Volume 4, Issue 10, October 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Building Cryptosystem Based on Genetic Algorithm and Pattern Recognition Concepts for Academic Institution

A. E. Amin
Department of Computer Science
Mansoura University, Mansoura, Egypt

A. Abd Elbadea
Department of Computer Science
Mansoura University, Mansoura, Egypt

Abstract: ***This paper introduces cryptography real time data transmission framework for based on concepts of artificial intelligence techniques. The proposed framework is integrated between concept of genetic algorithm to generates unique genetic key and use it to formulate patterns table then the secrete message is divided into blocks with same size according to length of key and pattern recognition is used to blocks matched by weighted Euclidean distance.***
The XOR operation plays a major role in modern cryptography, where the total length of the plaintext is not a multiple of block length, it is necessary to deal with the final short block. The final block must contain a count of the number of filler bytes, so the message length is always increased by a maximum of block length bytes. If this increase in length is not acceptable, a solution is to XOR the short block by re-enciphering the last complete cipher text block.
Performance of the proposed system is evaluated considering the encryption time decryption time, the proposed system possesses good performance in encryption, decryption speed and it is suitable for real-time cryptography and transmission.

Keywords: Information Security, Genetic Algorithm, Pattern Recognition, Cryptography.

I. INTRODUCTION

Today is the era of internet and network applications. So information security has become an important issue in data communication. The same holds true for academic institutions. Academic institutions use computer systems and computing to great effect for their academic, research, and administrative activities. Information security is a multidisciplinary area of study and professional activity, which is concerned with the development and implementation of security mechanisms to protection of information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

In a shared network environment, unprotected traffic is posed some security attacks. Moreover, network users need to be sure about their data integrity and privacy. The best method to provide data privacy and integrity is encrypting these traffics. All users in the network environment must be able to communicate securely with each other as well as with servers.

Much of what do in the world involves risk [1]; the nature of threats to security in cyberspace is conceptually no different than the nature of threats in the real world. In both worlds, it is possible to gain access to confidential information and use it in unintended or illegal ways [2].

Information Securing (IS) is a major concern for academic institutions. Unauthorized access to systems and the loss of confidentiality or data accuracy can damage academic institution's reputation. Even though security is viewed as an important concern, it sometimes conflicts with the principals of open access in the education setting.

The IS is a multidisciplinary area of study and professional activity which is concerned with the development and implementation of security mechanisms to protection of information systems from unauthorized access, use, disclosure, disruption, modification, and destruction in order to provide confidentiality, integrity, and availability [2-4].

In general, there are two types of cryptographic schemes: symmetric cryptography and asymmetric cryptography [5]. The symmetric scheme uses the same key for encryption and decryption. Two keys are used in asymmetrical cryptography, one for encryption, known as the public key, and the other for decryption, known as the private key [5-6].

There are five main goals of cryptography. Every security system must provide a bundle of security functions that can assure the secrecy of the system authentication, privacy/confidentiality, data integrity, non-repudiation, and service reliability and availability [3, 7].

This paper presents a new approach for cryptography real time data transmission by combining between two of the most famous artificial intelligence techniques. First concept of genetic algorithm is used to generate unique genetic key. Second pattern recognition technique is used to matching the blocks which formulated by divided the secret massage with the same size according to key length. A primary goal of proposed technique was to provide fast and improved performance results having practical and feasible implementation.

The rest of the paper is organized as follows. In Section 2, we introduce related work. The proposed method is presented in section 3 as general framework. Section 4 presents the cryptosystem processing. The experimental and results is discussed in section 5. Section 6 discuses the performance evaluation. Concludes of this paper presents in section 7.

II. RELATED WORK

D. Singh, P. Rani and R. Kumar [8] have designed a cryptographic algorithm using the concept of genetic algorithms. This algorithm enhances the quality, efficiency and effectiveness of the algorithm being used for the cryptography. From the experimental results, it can be easily seen that the present algorithm has achieved the objective set in the present study. Statistical analysis shows that the dimensions of original data and the encrypted are totally different. Also the histogram of the encrypted image is nearly uniform and is quite different from the original image; hence, it does not provide any clue to employ any type of statistical attack on the proposed image encryption technique. Time analysis results show the throughput rate of the proposed method and it is found that the algorithm gives a much better and acceptable throughput rate. The conventional encryption techniques are not a feasible solution in terms of their throughput rate. Hence, a secure encryption technique with high throughput has been designed for real time data transmission. From experimental results it is clear that the encryption results are completely random and very sensitive to the parametric fluctuation that makes transferring of secret information highly safe and highly reliable .

