International Journal on New Computer Architectures and Their Applications (IJNCAA) 2(1): 225-236
The Society of Digital Information and Wireless Communications, 2012 (ISSN: 2220-9085)

Innovative Approach to Improve Hybrid Cryptography by Using DNA Steganography

Mohammad Reza Najaf Torkaman[1], Nazanin Sadat Kazazi[1], Azizallah Rouddini[2]

[1] Faculy of Computer Science and Information System, UNIVERSITI TEKNOLOGI MALAYSIA (UTM), Kuala Lumpur, Malaysia
[2]Faculty of Management and Human Resources Development, UNIVERSITI TEKNOLOGI MALAYSIA (UTM), Kuala Lumpur, Malaysia

{rntmohammad2@live.utm.my, sknazanin2@live.utm.my, Azizroudini@gmail.com}

ABSTRACT

There exists a big demand for innovative secure electronic communications while the expertise level of attackers increases rapidly and that causes even bigger demands and needs for an extreme secure connection. An ideal security protocol should always be protecting the security of connections in many aspects, and leaves no trapdoor for the attackers. Nowadays, one of the popular cryptography protocols is hybrid cryptosystem that uses private and public key cryptography to change secret message. In available cryptography protocol attackers are always aware of transmission of sensitive data. Even non-interested attackers can get interested to break the ciphertext out of curiosity and challenge, when suddenly catches some scrambled data over the network. First of all, we try to explain the roles of innovative approaches in cryptography. After that we discuss about the disadvantages of public key cryptography to exchange secret key. Furthermore, DNA steganography is explained as an innovative paradigm to diminish the usage of public cryptography to exchange session key. In this protocol, session key between a sender and receiver is hidden by novel DNA data hiding technique. Consequently, the attackers are not aware of transmission of session key through unsecure channel. Finally, the strength point of the DNA steganography is discussed.

KEYWORDS

Cryptography**;** Cryptography Protocols; DNA steganography; Innovation; creativity;

1 INTRODUCTION

One of the scientific topic investigations in disciplines has been creativity [1]. The human creative thinking capabilities and the solving of problems make possible by evolvements of computer science and technology of information. On the other hand, the fundamental cells of an innovative system are the talents of entrepreneurial and creativity [2]. In addition, Creativity has defined an evident that crates the useful and new ideas such as involving the discovery of scientific, the invention of social, the innovation of technological

and the imagination of artistic in the many human activity [3].

Cryptography is the science and art of secret writing that it cannot form without creativity actions with entrepreneurial talent [4][5][6]. It studies some mathematical techniques and provides mechanisms necessary to provide aspects related to information security like confidentiality, data integrity, entity authentication, and data origin authentication [6].

Symmetric algorithms are cryptosystems that either a secret key will be shared for both encryption and decryption [7][8]. The algorithms of symmetric cryptosystems are very strong against possible attacks, but mainly weakness of symmetric cryptosystems is brute-forcing the secret key. This characteristic creates the biggest critical act in any cryptosystem that uses symmetric algorithms which is distribution of the shared secret between the two parties like DES algorithms [8] [9].

Asymmetric algorithms use different values for encryption and decryption and do not need to share secret between two parties. Each party only has to keep a secret of its own. The earliest foundation of asymmetric algorithms known as public key cryptosystems comes from key exchange problem of symmetric algorithms. In 1976, Whitfield Diffie and Martin Hellman proposed a method were the sender and receiver do not have to share a secret. That was the first work on hybrid cryptosystem [6][7][10].

The information of this study shows that how DNA steganography can be used in the information security. In fact proposed approach is innovative concept in hybrid cryptography.

1.1 Innovation and Creativity

One of the scientific subject investigations in disciplines has been creativity [1]. The human creative thinking capabilities and the solving of problems make possible by evolvements of computer science and technology of information. For instance, According to Ratten internet capabilities make possible mobile banking and it has caused that the most people can use from electronic all communication, which has enable them to market products and services by the mobile phones [12]. Moreover, it has increased and improvement these capabilities through gain entrance to the resources of large information and the interaction of multimodal with algorithms [13] [11]. On the other hand, the fundamental cells of an innovative system are the talents of entrepreneurial and creativity [2] [14] .In addition, education and research in entrepreneurship are developing as a critical area of a study program for the students of computer science [15].

