:	52,980

#	Value	Key	Mode	Text
1	[illegible]	[illegible]	R-C-C	[illegible]
2	[illegible]	[illegible]	R-C-C	[illegible]
3	[illegible]	[illegible]	R-C-C	[illegible]
4	[illegible]	[illegible]	R-C-C	[illegible]
5	[illegible]	[illegible]	R-C-C	[illegible]
6	[illegible]	[illegible]	R-C-C	[illegible]
7	[illegible]	[illegible]	R-C-C	[illegible]
8	[illegible]	[illegible]	R-C-C	[illegible]
9	[illegible]	[illegible]	R-C-C	[illegible]
10	[illegible]	[illegible]	R-C-C	[illegible]

0%

TranspositionAnalyzer

Text Output

DEQEQCPWCPXB

12 characters, 1 line

0%

Revealed Plaintext

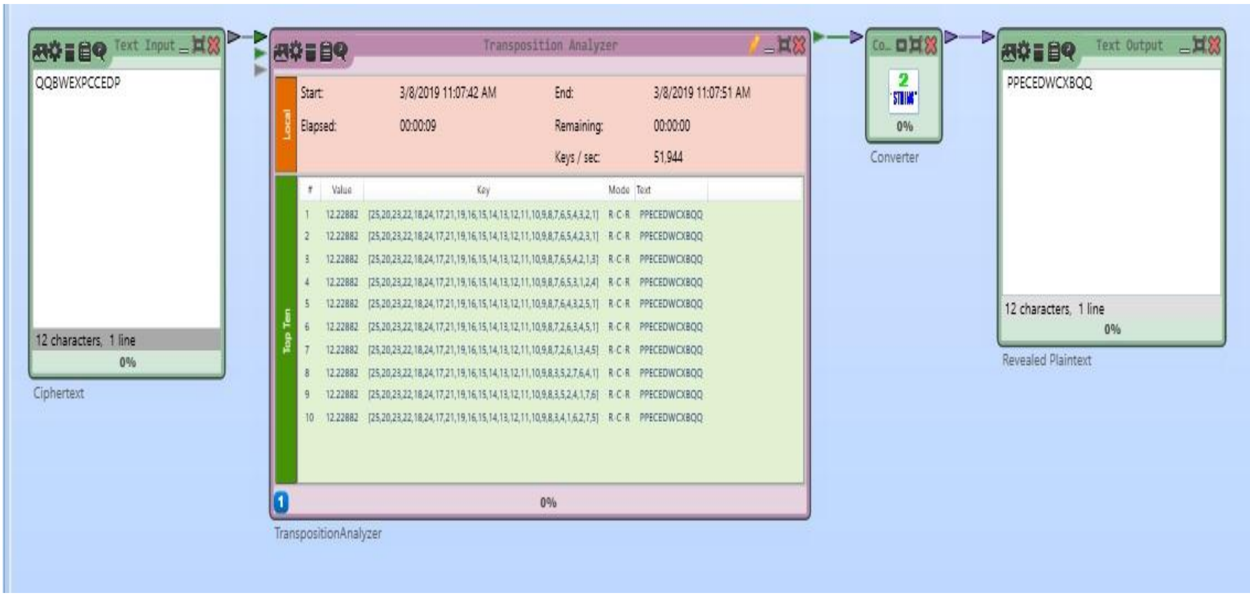
Co...

0%

Converter

Figure 7 Transposition genetic analysis

Through using the genetic analysis to determine the true message, according to the basics of genetic algorithm, this method also failed to know the plain text, as showed in Figure (7).