A. Jassim [9] has worked a GA utilized to establish an approach for random key to each letter in text massage encoding/decoding. The test results indicated that using this approach achieved good performance to hide text massage that because choosing random key by genetic algorithm gives the approach difficulties that can not easily discover or break the key. Every character in text message encoded by random key, the highest value is 128 bit .

S. Mishra and S. Bali [10] have presented application of GA in the field of cryptography. Key Selection in public key cryptography is a selection process in which keys can be categorized on the basis of their fitness, making GA a good candidate for key generation. The primary goals of this work were to produce better and fast performance results and to determine the validity of typical GA-based methods in the field of cryptography. Thus from statistical analysis of results, final keys obtained from GA were observed to be purely random and hence increasing the strength of keys and security.

The work in this search has been implemented using C++ language. 192 bits random Public and Private Key were generated. Public and Private Key Samples have been collected and analyzed in Microsoft Excel. In the analysis, population of 200 chromosomes were considered and were found to be randomly generated as proposed such that for each loop an entire new population is observed. Analysis was done for various sample values of keys generated which included frequency test (chi-square test) and gap test to check the nature of randomness and replication of chromosome, satisfactory results were obtained. In Gap Test, all 200 sample chromosomes were found to be unique and non-repeating possessing no relation of next random chromosome of keys with previous generated one . Threshold check was also performed after crossover and mutation steps which was a deciding factor for the acceptance of chromosome generated throughout the process. This process is stopped when a given termination condition is met. Roulette Wheel Selection was applied which resulted in the replication of favorable data, thus making the population fitter. Ring crossover was applied and the rate of mutation was taken as 5% .

Fitness of keys was found using Pearson's coefficient of auto-correlation followed by ranking using phi-coefficient which decided the best fitness and has been verified from results. Results were analyzed even for large number of chromosomes > 200. The results have been compared with the standard results and were found to be in accepted and satisfactory range after verification. Coefficient of Correlation is found to be satisfactory, random chromosome is selected which is taken as key for PKC.

M. Barati and et. al. [11] emphasize on Intrusion Detection System (IDS) in encrypted traffic and provides a review of recent proposed IDS in this context. Proposed systems are not appropriate enough for the defined requirement due to the shortcomings already shown. A weak point of all these systems are the low efficiency. For a comprehensive development of encrypted traffic IDS in productive environments, false alarms should be minimized. In this study, efficient features for IDS in encrypted traffic are selected using GA. The idea of using the most efficient features instead of all features for classification is shown promising by results .

M. Kumar and et. al. [12], have proposed a GA secret key image encryption method used two points crossover in the key generation. This encryption method fulfills the security aspects required in any encryption process.

J. Kumar and S. Nirmala [13], have presented a new image encryption scheme has been proposed which utilizes selection, crossover and mutation operations. The method proposed is tested on varieties of images. Statistical analysis is carried out through histograms. Performance of the approach is evaluated in terms of correlation coefficient. From the performance evaluation it is concluded that the algorithm proposed is robust to statistical attack.

In the proposed approach, it is hard to predict the key sequence as the key sequence generated depends on the input image and initial seed of the pseudorandom generator.

III. GENERAL FRAMEWORK

This paper presents a novel technique to information cryptography and de-cryptography based on the integration between two of the most famous artificial intelligence techniques namely genetic algorithm and pattern recognition as shown in figure 1.

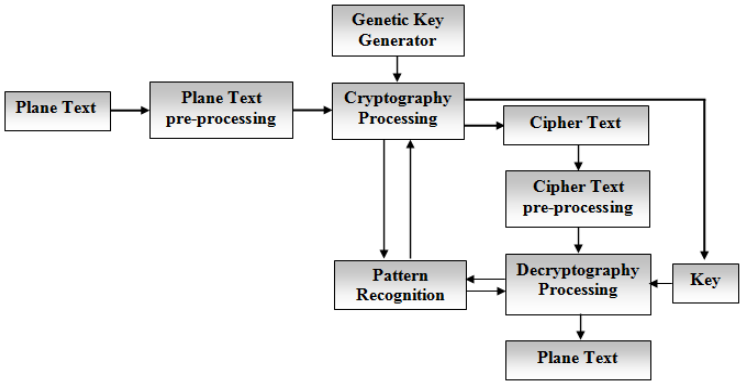


Fig 1: Block diagram of the general framework

Genetic algorithm technique is characterized by ability to create a high quality number generation by using principles of selection and evaluation. So, it is used to generate unique Genetic Key (GK) which used to formulate pattern table and make (XOR) operation with Binary Plain Text (BPT) after pattern recognition. Pattern recognition technique is a protocol offering the accuracy of cryptographic processing by using two main phases namely formulated patterns table and pattern recognition classifier which considered a strong cryptographic security. Interestingly, the characteristics of these classifiers allow us, not only to achieve better accuracy, but also to improve the degree of privacy provided by the pattern recognition technique.