Entrepreneurship matters are greatly believed that it can be significant to the global modern business [16]. Nowadays, there is a great correlation among knowledge, education, economic growth, and information and communication technology in the knowledge-based economy [17]. Therefore, what is entrepreneurship?

A wide of domain activeness and processes has covered the meanings of entrepreneurship, involving foundation of an organization and innovation [18].

Based on Styles and Seymour, claimed that Entrepreneurship has a direct attention to distinct or individual opportunistic actions [19]. These activities are forcefully connected with innovation that they produce the value

and give birth risk. Although, the scholars have had a different definition from the word of the entrepreneurship, they accepted that entrepreneurship connects with the creative activity of something new [20] [21]. In addition, Creativity has defined an evident that crates the useful and new ideas such as involving the discovery of scientific, the invention of social, the innovation of technological and the imagination of artistic in the many human activity [3][22].

1.2 Key Management in cryptography

To create the best cryptosystem, it is feasible to use symmetric algorithms since they are extremely fast in process and secure in algorithms comparing to asymmetric algorithms. However, the distribution of the secret key over an insecure channel is one of the most challenging topics in cryptosystems [4][7][8][9][10][23][24][25][26].
Here on wards, this paper will express viable information on how to incorporate symmetric algorithms with other methods to provide a new method that holds a strong security in many aspects. There are several steps in key management of a cryptosystem. The main ones are: Key generation, Key distribution, and Key revocation [27]. The distribution of the key is the critical step since it is the most interest of Eve to intercept and catch the key. If the cryptosystem uses the strongest algorithm with best generated key but distribution of the key has lack of security, the overall security of that cryptosystem would be zero. Diffie Hellman algorithm was the establisher of key distribution over insecure channels [28]. Some of the concerns of security in key management have been discussed in [29]:

i. **Data confidentiality** – the first role of cryptography is to protect data confidentiality. Given that keys have a major role in security of cryptosystem, they should fulfill this obligation.

ii. **Secure key distribution** – the keys should be well protected in the process of distribution to parties. They are the easiest way that Eve can get access to encrypted data. There are many points that Eve can get opportunity to attack the keys like key distribution, key updates, key revocation, etc.

iii. **Data authentication** – the keys can be a tool to authenticate the communicating party. Public key cryptography can provide this feature.

iv. **Efficiency of key management** – nowadays most of the cryptosystems rely on centralized key certification authorities for key management processes. Here all value and significance of the security of the keys is granted to these authorities. Consequently, the efficiency and security performance of these certification authorities has a great deal in providing security to communicating parties.

1.3 Public Key Methods Hybrid Cryptosystem

The best existing method for a cryptosystem to provide best security possible seems to be hybrid cryptosystems. They are called hybrid because they are a mixture of symmetric and asymmetric algorithms, using

security and speed of symmetric together with asymmetric strength in secure key distribution, authentication, etc.
Public key methods have much strength but there are lots of drawbacks to these cryptosystems. The following is a short list of these drawbacks:

1. Public key methods are very low in speed [7]. The usage of symmetric algorithms has decreased this problem but this still is an issue in asymmetric role.
2. The asymmetric algorithms are very vulnerable to chosen-plaintext attacks. This attack is effective because of the fact that encryption key is published [7][30][31].
3. Another consideration in asymmetric algorithms is algorithmic attacks. Even though factoring *n* is known as nearly impossible calculation, but researchers have shown the possibility of this attack especially with the growth of technology and speed of computer's processors [32].
4. Although the database that holds the value of the public keys are very secured and only authorized user can modify it, there still exists a high risk of Eve's chance in modifying the data of the database[7].
5. Man-in-the-Middle-Attack is the most popular attak to public key cryptosystem[7]. Interlock Protocol [33] has been proposed to solve this problem but there are still big arguments against the efficiency and effectiveness of this protocol [34].

