THINK INDIA JOURNAL

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

A Novel Approach Using 3-Des Algorithm Against Cryptographic Attacks

Richa Sharma[1],Ritika Sharma[2]

[1]School of Computer Science & Engineering, Lovely Professional University, Phagwara Punjab,India.
[2]Department of Computer Science, R.K.S.D(P.G) College, Kaithal Haryana,India.
richa.18364@lpu.co.in[1], sharmaritika2929@gmail.com[2]

Abstract- DES is considered insecure because many different attacks are possible in it. For the encryption of electronic data, we use the Data Encryption Standard which is symmetric-key algorithm. The two basic facts of current day data encryption are authentication and data privacy. As modern society is now becoming more connected day by day, so large amount of information is under threat. Therefore, there is a need for protection which brings data secrecy and data integrity.

This paper discusses about the improvement of DES algorithm to make it more secure. It also points out some disadvantage of DES and 3-DES algorithms. It also discusses about one new algorithm which is an improvement of the 3-DES algorithm. A Comparison has been made between DES, 3-DES and New algorithm. This comparison is conducted on the basis of key size, total rounds, complexity, user effort needed etc.

Keywords: DES, TDES.

I. INTRODUCTION

In cryptography, to make data accessible to the authorized user, it is encoded using encryption techniques[1]. In an encryption technique, the useful information or message, which is referred as plain text, is converted or encrypted using an encryption algorithm. There are many different algorithms which are available and are used to secure information. Some of them are AES, DES, and 3-DES, RC2, RC6, and BLOWFISH [2].

Still confidential information is unsafe from intruders who easily get access and modify the secret data. Intruders mainly try to steal important data or identities and become deceit person. Some additional improvements are required in already existing algorithms to enhance the security. Data Encryption is a very essential process to provide security. It is necessary to encrypt data before passing it to the network and then at receiver side this data is decrypted to get the original data. However, nowadays most all types of encryption techniques are subject to attack easily. For all cipher text, the most common way of attack is brute force attack in which all possible keys are tried by the intruder to decrypt the data. There are some algorithms in which question is raised for their small key sizes and they dictated a need for a replacement algorithm.

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

As Data encryption standard (DES) is a symmetric-key algorithm, it is used to encrypt the electronic data. But DES is now considered to be more vulnerable for many applications. One of the biggest reasons behind this is the key length (which is 56 bits only) [2]. The brute force attack has the capacity to easily break DES security.

DES is the standard block cipher which takes data or plaintext of fixed length and encrypts it by using a number of complicated operations into some different cipher text[3]. The Key seemingly consists of 64 bits; in which only 56 bits are used by the algorithm. In a similar way there is an algorithm known as Triple Data Encryption Standard (TDES or 3DES) which applies DES 3 times on any particular data or data block. Triple DES generates a very simple method in which size of DES key length increases to protect against different attacks [3,4]. Triple DES uses 3 different keys to encrypt the data. Triple DES has a key length size of 168 bits because of that three keys, but only 112 bits provide the effectuality security. This is showing that this algorithm is also not much secure.

So there is a need of some improvement in this algorithm so that security of data increases upto some more extent.

II. RELATED WORK

A. Evolution of DES

In the field of encryption, DES has undergone many advancements or improvement and served as a base for many different techniques. One of its improvements is Triple DES (3DES or TDES). Triple DES uses 3 keys to encrypt data. So, the total key length size of 3DES is 168 bits. But in reality the effective security provided by it is only 112 bits. As a DES uses 16 rounds to encrypt the data, triple DES uses 48 bits in total to encrypt the data. This technique helps to increase the security up to 3 levels or increase the security, efficiency 3 times more than DES [4]. As 3-DES performs every task 3 times related so its performance also increase 3-times more the DES algorithm. 3-DES uses three keys to encrypt the data.

DES, sometimes used simultaneously with other encryption techniques. Sometimes they are fused to some other encryption algorithms. This type of fusion is used to secure the key generation of the DES. It uses 2 keys to perform initial permutation which is followed by 16 rounds of crossover iterations and finally go through the inverse permutation. It sometimes decreases the brute force chances, but slowed down the process.