IV. CRYPTOSYSTEM PROCESSING

Cryptosystem is a method used to hides the information from all others by using cryptography science. Cryptography is process of making and using codes to secure transmission of information. There are two main parts for cryptosystem namely encryption processing and decryption processing.

1.1. Encryption processing

Encryption is converting original information into a form unreadable by unauthorized individuals. In this processing, there are two techniques from artificial intelligent techniques are integrated called genetic algorithm and pattern recognition.

1.1.1. Genetic algorithm technique

Genetic Algorithm (GA) is stochastic search algorithms based on the mechanism of natural selection and natural genetics [14]. GA is belongs to the class of evolutionary algorithms [15-16], which are used to find solutions to optimization problems using mechanisms based on biological evolution. The main idea of (GA) is that in order for a population of individuals to adapt to some environment, it should behave like a natural system. This means that survival and reproduction of an individual is promoted by the elimination of useless traits and by rewarding useful behavior [15]. This concept is used to generate keys which used in encryption process as shown in figure 2.

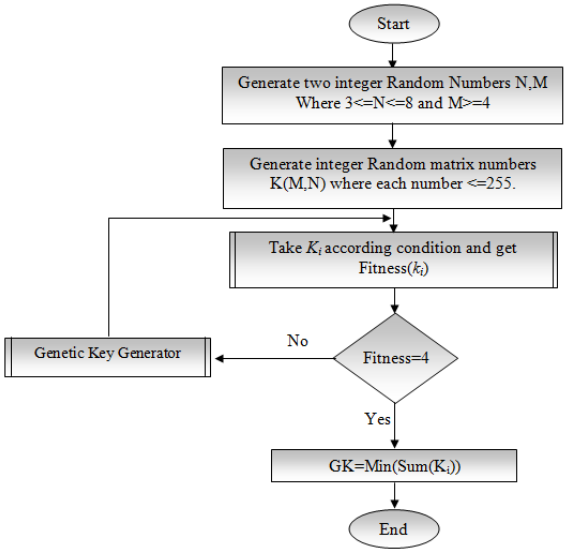


Fig 2: Flowchart of the Genetic key generator.

1.1.1.1. Genetic key generator

Genetic key generator passes throw several steps as show in figure 2. The first initialization of keys; generate two integer random numbers N, M; where:

$$3 \le N \le 8, \quad M \ge 4$$

From M, N generate integer random keys matrix $K(M,N)$, where each element in the matrix less than or equal 255. For obtain on the objective function which represents the maximization of sum the initial condition results as shown in initial condition algorithm.

The second step if probability equal one the sum of corresponding key is calculated and sorted it to obtain on the suitable (GK) that corresponding to minimum sum else use genetic operators to generate (GK).

Initial Condition Algorithm

for $i = 1$ *to* M
  if each element in $K(i,:) \neq 0$
    Then $R_1 = 1$
    Else $R_1 = 0$
  if each element in $K(i,:)$ *is unique*
    Then $R_2 = 1$
    Else $R_2 = 0$
  if $\sum K(i,:) < 2$
    Then $R_3 = 1$
    Else $R_3 = 0$
  if $\sum_{n=1}^{N} (K(i,n), K(i,n+1)) \neq \sum_{n=1}^{N} (K(i,n+1), K(i,n+2)) \neq \sum (K(i,1), K(i,N))$
  Then $R_4 = 1$
  Else $R_4 = 0$
The Object Function $= R_1 + R_2 + R_3 + R_4$
$\text{Probability} = \dfrac{\text{The Object Function}}{4}$
Next i
if probability $= 1$
    Then Take all $K(i,:)$ *with probability* $= 1$
      $S = \sum K(i,:)$
      $Sort(S)$
      $GK = Min(S)$
    Else
      use genetic operators to Generate GK
Endif

1.1.12. Genetic Operators

The genetic operators mimic the process of heredity of genes to create new offspring at each generation [17]. In essence, the operators perform a random search, and cannot guarantee to yield an improved offspring. There are four common genetic operators [14, 18] as shown in figure 3: selection [19], crossover [20], mutation [21], and inheritance [22].