Certification Authorities (CA) were a solution to public key distribution. But there still exists critical issues for this method as well, such as the terms certificate, trust, how to choose the authority on top of everyone, and how much of a time period that authority is trusted [7].

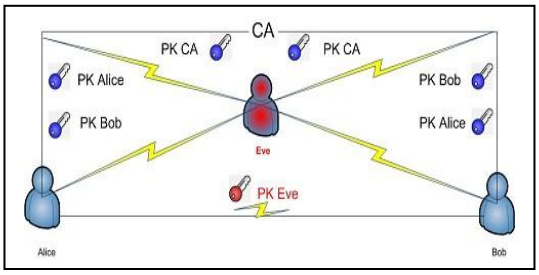

Figure 1: Conventional Hybrid Cryptosystem

1.4 Steganography

Steganography is the science and art of information hiding. Cryptography and Steganography have same mission with different method, the former changes the content but latter covers the existence of the information. In Greek's literature, Steganography means "covered writing" [35].
The famous traditional story of Steganography is known as Simmons' Prisoner's Problem. Two of the prisoners are planning for an escape; they have to discuss the plan without getting the attention of the guards. The only practical way for them is by having a normal insusceptible communication that carries the message in a hidden way [36].
In Steganography ancient history, Histiaeus in 5th century BC used a steganography technique to send his message by tattooing shaved head of a slave and sending him as a carrier when the hair grew back. Another historical story is a reinvention of a Chinese old method of secret writing by an Italian mathematician using a paper mask that holds some holes and will be put on a blank page, the holes should be filled up

with letters of the secret message, and when the mask is removed, the blank spaces between letter will be filled up with other letters to make a normal sentence so the message looks differently, but when the mask is put back, the letters of the secret message will be distinct. The mask is shared between two parties. [37]

Every method that includes Steganography uses an algorithm that embeds the data into a carrier and employs a detector function that retrieves back the embedded information. The embedding function has to use a secret key that only authorized parties are aware of. The function detects and recovers the message using the secret key. The hardest part in embedding the data is to not to create any detectable changes in carrier media while embedding. The most important point here is although detection of embedded data and secret data does not necessarily results to recovering it, but the risk of the chance of attacker's success is very high, hence avoiding obvious modifications is a must. The other important point to consider is that avoiding detectable changes does not guarantee invisibility of embedded data [38][39].

Some requirements of Steganography are capacity, imperceptibility, and robustness. Where, each concentrates respectfully on: the biggest amount of data that can be embedded in the carrier, avoiding unauthorized detection of embedded data, and strength of embedded data against being removed or damaged by operations done on the carrier like copy, cut, and paste [36].

1.4.1 Fingerprinting and Watermarking

Fingerprinting and watermarking is an application of steganography that mostly is used for copyright protection and purposes. This allows the owner to search in the internet and detect illegal use of his product. Also, sometimes when there is a restriction in delivering the information of a specific image, it can be embedded into the image so carried everywhere together with the image. Fingerprinting and watermarking differ when used for protection of intellectual properties. Watermarking embeds the copyright so when distributed to all users, any point of time the copyright can be retrieved. With fingerprint, however, the owner embeds different serial numbers in the product and can trace thirds party suppliers of their products. One of the most important jobs that these techniques provide is changes in the carrier does not reflect the embedded data [40].

1.4.2 Least Significant Bit Insertion

Steganography algorithms can be categorized into two categories of spatial/time domain and transform domain techniques. LSB method is spatial/time domain type of steganography where the information is embedded in the spatial domain of the image or time domain of audio carrier. This method plays with the binary representation of the hidden data. The progress is that the least significant bit of a binary number of the carrier media which is the most right digit of the binary number will be alternated to the value of binary number of the message to be embedded. Any changes in the

carrier will directly affect the embedded data like cropping, compression, color degradation, and so on [23]. This method is best effective when applying on gray scale images. Rather than that, it is vulnerable to steganalysis [40].

