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 \[k_m + O(ch(WG(x_n)))\]
8- The result is the wolf cipher text

**Decryption Process**

1- \[k_m - k_m + [k_n + O(ch(WG(x_n)))] \mod 26\]
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 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | 1 | 2 | 3 | 4 | 5 |
| 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 \(\leftrightarrow H \leftrightarrow O \leftrightarrow G \leftrightarrow 14+1 \leftrightarrow 6+2 \leftrightarrow 15 \leftrightarrow 8 \leftrightarrow L \leftrightarrow I\)
   2&11 \(\leftrightarrow W \leftrightarrow G \leftrightarrow R \leftrightarrow D \leftrightarrow 17+3 \leftrightarrow 3+5 \leftrightarrow 20 \leftrightarrow 8 \leftrightarrow U \leftrightarrow I\)
   3&4 \(\leftrightarrow Q \leftrightarrow M \leftrightarrow O \leftrightarrow 12+2 \leftrightarrow 14+4 \leftrightarrow 14 \leftrightarrow 18 \leftrightarrow K \leftrightarrow S\)
   5&10 \(\leftrightarrow P \leftrightarrow O \leftrightarrow I \leftrightarrow 14+7 \leftrightarrow 8+2 \leftrightarrow 21 \leftrightarrow 10 \leftrightarrow V \leftrightarrow J\)
   7&12 \(\leftrightarrow H \leftrightarrow G \leftrightarrow G \leftrightarrow 6+1 \leftrightarrow 6+1 \leftrightarrow 7 \leftrightarrow 7 \leftrightarrow H \leftrightarrow H\)
   8&9 \(\leftrightarrow T \leftrightarrow T \leftrightarrow N \leftrightarrow N \leftrightarrow 13+6 \leftrightarrow 13+6 \leftrightarrow 19 \leftrightarrow 19 \leftrightarrow T \leftrightarrow T\)
6- Exchange1 = LUKSVIHTTJIH
7- Exchange2 = IJSKJLHTTVUH
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 QWQQHQHHTTPGH
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.

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).

**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).

**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).

Figure 4 Crypto K1 attack

Figure (4) shows 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 shown.

Figure 5 Monoalphabitic substitution analysis
monoalphabetic substitution analysis applied on the proposed method in order to break the cipher text and extract the original text from the secret message, but the result showed the reverse of that as in the figure (5).

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.

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).

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**