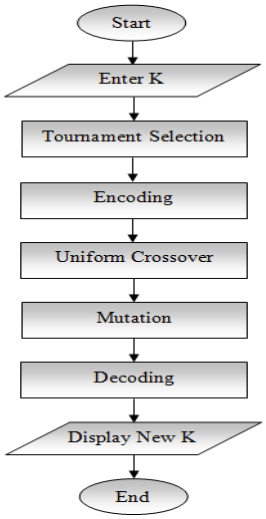


Fig 3: Flowchart of the genetic operators

1.1.2. Pattern Recognition Technique

Pattern Recognition is the study of how machines can observe the environments learn to distinguish patterns of interest from their background, make sound and reasonable decisions about the categories of the patterns [4].

In order to implement the pattern recognition technique the information must be passing through prepare phase called plaintext pre-processing.

1.1.2.1. Plaintext pre-processing

The plaintext exchanged to binary encoding text by two processing namely binary encoding and binary blocks code as shown in figure 4.

In binary coding; each character in plain text is converted to ASCII Plain Text (APT) then exchange (APT) to corresponding Binary Plain Text (BPT). Whereas; in binary blocks code are split BPT to blocks (B); where length of each blocks equals N bits. If block length less than 'N' bits, padded bits are appended from right to this block. The BPT blocks are used in pattern recognition technique.

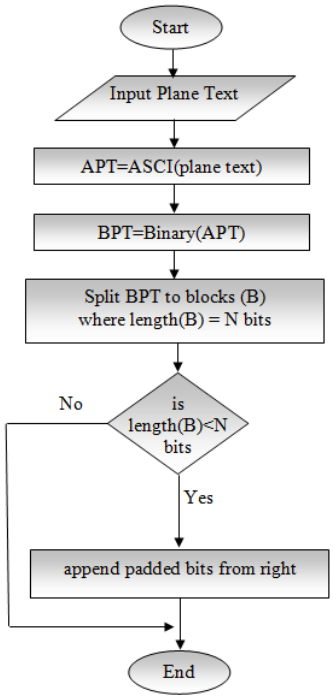


Fig 4: Flowchart of the plain text pre-processing

In the Pattern Recognition Technique (PRT) is divided to two main phases namely patterns table formulate and pattern recognition. In the first phase formulate patterns table depending on the random number N. Patterns table consists of Input Pattern (IP) and Output Pattern (OP). To formulate (IP) follow the next algorithm:

Formulated IP Algorithm

For i=0 to 2^N-1
IP(i) = Binary (i)
Where:
- ***The least significant bit is represented by the first .***
- ***Produces a binary representation with at least N bits.***

Next i

Whereas the (OP) is formulated as follow.

Formulated OP Algorithm

For i = 1 to 2^N
S=0
For j = 1 to N
If IP(i,j) =1 Then
S = S + GK(j)
End IF
Next j
OP= Binary (S)

Where:
- ***The least significant bit is represented by the first.***
- ***Produces a binary representation with at least O bits.***

Next i

In the second phase each block in (BPT) matched by weighted Euclidean distance with the (IP) to get the corresponding (OP). The cryptography processing is used the (OP) vector and (GK) to get cipher text.

- Pre-Processing encryption:

In this step; the (GK) is converted to generate Binary Genetic Key (BGK). By comparing the length of (BGK) with length of (OP) vector, if the result of the length of (OP) vector is longer than the length of (BGK) repeat (BGK) until getting the equal length via the length of (BGK) is longer remove padded bits from (BGK). After the lengths of (OP) vector and (BGK) are equal XOR operation is applied.

- XOR Operation:

In this step; (XOR) operation is applied on equal lengths of (OP) vector and (BGK) to increase the performance of security. The next example is show how the idea of XOR operation.

(OP)Vector	0	1	0	1	0	0	0	0
XOR								
BGK	0	0	0	1	0	0	1	1
Result								
	0	1	0	0	0	0	1	1

- Display Cipher Text:

Split XOR result to blocks equal 8 bits. If the block length is less than 8 bits append padded bits from right to this block. Convert each block into characters.

1.2. De-cryptography Processing:

Decryption is the process of transforming information that has been rendered unreadable through encryption back to its unencrypted form. In decryption, the system extracts and converts the garbled information and transforms it to texts and images that are easily understandable not only by the reader but also by the system as shown in decryption algorithm.