1.4.3 Transform Domain Based Steganography

As it is discussed, LSB method is spatial/time domain type of steganography where the information is embedded in the spatial domain of the image or time domain of audio carrier. However, Transform domain methods use different parts of the media to embed the data. They operate on three different methods of: Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), and Discrete Wavelet Transform (DWT) [40].

1.4.4 Text Information Hiding Steganography

Texts are one of the most important media used today in telecommunication technology. The characteristics of being exceedingly efficient in transmissions, occupying fewer resources, along with its intelligible meaning put together to make it the universal most used media [40].

1.4.5 DNA Steganography

Nowadays, scientists work on different kind of Steganography algorithms to ameliorate the security of system. There are many Steganography algorithms to hide the secret data in to the host carrier. DNA Steganography is one of the cutting edge techniques in this area.

Basic concepts of the DNA Steganography are based on the properties of natural DNA sequences in the cell. In molecular biology, genetic information is stored in deoxyribonucleic acid which is known as DNA in the cells. DNA is made by four nucleotides which are thymidine (T), cytidine (C), guanosine (G), and adenosine (A). These bases are linked by backbone of DNA strands which are sugar components and phosphate groups. This backbone identifies the direction of the DNA strands [41].

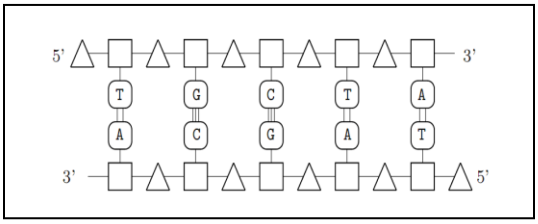

Figure 2: The Backbone of DNA strand [23]

Each single strand is linked by hydrogen bond to make the DNA double strand. The standard situation of nucleotides allows to make a hydrogen bind between C and G; or A and T. This complementarily standard rule is known as Watson-Crick base-pairing. C and G are bonded by triple hydrogen bond, although A and T are linked by double hydrogen bond. This complementarily concept is the fundamental issue in genetic activities that leads to double DNA strands are twisted together and make DNA double helix. The mixture of these basic nucleotides which are thymidine (T), cytidine (C), guanosine (G), and adenosine (A) make the long polymer strands which able to make massive amount of combinations of DNA double helix that stores the every

living features and properties of creatures such as human and mammal.
There are several DNA data hiding approaches based on [42] [43] [44]. It means that scientists work on real molecular DNA. Although, these works are very worthwhile and introduced new area of data hiding approaches, they have some drawbacks. One of the most popular disadvantages of natural DNA-based data hiding is the biological errors like mutation and difficulty of implementation of DNA system. Luckily, Shiu worked on three different data hiding methods based on DNA-coding technology. He proved that his algorithm is robust and do not need equipped laboratory. Actually, DNA reference sequence S is chosen and sample message N is mixed with it to produce final data hiding result ($S^{'}$). Moreover, he compared these three algorithms based on capacity and payload. DNA reference sequence can be selected from different DNA database. One very important DNA database is EBI that provides fundamental genetic information [45].

2 THE PROPOSED PROTOCOL: CRYPTOGRAPHY-STEGANOGRAPHY TEGANOGRAPHY PROTOCOL

As discussed earlier, public key methods have much strength but there are lots of drawbacks to these cryptosystems. We are proposing a technique for best security possible using a combination of cryptographic and steganography techniques. The method answers to requirements of a secure communication while defeating most of the popular attacks known up until today. The proposed protocol's aim is reducing the usage of public key cryptography.
The structure of proposed algorithm is combinational of concepts of cryptography and steganography. Available cryptography protocols use potential advantages of symmetric and public cryptography. As we know, private key cryptography is strong in terms of their algorithms and public key cryptography can be used to protect symmetric algorithm by distributing its key. However, because of the nature of cryptographic algorithms the attacker is always aware of transmission of sensitive data. Even a non-interested attackers can get interested to break the ciphertext out of curiosity and challenge, when abruptly catches some scrambled data over the network, and who knows, this might be some crucial information of a an organization! So the problem still is how to distribute the secret key of symmetric algorithms.
The existence of transmission of message is hidden by using steganography which propose in this paper. Steganography needs a secret key, which is distributed among two parties for every establishment of new communication, for embedding the data. The steganography method in this paper is DNA-based algorithm to hide secret messages.
Every DNA steganography algorithm has its secret key to extract real message from the carrier. We can employ some different techniques to transfer the steganography key. In this paper, we do not want to focus on approach to exchange DNA steganography, but we can use hybrid cryptosystem based on DNA steganography which is proposed in NajafTorkaman's work [46]. Sender

and receiver use following protocol to exchange the session key.