B. Known Attacks on DES

There are many different attacks that are possible on DES in which Brute Force and cryptanalysis techniques are most common. Brute Force is one of the most strongformsof attack on any encryption uptill now. It tries to decrypt the block of encrypted data with all possible keys. So the data we have on the clear text will allow us to accept the right key and stop the

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

search. In average, we will have to try nearly 36'028'797'018'963'968 (36 million of billions) of keys.Modern PC can easily evaluate one to millions keys per seconds. Differential cryptanalysis is a new generic symmetric algorithm. It works by presuming the attacker has some part of original plaintext. The attacker then diminishes the security of the encryption until he or she deciphers the key. The data analysis phase computes the keys by analyzing near about 2^24 chosen plaintext. But mainly, the attacker analysis near about 2^14 chosen plaintext and succeeds with probability of 2^-33.

III. DESCRIPTION ABOUT MODIFIED DES

A. Key Generation Process

The code used in this algorithm provides the security to the data more than the security provided by Data Encryption Standard (DES) and 3- DES algorithm. As in this algorithm, encryption of data is taking place more than 3 times, which was fixed in 3-DES algorithm up to 3 times only [6].

In DES and 3- DES algorithm, it was fixed that the user has to enter data and key of size 64 bits only, but in this new algorithm user can enter data and key of any size. One more advantage of this new algorithm over 3-DES algorithm, in 3-DES user has to enter more than one key for encryption, but in this new algorithm only one key is sufficient to encrypt the data in a better way than a 3-DES algorithm.

In this algorithm, if the user enters key of size less than 64 bits, then it by default fill 0's on the end to make it of size 64 bits.Suppose a user enter key (1023456) in hexadecimal form then it covers 28 bits only. So to make this key of size 64 bit it by default fills 09 0'sin the end of key in hexadecimal form. Now, as this new algorithm is encrypting data up to N times it needs N different Keys during the process.

The advantage of this algorithm is that when users enter the first key (K1), it will generate these N no. of keys by own without any effort needed by the user.

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

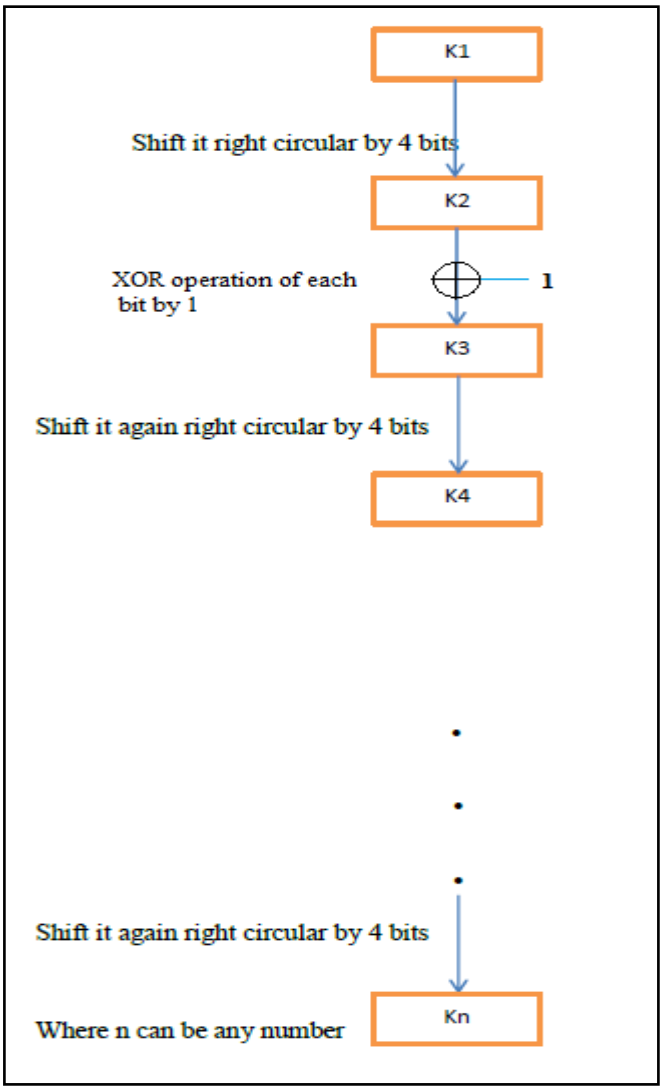

Figure 1: KEY GENERATION

Figure 1 shows how different keys are generated by one particular key (K1) in this new algorithm.