De-cryptography Algorithm

1. ***Cipher text pre-processing:***
   For each cipher text character is converted to ASCII.
   Convert ASCII plain text to Binary plain text.
2. ***Decryption:***
   Convert the (GK) to Binary Genetic Key (BGK)
   IF length (BGK) < length (BCT) Then
   Repeat (BGK) from left to right.
   Else if length (BGK) length (BCT) Then
   Remove bits from GK until lengths (BGK) and (BCT) is equal
   End if
   Apply (XOR) operation on equal lengths of (BGK) and (BCT)
   Split (BCT) after XOR to blocks where length of each blocks = O bits.
   IF block length < O bits Then remove this block
3. ***Pattern Recognition:***
   S=Sum (GK)
   N = Length (GK)
   O = Length (Binary(S)).
   Create IP(2^N, O), OP(2^N,N)
   - *Formulate (OP):*
     For i = 0 to 2^N -1
     OP(i) = Binary (i)
     Where:
     - The least significant bit is represented by the first.
     - Produces a binary representation with at least N bits.

     Next i
   - *Formulate (IP):*
     For i = 1 to 2^N
     S=0

For j = 1 to N
If OP(i,j) =1 Then
S = S + GK(j)
End IF
Next j
IP= Binary (S)
Where:

- The least significant bit is represented by the first.
- Produces a binary representation with at least O bits.

Next i

4. ***Display plain text*:**
Split (OP) vector to blocks equal 8 bits
Convert each block into characters

V. EXPERIMENTAL AND RESULTS

"A proposed electronic system for information security in academic institutions (MAAS)" is the name of proposed system which was run and tested on Mansoura University to transfer the information without worries of deceit and deception as shown in figure 5.

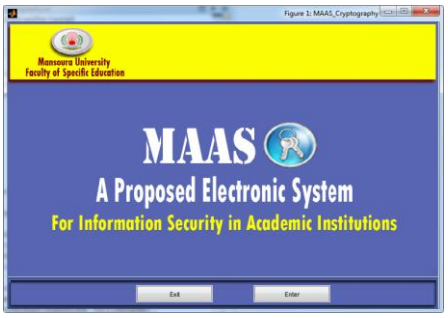
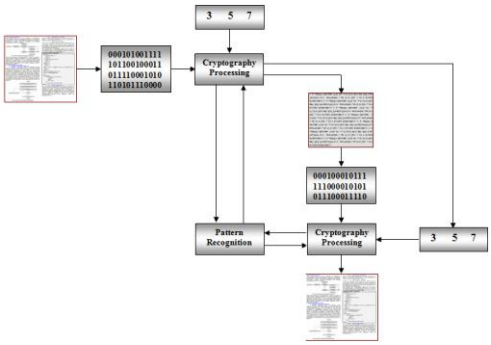


Fig. 5: The GUI for proposed system.

MAAS is passing by two main stages namely information send and information retrieval. For information send the plain text is encryption stage while as decryption represents the information retrieval as shown in figure 6. Figure 6-a is shown the abstract graph for encryption and decryption processing and the corresponding graphical user interface (GUI) is shown in figure 6-b.



a. Encryption and decryption abstract graph

b. Corresponding encryption and decryption GUI

Fig. 6: The main stages for MAAS.

The information send stage:

The sender sent a plain text including on text, mathematical equation and image as a test message as shown in figure 7.

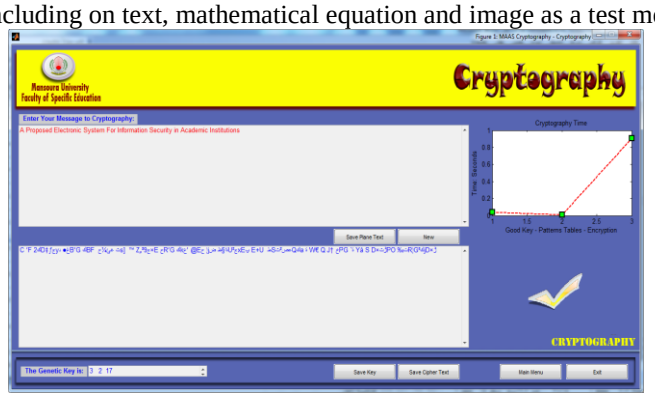


Fig. 7: The GUI of plain text.

When the Cryptography button is clicked, the MAAS started to encryption the plain text from GK stage until display cipher text as shown in figure 8.