For the first communication,

1. Alice communicates with Bob to share a secret key (DNA steganography key).
2. Bob receives the steganography key and uses it to embed the symmetric key in a DNA stream
3. Alice receives the DNA stream, extracts the symmetric key and the symmetric connection is established.

For all next communications,

1. Alice embeds a new symmetric key in a DNA stream, sends it to Bob.
2. Using the same DNA Steganography key, Bob extracts the symmetric key and generates a symmetric connection.

The following figure demonstrates a graphical representation of the proposed protocol:

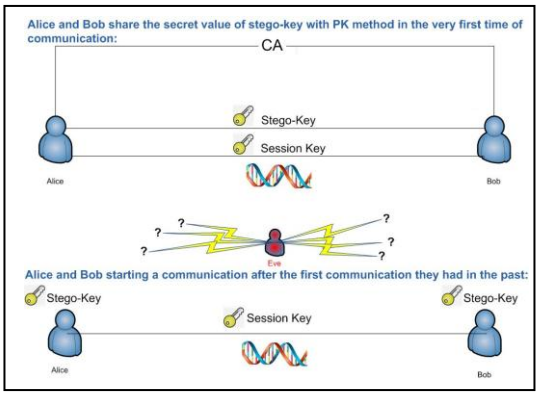

Figure 3: Proposed method – hybrid cryptosystem integrated with DNA Steganography

2.1 Proposed DNA Steganography

Shiu experiment is used as basic information of proposed algorithm in this section to hide the session key [45]. In fact there are different DNA sequences on diverse DNA bank web sites like EBI database (European Bioinformatics Institute) [47]. The proposed algorithm uses the EBI DNA bank to extract 163 million DNA based sequences.

There are two main rules in this DNA steganography process. The first rule is the DNA coding technology rule that is kept secret among the sender and receiver. DNA coding technology is the approach to convert binary data to DNA string. The second one is DNA complementary rule is also kept secret in sender and receiver side. There are six major complementary rules for each letter of DNA sequence. For all letter x, C(x), C(C(x)), C(C(C(x))) is not equal.

AT	TC	CG	GA
AT	TG	GC	CA
AC	CT	TG	GA
AC	CG	GT	TA
AG	GT	TC	CA
AG	GC	CT	TA

Figure 4: Six major complementary rules for each DNA sequence

Moreover, our DNA coding technology rules to convert binary data to DNA string in this paper is based on table following rules. 00 is converted to AA, 01 converted to T, 10 converted to C, 11 converted to GG, 0 converted to A, and 1 converted to G.

The DNA-based data hiding algorithm is divided to two main part sender and receiver process. Sender follows several steps to conceal binary data in the DNA sequence. First, sender extracts reference sequence from EBI database which is accessible publicly or uses DNA coding

technology to convert any binary data and make reference DNA sequence. For instance, the reference sequence is S= 'CGTATCGAATCGATGCAGAT'. In this example secret message is M='10001101'. As we can see the length of reference sequence is 20 and the length of secret message is 8. After that we can use different random generator functions to generate 8 integer random numbers. The random generator function produces numbers from 1 to 20 (length of reference sequence). Finally, the pseudo code algorithm is implemented in MATLAB software to produce the final output. For this example output of the algorithm is s'= 'CGATGATCGGATCGAATGCA'.
Sender can send this DNA string in public channel to receiver.