QQBWEXPCCEDP

12 characters, 1 line

0%

Ciphertext

Start: 3/8/2019 11:07:42 AM End: 3/8/2019 11:07:51 AM

Elapsed: 00:00:09 Remaining: 00:00:00

Keys / sec: 51,944

#	Value	Key	Mode	Text
1	12.22882	[25,20,23,22,18,24,17,21,19,16,15,14,13,12,11,10,9,8,7,6,5,4,3,2,1]	R-C-R	PPECEDWCXBQQ
2	12.22882	[25,20,23,22,18,24,17,21,19,16,15,14,13,12,11,10,9,8,7,6,5,4,2,3,1]	R-C-R	PPECEDWCXBQQ
3	12.22882	[25,20,23,22,18,24,17,21,19,16,15,14,13,12,11,10,9,8,7,6,5,4,2,1,3]	R-C-R	PPECEDWCXBQQ
4	12.22882	[25,20,23,22,18,24,17,21,19,16,15,14,13,12,11,10,9,8,7,6,5,3,1,2,4]	R-C-R	PPECEDWCXBQQ
5	12.22882	[25,20,23,22,18,24,17,21,19,16,15,14,13,12,11,10,9,8,7,6,4,3,2,5,1]	R-C-R	PPECEDWCXBQQ
6	12.22882	[25,20,23,22,18,24,17,21,19,16,15,14,13,12,11,10,9,8,7,2,6,3,4,5,1]	R-C-R	PPECEDWCXBQQ
7	12.22882	[25,20,23,22,18,24,17,21,19,16,15,14,13,12,11,10,9,8,7,2,6,1,3,4,5]	R-C-R	PPECEDWCXBQQ
8	12.22882	[25,20,23,22,18,24,17,21,19,16,15,14,13,12,11,10,9,8,3,5,2,7,6,4,1]	R-C-R	PPECEDWCXBQQ
9	12.22882	[25,20,23,22,18,24,17,21,19,16,15,14,13,12,11,10,9,8,3,5,2,4,1,7,6]	R-C-R	PPECEDWCXBQQ
10	12.22882	[25,20,23,22,18,24,17,21,19,16,15,14,13,12,11,10,9,8,3,4,1,6,2,7,5]	R-C-R	PPECEDWCXBQQ

0%

TranspositionAnalyzer

0%

PPECEDWCXBQQ

12 characters, 1 line

0%

Revealed Plaintext

Figure 8 Transposition hill clamping analysis

Finally, the hill clamping analysis failed to guess the original plain text as showing in the figure (8).

Conclusion

In this paper a new algorithm was proposed as a new cryptosystem, which is considered a mimic of wolf’s group society, so it called “wolf algorithm”. This algorithm uses a new technique differs from all techniques used in cryptosystems to add more difficulty and secrecy to the proposed cryptosystem in order to protect the data that transmitted over the internet securely. Many attacks were applied on the proposed cryptosystem to evaluate the complexity and difficulty of the cryptosystem and all results showed that this cryptosystem was unbreakable and proved the strength of the proposed algorithm against different types of attacks.

References

Abed, B.N.A.D., & Noaman, S.A. (2013). *Cipher Text as an RGB Color Image*. Science and World.

Abed, B.N.A.D., Noaman, S.A., & Salman, A.D. (2013). *Cryptosystem based on the Principles of Indefinite Integral*. Science and World.

Abed, B.N.A.D., & Noaman, S.A. (2019). McLaurin series as a new technique to improve encryption process. *In Journal of Physics: Conference Series, IOP Publishing*, *1294*(4), 042008.

Figari, H., & Skogen K. (2011). Social representations of the wolf. *Acta Sociologica*, *54*(4), 317-332.

Manasrah, A.M., & Al-Din, B.N. (2016). Mapping private keys into one public key using binary matrices and masonic cipher: Caesar cipher as a case study. *Security and Communication Networks*, *9*(11), 1450-1461.

Mirjalili, S., Mirjalili, S.M., & Lewis, A. (2014). Grey wolf optimizer. *Advances in Engineering Software*, *69*, 46-61.

Muro, C., Escobedo, R., Spector, L., & Coppinger, R.P. (2011). Wolf-pack (Canis lupus) hunting strategies emerge from simple rules in computational simulations. *Behavioral processes*, *8*(3), 192-197.

Noaman, S.A., Abed, B.N.A.D., Hashim, K.S., & Ibrahim, N.J. (2013). Simple encryption algorithm using mathematical complement. *Science and world*, 58.

Packard, J.M. (2012). *Wolf Social Intelligence*. Wolves: Biology, behavior and conservation.

Shaban, S.A., & Najim Al-din B. (2017). A new algorithm for encrypting arabic text using the mathematical equation. *Diyala journal of engineering sciences*, *10*(1), 21-30.