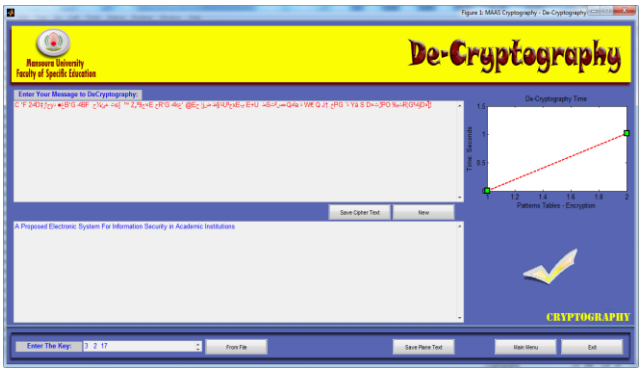


Fig. 8: Cipher text

The information retrieval stage:

To retrieval the information at any receiver uses requests to cipher ID from database and public genetic key for decryption as shown in figure 9.

The database identifies the message and the corresponding Cipher ID. This converts the Cipher text to ASCII codes and returns it in the “Encoded Text” box

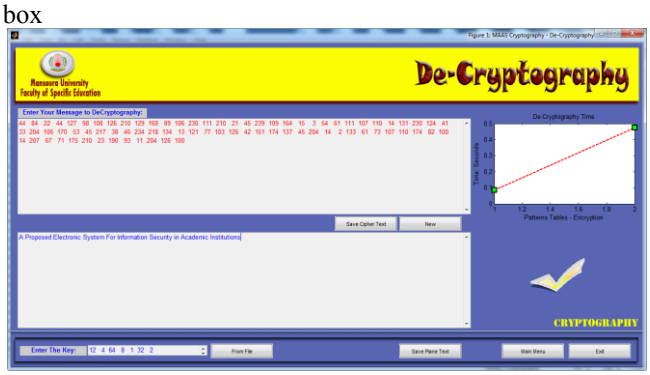


Fig. 9: A Correct Entry of the Cipher ID with the Requested Value of "GK"

VI. PERFORMANCE EVALUATION

The evaluation of cryptography and de-cryptography performance is depending on certain parameters as:

- Plaintext length.
- Cipher text length.
- Genetic key length.
- Generate key time.
- Formulate patterns tables' time.
- Encryption time.
- Decryption time.

To illustrate the high performance of the proposed system has been tested above factors on the following plain text:

"A Proposed Electronic System for Information Security in Academic Institutions"

The results were as shown in tables 1, 2:

TABLE 1: PARAMETER LENGTH EVALUATION

Factors	Values
Plaintext Length	78 byte
Cipher Text Length	130 byte
Genetic Key Length	3 byte

TABLE 2: PARAMETER TIME EVALUATION

Parameters	Time in Sec
Generate Key Time	0.0585
Formulate Patterns Tables Time	0.0033
Encryption Time	0.3234
Decryption Time	0.3176
Total Time	0.7028

In order to measure the effectiveness of the proposed system experiments were conducted with change the genetic key length and plain text length and the results were as shown in table 3.

TABLE 3: CRYPTOGRAPHY RESULTS

No.	Key Length (Bits)	Cipher Text Length (Bits)	Iteration for GK generator	Generate Key Time (Sec)	Patterns Tables Time (Sec)	Encryption Time (Sec)	Decryption Time (Sec)
1	24	1040	2	0.0585	0.0033	0.3234	0.3176
2	32	1248	3	0.0249	0.0098	0.3488	0.3492
3	40	1000	2	0.0056	0.0251	0.2805	0.2705
4	48	832	3	0.0358	0.0450	0.3117	0.3003
5	48	832	2	0.1086	0.0421	0.3053	0.3451
6	56	720	2	0.0465	0.0573	0.2904	0.3000
7	56	632	2	0.0220	0.0320	0.2143	0.2110
8	64	624	3	0.0241	0.0873	0.5735	0.5005
9	64	624	2	0.0158	0.0881	0.5815	0.5441
10	64	624	4	0.0542	0.0899	0.6010	0.6314
Average Time				0.0396	0.048	0.383	0.377

Table is shown that every time is encrypted text generated a new key is different from the keys that generated in the previous times. There is also an inverse relationship between the length of the generated key and the size of the cipher text as shown in figure 10. So that the greater key length which used in the encryption processes reduces the size of cipher text to be the cipher text size equal to plain text size.

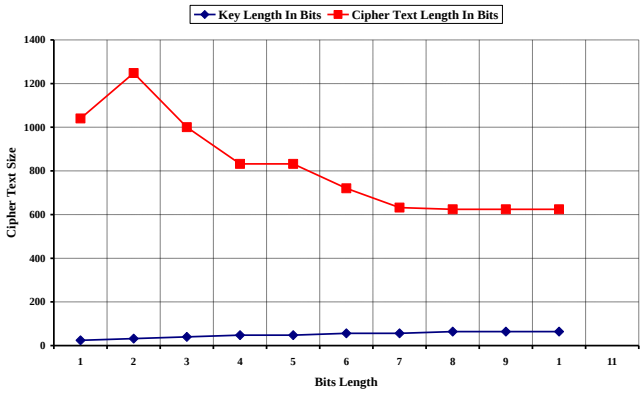


Fig. 10: Relation between bits length and cipher text size.