$S=s_1+s_2+s_3+\ldots+s_m$ = CGTATCGAATCGATGCAGAT
$M=m_1+m_2+m_3+\ldots+m_p$= '10001101'
$A= \{A_1+A_2+A_3+\ldots+A_p\} = \{1, 3, 4, 6, 9, 11, 13, 16\}$

```
  function S'=hide(S,M,A)
  x= size(S,2); // get the length
of reference sequence
  y= size(A,2); // get the length
of set of random number
   for i=1:x
    for j=1:y
  if (i== A(j) && M(j)==1 )
     S'(i)= C(s(i))   // use
complementary rule
  else if  (i== A(j) && M(j)==0 )
       S'(i)= s(i);
  else
  S'(i)=  C( C(s(i))) // use
complementary rule
      end
  end
  end
```

Receiver knows about complementary rule and the DNA reference sequence S. He uses this pseudo code to discover original secret message. As we mentioned C(s(i)) is complementary based on complementary rule . The output of this pseudo code is M which is the original secret message.

```
function S'=extract(S, S')
i=1;
j=1;
x= size(S',2);
for i=1:x
 if (s(i)==s(i'))
      M(j)= 0;
      j=j+1;
 else (s'(i)== C(s(i)))
    M(j)= 1;
  j=j+1;
end
end
```

In connection establishment, sender and receiver transfer steganography key which is complementary rules. This transformation process can be done with different kind of current cryptography or DNA cryptography algorithms. After that session key of communication is transferred by proposed DNA steganography.

2.2 Strength of Proposed DNA Steganography

In proposed DNA steganography, as we mentioned there are six main complementary rules for each letter in DNA sequence. The strength point of the steganography method is DNA reference sequences which are chosen from EBI database. There are approximately 163 million DNA sequences. It is unfeasible for the attackers to find any information about existence of a secret message which is concealed in the DNA sequence. In case the attacker knows that a secret message is embedded in the DNA sequence, it is unfeasible to guess

the correct sequence among 163 million DNA sequences. Therefore the probability of finding the original secret message from 163 million DNA sequences is:

$$\frac{1}{1.63 \times 10^8} \times \frac{1}{6}$$

Proposed DNA steganography algorithm is based on the third algorithm of shiu [45] and he compared different DNA steganography based on capacity and payload. This algorithm has some properties. The first property is using DNA reference sequence from EBI database. Therefore, it is impossible to find correct message among 163 million DNA sequences. The second property is its capacity which is equal to selected DNA string (|S|) that means the payload of this algorithm is zero. Table 1 shows the comparison between proposed algorithm and two other DNA data hiding method which are presented in Shiu's papper [45].

Table 1: A comparison of the different DNA data hiding methods

DNA data hiding method	Capacity	Payload
Insertion	$\|S\| + \frac{\|M\|}{2}$	$\frac{\|M\|}{2}$
Complementary pair	$\|S\| + \|M\|(K + 3\frac{1}{2})$	$\|M\|(K + 3\frac{1}{2})$
Algorithm of this paper	$\|S\|$	0

3 CONCLUSION

Hybrid cryptosystem is one of the post popular algorithms in cryptography to encrypt data. Hybrid cryptosystem is combination of public and private key cryptography. According to the information of this work, asymmetric cryptography brings many disadvantages when used in key distribution protocols. Therefore, in this paper we proposed to decrease the usage of asymmetric cryptography and introduced a novel cryptographic-steganography protocol. Furthermore, we explained the importance of creativity approaches in information security especially in cryptography. The main advantage of proposed cryptography protocol was using innovative DNA steganography techniques to conceal secret session key which is transferred among sender and receiver throughout unsecured channel. In proposed protocol attackers are not aware of exchanging session key which is hidden by DNA data hiding method. The strength point of the DNA steganography algorithm is using DNA reference sequences which are selected from EBI database. We have approximately used 163 million DNA sequences from EBI database. It is impossible for attackers to find whether or not there are secret message hidden in DNA sequences. Even if attackers know a secret message is embedded in DNA sequences, it is impossible to guess the correct sequence among 163 million DNA sequences.