B. Plain Text Encryption Process

In this Plain text encryption process, the size of input data can be of any length.In this algorithm,if the user enters data of size less than 64 bits, then it by default fill 0's in the end to make it of size 64 bits.For example, if user enters data (abcde) in hexadecimal form, then it covers 20 bits only.So to make this data of size 64 bit it by default fill 11 0's in the end of key in hexadecimal form.In this encryption process user first enter data and key of any size. Then by adding 0's it is converted up to64 bits. Now these data and key bits go through the DES algorithm and give the output of 64 bits in the encrypted form.

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

Now the key using in this process will first perform a right circular process to generate the next key then perform XOR operation to generate next key. This new key will again go through the DES algorithm with the encrypted data comes as an output in the previous process.This process will continue up to the N times where N is the number of times encryption enters by the user.

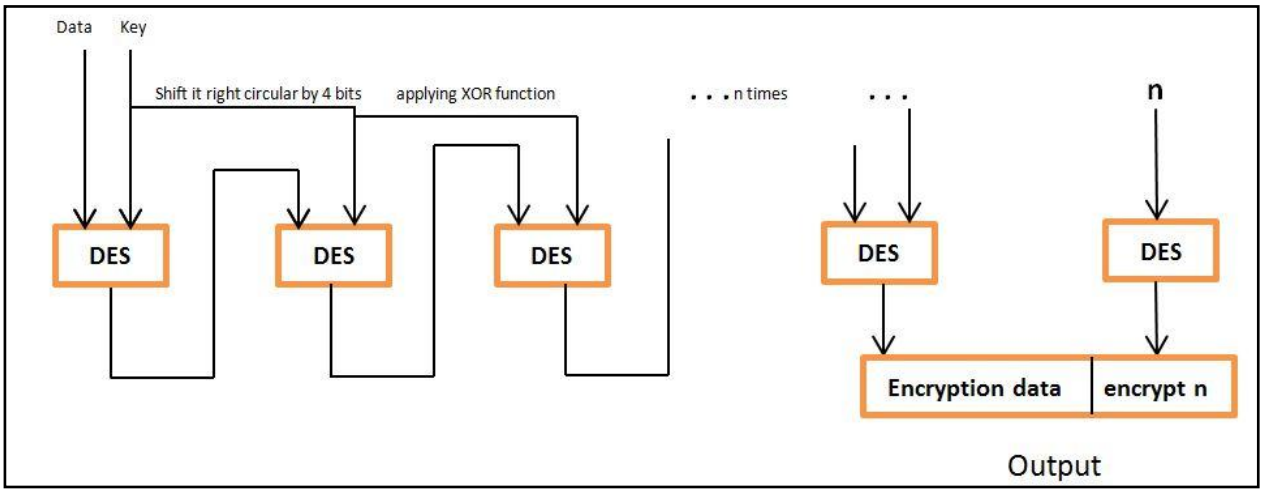

Figure 2: ENCRYPTION ALGORITHM

Figure 2 is showing how one process is related to another process. This diagram is also telling how the output of the one process will become the input for the next process.

Here N(number of times encryption) can be decided by the user and the value of N is also sent in the encrypted form with the cipher text so that an attacker will not able to get the value of N. The value of N is encrypted using DES and then concatenate with the final cipher text before sending it to destination.

While decryption, firstly encrypted value of N can be decrypted to get number of times encryption (N) then this value is used to decrypt the cipher text to get actual plaintext.