Also the experiments focused on encryption and decryption time of MAAS compared with Data Encryption Standard (DES) and Advanced Encryption Standard (AES).

The data encryption standard (DES) is widely used to encryption of large amount of data based on symmetric encryption algorithm. DES uses two basic techniques of encryption namely confusion and diffusion. The relationship between plaintext and cipher text is achieved by a key dependent substitution in the round function is denoted confusion. Whereas the plaintext is diffused throughout the cipher text - making every part of the Cipher text dependent on every part of the plaintext- by the swapping between stages denoted diffusion. The advantages of DES are concentrated in the symmetric encryption attractiveness in un-concerted environments and often using a random session key secretly sent by the digital envelope.

The evaluation results from the MAAS and the other models indicate that the proposed model achieves a very good performance in term encryption and decryption time. The time of the MAAS and the other two compared models, DES and AES, is shown in figures 11, 12.

As shown in figure 11, the average encryption time value for MAAS is 21.514 Sec is decreased by 66.1% and 55.93%, when compared with DES and AES respectively. Where, the average of decryption time value is 21.684 Sec for MAAS which decreased by 30.85% and 15.99% from other compared models DES and AES respectively as shown in figure 12.

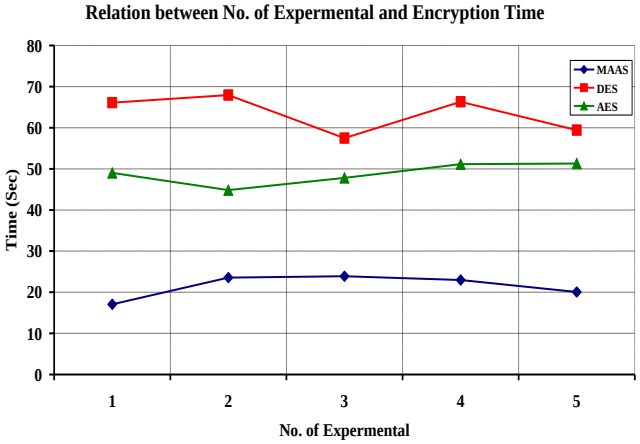


Fig. 11: Encryption Time

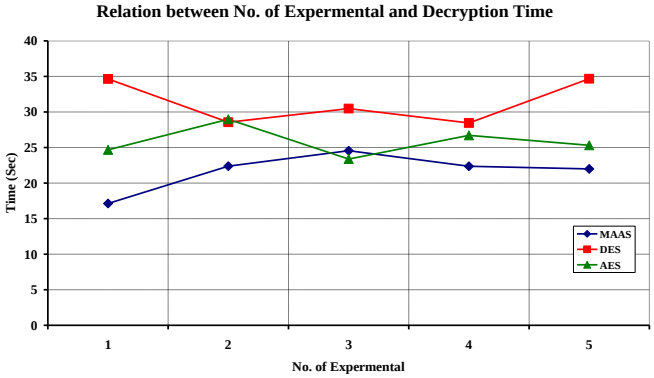


Fig. 12: Decryption Time

Figure 13 shows the total time values in Sec for encryption and decryption MAAS stages compared by DES and AES models. In encryption processes, the total time values for MAAS, DES and AES are 107.57, 317.21 and 244.09 Sec respectively. Where, in Decryption processes, the total time values for proposed model, DES and AES are 108.42, 156.79 and 129.06 Sec respectively as shown in figure 13.

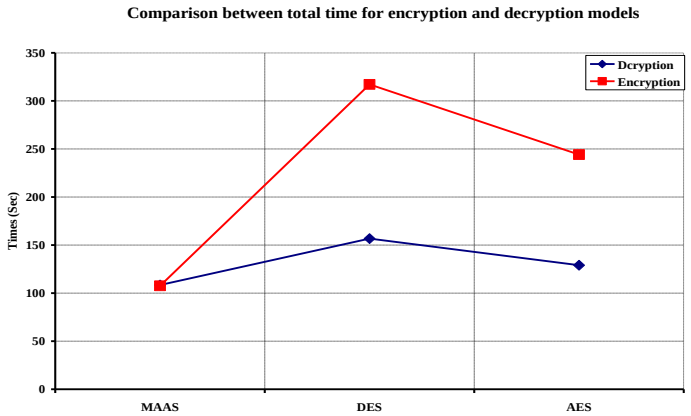


Fig.13: Total Encryption and Decryption time for different models

VII. CONCLUSION

In this paper, we have proposed a new approach for academic institutions information security (MAAS). MAAS integrated between two of famous artificial intelligent techniques namely genetic algorithm and pattern recognition. Both techniques are contribute to significant encryption Performance, encryption speed and are suitable for real-time cryptography and transmission as shown in results.