4 REFERENCES

1. VAN LANGEN, P. H. G., WIJNGAARDS, N. J. E. & BRAZIER, F. M. T. Designing creative artificial systems. *Artificial Intelligence for Engineering Design, Analysis and Manufacturing*(2004), 18**,** 217-225.
2. SUN, H. The 3-3-3 framework and 7P model for teaching creativity, innovation and entrepreneurship. *Journal of Chinese Entrepreneurship*,(2011) 3**,** 159-166.

3. THAGARD, P. & STEWART, T. C. The Aha! experience: Creativity through emergent binding in neural networks. *Cognitive science*.(2011)
4. Willett, M., Cryptography old and new, ScienceDirect, Computers & Security, (1982) 177- 186.
5. Lin, H. S., Cryptography and Public Policy, *Journal of Government Information*, (1998) 135–148.
6. Alia, M.A., Yahya, A., Public–Key Steganography Based on Matching Method, *European Journal of Scientific Research*,(2010) 223-231.
7. Schneier, B., Applied Cryptography,New York : John Wiley & Sons, 1996.
8. Kumar, S., & Wollinger, T. ,Fundamentals of Symmetric Cryptography, *Embedded Security in Cars*, (2006) 125-143.
9. Burke, J., McDonald, J., & Austin, T., Architectural support for fast symmetric-key cryptography. *Architectural support for programming languages and operating systems.* (2000) Association of Computing Machinery.Stone, J.V.: Independent Component Analysis: A Tutorial Introduction. MIT Press, Cambridge, MA (2004).
10. Mohapatra, P. K.,Public-Key Cryptography, 2000, Crossroads.
11. Christensen, C. "The Rules of Innovation". Technology Review ,(2002),105 (5): 32–38.
12. RATTEN, V. Mobile Banking Innovations and Entrepreneurial Adoption Decisions. *International Journal of E-Entrepreneurship and Innovation (IJEEI)*(2011), 2**,** 27-38.
13. MAHER, M. L., BONNARDEL, N. & KIM, Y. S. Creativity: Simulation, stimulation, and studies. *Artificial Intelligence for Engineering Design, Analysis and Manufacturing,(2010)*, 24**,** 149-151.
14. Thomke, S. H. . "Experimentation Matters: Unlocking the Potential of New Technologies for Innovation". Harvard Business School Press, 2003.
15. LAWLER, J. A Financial Technology Entrepreneurship Program for Computer Science Students. *Information Systems Education Journal*,(2011) 9**,** 53.
16. LI, X. Entrepreneurial Competencies as an Entrepreneurial Distinctive: An Examination of the Competency Approach in Defining Entrepreneurs,(2009).
17. ZAMFIR, A. & PLUMB, I. Year. Using a Computer-based Model for Developing Business Students' Skills: Case Study on the Regional Application of the Model. *In*, World Scientific and Engineering Academy and Society (WSEAS),(2011) 49-54.
18. GARTNER, W. Who is an entrepreneur? Is the wrong question. *American Journal of Small Business* (1988), 12**,** 11-32
19. STYLES, C. & SEYMOUR, R. G. Opportunities for marketing researchers in international entrepreneurship. *International Marketing Review*,(2006) 23**,** 126-145.
20. AUTIO, E. Creative tension: the significance of Ben Oviatts and Patricia McDougalls articletoward a theory of international new ventures'. *Journal of International Business Studies*,(2005) 36**,** 9-19.
21. HESSELS, J. International Entrepreneurship: Value Creation Across National Borders. *Scales Research Reports*, (2008).
22. Khan, A. M , Innovative and Noninnovative Small Firms: Types and Characteristics. Management Science,(1989) Vol. 35, no. 5. Pp. 597–606.
23. Knudsen, L.R. ,Block ciphers-analysis, design, applications, Doctor Philosohy, Aarhus University, 1994.
24. Stinson, D., Cryptography: Theory and Practice (discrete mathematics and its applications). s.l. : CRC Press, 1995.
25. de Canniere, C., Biryukov, A. , Preneel, B., An introduction to Block Cipher Cryptanalysis, (2006)346 – 356.
26. Vignesh, R.S., Sudharssun, S. ,Kumar, K.J.J. , Limitations of quantum & the versatility of classical cryptography: a comparative study, *Environmental and Computer Science*, (2009) 333 - 337.
27. Chaeikar, S., Razak, S., Honarbakhsh, S., Zeidanloo, H., Zamani, M., & Jaryani, F. Interpretative Key Management (IKM), A Novel Framework, *Computer Research and Development, (2010)*265 – 269.
28. Diffie, W. , Hellman, M. E., New Directions in Cryptography, s.l. : IEEE, *Transactions on Information Theory,(*1976*)* 644 - 654.
29. Boukerche, A., Ren, Y., & Samarah, S. A Secure Key Management Scheme for Wireless and Mobile Ad Hoc Networks Using Frequency-Based Approach: Proof and Correctness. *GlobalTelecommunications Conference* (2008) (pp. 1 - 5). IEEE.