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

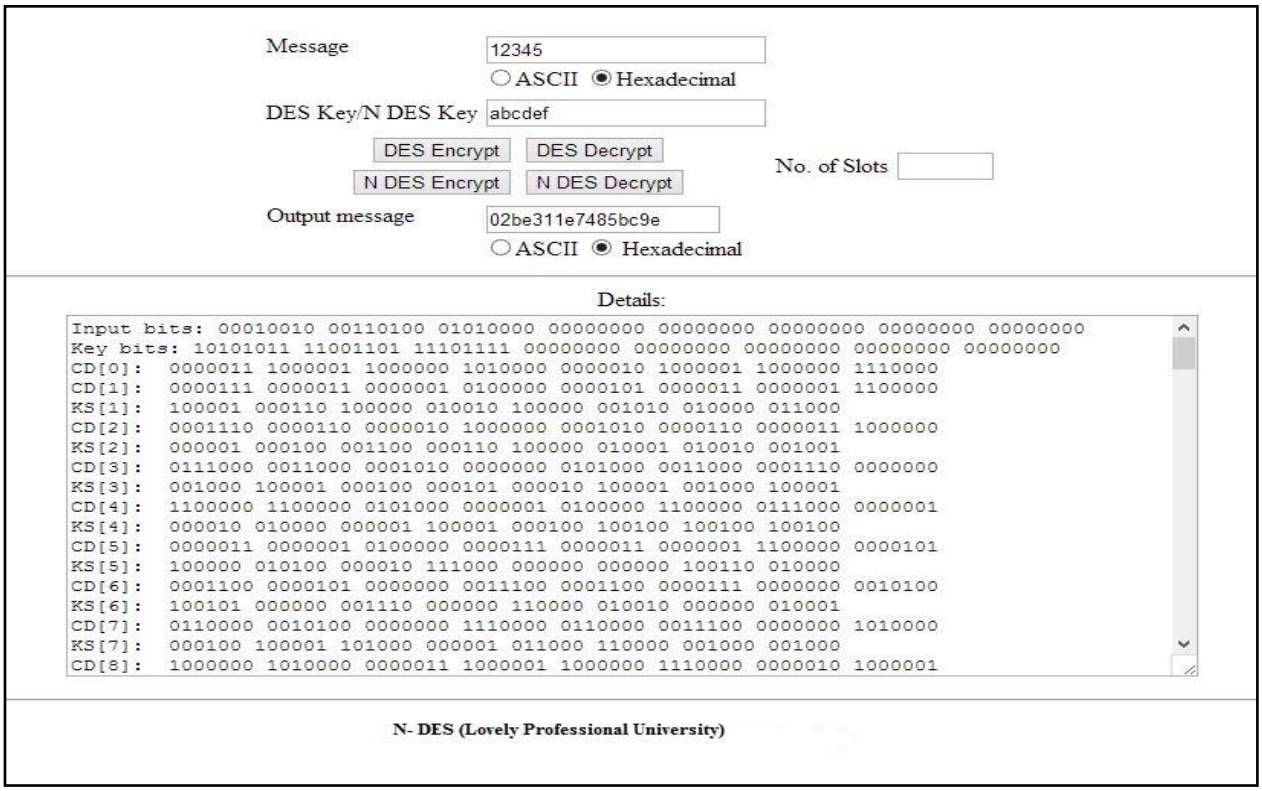

Figure 3: INTERFACE OF THE APPLICATION

C. Decryption Process

In DES, encryption and decryption are using the same algorithm. In decryption process the input is the ciphertext and the key processing is always performed in reverse order. The new algorithm is designed like that so that it can decrypt ciphertext to its original form. A very important point during the decryption process, we need to remember about the ciphers is that the round keys (K1 to K16) should be applied in the reverse order. At the encryption site, round 1 uses K1 and round 16 uses K16; of the decryption site, round 1 uses K16 and round 16 uses K1.

In the decryption process user first start with the last key (KN) and the cipher text. This last key is directly calculated by first shifting the original key up to 4 bit right circular and then applying XOR operation this process will continue upto (N) *4 time. Here the value of N is calculated by cipher text because its last half part is the encrypted form of the value N. So firstly last half part of this cipher text decrypted by DES to calculate value of N and then by using that value of N we calculate actual plaintext.

Now these cipher data and key bits go through the Decrypt-DES algorithm and give the output of 64 bits.

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

Now the key using in this process will perform a Left circular process and XOR operation to generate the next key. This new key will again go through the Decrypt-DES algorithm with the data comes as an outpatient the prrevious process. This process will continue up to the N times where N is number of times encryption enters by the user.