REFERENCE

[1] Sadowsky G. and et al. (2003): Information Technology Security Handbook, Computer Security Institute, San Francisco, USA.

[2] Technology Security Expert Advisory Group. (2007): Secure Your Information: Information Security Principles for Enterprise Architecture, Technology Security Expert Advisory, USA.

[3] George D. and et al. (2000): Information Security Primer, EPRI and Secure Computing Corporation, USA.

[4] Cherdantseva Y. and Hilton J. (2013): Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals. In: Organizational, Legal, and Technological Dimensions of Information System Administrator. Almeida F., Portela, I. (eds.). IGI Global Publishing.

[5] Almarimi A. and et al. (2012):A NEW APPROACH FOR DATA ENCRYPTION USING GENETIC ALGORITHMS, Advances in Intelligent Systems and Computing, Vol. 167, PP. 783-791.

[6] Preneel B. (2010): Understanding Cryptography, Springer Heidelberg Dordrecht London New York, USA.

[7] Behrouz A. (2007): Cryptography & Network Security, Tata McGraw-Hill, New Delhi, India.

[8] D. Singh, P. Rani and R. Kumar (2013): To Design a Genetic Algorithm for Cryptography to Enhance the Security. "International Journal of Innovations in Engineering and Technology", Vol. 2, Issue. 2, PP. 380-385.

[9] A. Jassim (2013): Randomly Encryption Using Genetic Algorithm, International Journal of Application or Innovation in Engineering & Management, Vol. 2, Issue. 8, PP. 242-246.

[10] S. Mishra and S. Bali (2013): Public Key Cryptography Using Genetic Algorithm, International Journal of Recent Technology and Engineering, Vol.2, Issue.2, PP.150-154.

[11] M. Barati end et al (2013): Features Selection for Ids in Encrypted Traffic Using Genetic Algorithm, Proceedings of the 4th International Conference on Computing and Informatics, University Utara Malaysia, Sarawak, Malaysia, PP.279-285.

[12] M. Kumar end et al (2013): Encryption Algorithm Using Genetic Algorithm, 2nd National Conference in Intelligent Computing & Communication, Greater Noida, INDIA.

[13] J. Kumar and S. Nirmala (2012): Encryption of Images Based on Genetic Algorithm – A New Approach, Advances in Computer Science, Eng. & Appl, AISC 167, PP. 783–791.

[14] R. Toemeh, S. Arumugam (2007): Breaking Transposition Cipher with Genetic Algorithm, Electronics and Electrical Engineering, Vol. 79, No. 7, PP 75-78.

[15] G. Patel (2008): Genetic Algorithm for Cryptanalysis, Birla Institute of Technology & Science (BITS) Pilani, USA.

[16] S. Goyat (2012): Cryptography Using Genetic Algorithms (GAs), Journal of Computer Engineering, Vol. 1, Issue. 5, PP. 6-8.

[17] L. Sharma, B. Kumar Pathak and R. Sharma (2012): Breaking of Simplified Data Encryption Standard Using Genetic Algorithm, Global Journal of Computer Science and Technology, Vol. 12, Issue. 5, PP. 55-60.

[18] M. Gen and R. Cheng (2008): Network Models and Optimization Multiobjective Genetic Algorithm Approach, Decision Engineering, Springer-Verlag, London.
[19] A. Kumar (2010): Network Design Using Genetic Algorithm, Ph.D, Saurashtra University, Rajkot, INDIA.
[20] R. L. Haupt and S. E. Haupt (2004): Practical Genetic Algorithms, a john wiley & sons, inc., publication, Canada.
[21] A. Kumar and M. K. Ghose (2009): Information Security using Genetic Algorithm and Chaos, Information Security Journal: A Global Perspective, Vol. 18, Issue. 6, PP. 306-315.
[22] A. Soni and S. Agrawal (2012): Using Genetic Algorithm for Symmetric key Generation in Image Encryption, International Journal of Advanced Research in Computer Engineering & Technology, Vol. 1, Issue. 10, PP. 137-140.