30. Tzeng, W.G., Common modulus and chosen-message attacks on public-key schemes with linear recurrence relations, *Information Processing Letters*, (1999) 153-156.
31. Izmerly,O., Mor, T., Chosen ciphertext attacks on lattice-based public key encryption and modern (non-quantum) cryptography in a quantum environment, *Theoretical Computer Science*,(2006) 308-323.
32. Aboud, S.J., An efficient method for attack RSA scheme. , s.l. : IEEE, *Applications of Digital Information and Web Technologies*.(2009) 587 - 591.
33. Rivest, R.L. , Shamir, A. ,How to Expose an Eavesdropper., *Communications of the ACM*, (1984) 393-395.
34. Bellovin, S.M., Merritt, M., An attack on the Interlock Protocol when used for authentication.,s.l. : IEEE, *Information Theory*. (1994) 273 - 275.
35. Johnson, N. F., Jajodia,S., Exploring Steganography: Seeing the Unseen. s.l. : IEEE, (1998)26 - 34.
36. Lenti, j., Steganographic Methods, *Periodica Polytechnica*, (2000) 249–258.
37. Cheddad, A., Condell, J., Curran, K., Kevitt, P. M., Digital image steganography: Survey and analysis of current methods Signal Processing 90 (2010) 727–752.
38. Fridrich, J., Du, R., Secure Steganographic Methods for Palette Images. Lecture Notes in Computer Science. s.l. : Springer-Verlag, (2000)47-60.
39. Phoenix, S., Cryptography, trusted third parties and escrow, *Bt technol journal* 32 (1997) 45-62 .
40. Guillermo A. Francia, I. T. Steganography obliterator: an attack on the least significant bits. *Proceedings of the 3rd annual conference on Information security curriculum development.* (2006). Association of Computing Machinery.
41. Watson, J. , Crick, F., Molecular structure of nucleic acids: a structure for deoxyribose nucleic acid, *JAMA*, 1993.
42. Leier, A., Richter, C., Banzhaf, W., Rauhe, H., Cryptography with DNA binary strands,BioSystems 57 (2000)13–22.
43. Manacher, G.,A new linear-time on-line algorithm for finding the smallest initial palindrome of the string, Journal of the ACM 22(1975)346–351.
44. Shimanovsky, B., Feng, J. , Potkonjak, M., Hiding data in DNA, in: Revised Papers from the 5th International Workshop on Information Hiding, Lecture Notes in Computer Science 2578 (2002) 373–386.
45. Shiu, H., Ng, K., Fnag, J. F., Lee, R., Huang, C., Data hiding methods based upon DNA sequences, *Information Sciences*, 180 (2010) 2196–2208.
46. Najaftorkaman, M., Shanmuham, B., Abbasy, M., & Ordi, A., Hybrid Cryptosystem with DNA Technology. *International Conference on Information Security and Artificial Intelligence Vol.1*(2010)460-464 .
47. European Bioinformatics Institute Corporation, <http://www.ebi.ac.uk/>.
48. Weihui Dai, Y. Y. BinText steganography based on Markov state transferring probability. *Proceedings of the 2nd International Conference on Interaction Sciences: Information Technology, Culture and Human*. (2009). Association of Computing Machinery.