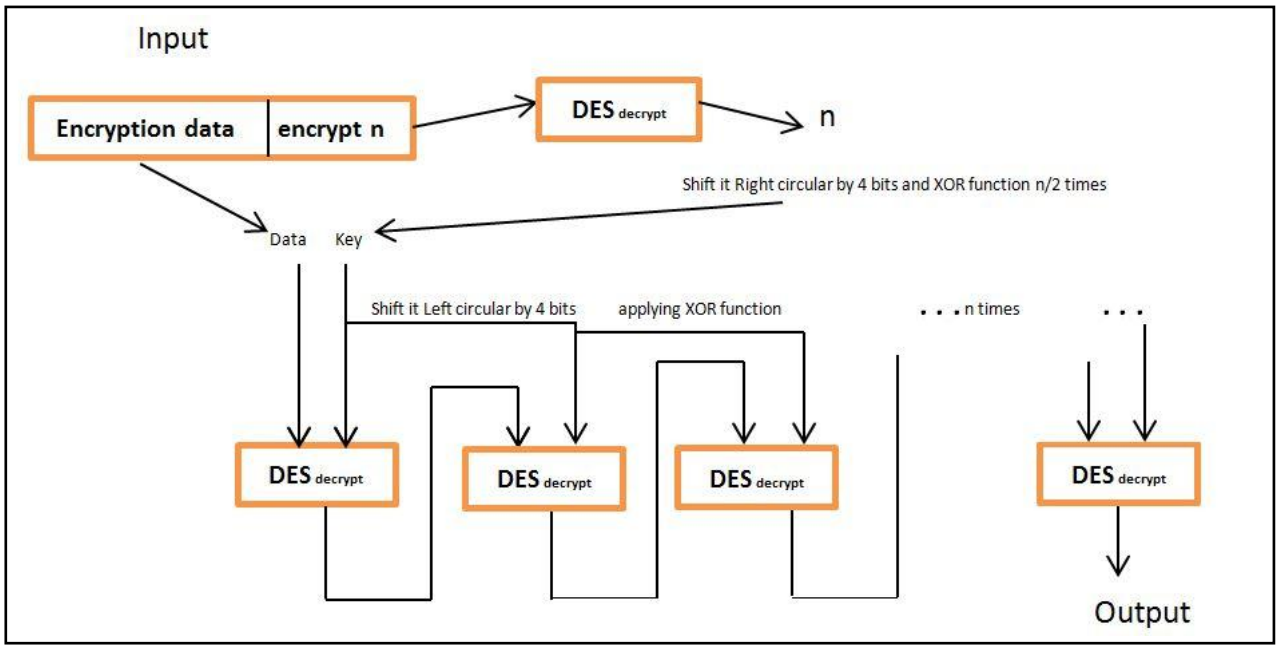

Figure 4: DECRYPTION ALGORITHM

Figure 4 is showing how one decryption process is related to another process. This diagram is also telling how the decrypted output of the one process will become the input for the next process.

IV. COMPARISON BETWEEN DES, 3-DES AND N-DES

There are many points which describe the difference between the previous algorithm(DES and 3-DES)and new algorithm(N-DES). The difference is calculated on the basis of input data size, input key size, etc.. The new algorithm performs filling of 0's at the end, which was notthere in DES and 3-DES.There is also some difference between 3-DES and N-DES on the basis of Decrypt time.

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

Table 2: COMPARISON TABLE

DES	3-DES	N-DES
Enter Key one time	Enter key 3 times	Enter Key one time
Brute force attack need 2^52 pattern to analyze	Brute force attack need 2^156 pattern to analyze	Brute force attack need 2^(n*52) pattern to analyze
Rounds : 16	Rounds : 3*(16)	Rounds : n*(16)
Need to enter one Key	Need to enter 3 Keys	Need to enter one Key it will simultaneously generate (n) number of keys.
Need user effort more	Need user effort more than needed in case of DES.	Need user effort even less than needed in case of DES.
Computation power increase normally from 8-16% on increasing key size.	Computation power increase in larger amount more than 16% each time on increasing key size.	Computation power increases same as DES algorithm.

V. SUMMARY AND CONCLUSION

This research will help to increase the Security level of data. This code provides the security to the data more than security provided by Data Encryption Standard (DES) and 3- DES algorithm. As in this algorithm encryption of data is take more than 3 times which was in 3-DES algorithm. The interface used here is also very user friendly.

Few best properties of this algorithm are:

- User can enter any size of data which is not in case of DES and 3-DES algorithm.
- User can enter any size of Key which is not in case of DES and 3-DES algorithm.
- Users have to enter only one Key here and it will encrypt data n time by generating n different Keys which is not in case of DES and 3-DES algorithm.
- Complexity of algorithm increases much more than 3-DES algorithm.

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

REFERENCES

[1] S. Kumar, M. Kumar, R. Budhiraja, M. K. Das, & S. Singh, " A cryptographic model for better information security. Journal of Information Security and Applications, vol. 43, pp. 123–138, 2018

[2] X. Wu, C. Bai, H. Kan " A new color image cryptosystem via hyperchaos synchronization," Commun Nonlinear Sci Numer Simullation. Vol. 19(6). pp. 1884–97, 2014.

[3] C. Pak, L. Huang "A new color image encryption using combination of the 1d chaotic map". Signal Process vol. 138 pp. 129–37, March 2017 .

[4] X. Li, X. Meng, X. Yang, Y. Wang, Y. Yin, X. Peng, et al, "Multiple-image encryption via lifting wavelet transform and xor operation based on compressive ghost imaging scheme", Opt Lasers Eng vol. 11 pp. 102:106, Oct 2017.

[5] W. Paper, & S. Fpgas, " Data Encryption using DES / Triple-DES Functionality in Spartan-II FPGAs" , vol 1.0, pp. 1–14, Mar. 2000

[6] G. Singh and Supriya. 2013. "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security". International Journal of Computer Applications Vol. 67, No. 19, April 2013.

[7] R. Anderson, E. Biham, & L. Knudsen, " Serpent : A proposal for the advanced encryption standard". NIST AES Proposal, pp. 1–23. 1998

[8] P. Patil,P Narayanka, D. G. Naraya & S. M. Meena " A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish." Procedia Computer Science, vol. 78, pp. 617–624, Feb 2016.

[9] H. Page, F. Information, S. T. Policy, E. Funds & S. T. Policy, "Computer data authentication", pp. 1–6, 1987.

[10] D. S. AbdElminaam, H. M. A. Kader, & M. M. Hadhoud, "Evaluating the performance of symmetric encryption algorithms" International Journal of Network Security, ED. 10(3), pp. 213–219, 2010.

[11] A. M. Sison, B. T. Tanguilig, B. D. Gerardo, & Y. C. Byun, "Implementation of improved des algorithm in securing smart card data" Communications in Computer and Information Science, pp. 252–263, 2012.

[12] H. O. Alanazi, B. B. Zaidan, A. Zaidan, H. A. Jalab, M. Shabbir and Y. Al-Nabhani "New Comparative Study Between DES, 3DES and AES within Nine Factors" JOURNAL OF COMPUTING, vol. 2(3), Mar 2010.

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

[13] R. M. Davis, A. Konheim, and D. Coppersmith, "Data Encryption Standard," pp. 250–253, 1981.

[14] V. Rijmen, "Practical-Titled Attack on AES-128 Using Chosen-Text Relations," p. 2009, 2010.

[15] L. Sharma, B. K. Pathak, and N. Sharma, "Breaking of Simplified Data Encryption Standard Using Binary Particle Swarm Optimization," vol. 9(3), pp. 307–313, 2012.

[16] H. D. E. S. Works, "How DES Works in Detail Step 1 : Create 16 subkeys , each of which is 48-bits long .," vol. 64, pp. 1–14.

[17] M. S. Policies, "IACIS Home JCIS Submission Guidelines," no. 10, pp. 11–12, 2015.

[18] I. Aes and S. Cipher, "broken in the practical sense .," pp. 1–14, 2004.

[19] S.Mankotia and M. Sood "A Critical Analysis of Some Symmetric Key Block Cipher Algorithms". International Journal of Computer Science and Information Technologies, vol. 6, 2015