A Survey of VPN Security Issues

M.A. Mohamed[1], M.E.A. Abou-El-Seoud[1], A.M. El-Feki[2]

[1] Faculty of Engineering-Mansoura University
Mansoura-Egypt

[2] North Delta Electric Distribution Company
Mansoura-Egypt

Abstract

Data security plays a crucial role in modern times; most business is transacted over the internet and even to wireless devices, which is much more vulnerable than when running on an internal network. It can be intercepted by non-authorized people; this explains why considerable effort is being devoted at the current time to data encryption and secure transmission. This paper focuses mainly on performing a comparative study of the existing VPN security and encryption techniques.

Keywords: *Virtual Private Network (VPN), Internet Protocol Security (IPsec), Encryption Techniques*

1. Introduction

Recently secure access to the private sources is considered as of the essential needs. Thus, one of the most efficient and cost-effective ways for granting secure access needs from far path in the organizations is the use of VPN [1]. VPN is a popular service to logically construct a geographically dispersed LAN. This logical private network can securely communicate data using Internet [2]. Most private networks lack data security and allow hackers to have access to read and attack the data directly. A VPN shares a network that data can be passed through the private traffic in the way that only authorized users have access to it. IPsec-based VPNs can be established on different types of networks such as ATM, Frame Relay, MPLS, and internet. Since the internet is cheaper and accessible, however, users prefer to use it instead. There are different types of virtual private networks due to operational requirements, however, several ways to create each of these VPNs are available [3]. IPsec based VPN uses encryption method for data security. In order to make this process possible, VPNs connect and combine public and private networks to each other, encrypt packets that are transferred in the net, and increase the resistance of net in front of hackers attack, data retouch, and robbery [4]. The main purpose of VPNs is to prevent the sniff of data that are being sent in the connection platform and the other one is to maintain the integrity of untrusted networks [5]. The next of this paper is organized as follows; section-2 provides the related work, section-3 present IPsec overview, section-4 introduces VPN encryption methodologies, and section-5 presents conclusions.

2. Related Work

The purpose of VPNs is to get access to common sources. Because the connection between these sources is secure, organization can allow its customers and partners to have access to information. Considering VPNs from user's point of view, they can be noticed as a point to point connection between computers and servers [6].

Ram raj [7] proposed a new encryption protocol for data in VPN and a management key that in this model VPN server is a trusted one. In this model VPN server is a trusted one. In this method, Customer presents his request to VPN server and it assigns a key value for customer. Thus, customer begins encrypting data by using this key and advanced encryption standard AES. In this method, the customer receives a public key and with this key the user is able to send data. There is a private key in VPN server that enables the customer to identify the value of the main key. And by RSA encryption algorithm can decode the coded information again, so we can say this method has high security.

M.C. Nicalescu [8] has presented IP mobile security in VPNs. At first AH, ESP examined the defined protocols in IKE in IPsec-IETF architecture. Based on these protocols, protection against denial of viruses, sniff and the other active dangers was discussed. This paper developed this discussion to a large scope called "Internet". In which the use of secure tunneling as a main protective mechanism was tested.

Elkeelany et al. [9] look at the processing overhead from employing Data Encryption Standard (DES) (for confidentiality) and Message Digest (MD5) Secure Hash Algorithm 1 (SHA-1) (for authentication security) in conjunction with IPsec. [10] Extends this study by jointly considering the Advanced Encryption Standard (AES), which is not considered in [9]. AES is quite important as it

is the replacement of DES and 3DES for confidentiality services.

Miltchev et al. [11] present a benchmark-based investigation of the performance of IPsec in an OpenBSD system. The same work examines the benefits of using hardware accelerators for speeding up the cryptographic processing. Ganesan et al. [12] perform an experimental evaluation of deploying security algorithms such as, RC4, RC5, MD5 and SHA-1, on low-end embedded systems (Atmel AVR, Mitsubishi M16C, StrongARM, Xscale), as well as on general-purpose systems (SPARC).

In paper [13] consider the performance of encryption algorithm for text files, it uses AES, DES and RSA algorithm and is evaluated from the following parameters like Computation time, Memory usage, Output bytes. First, the encryption time is computed. The time is taken to convert plain text to cipher text is known as encryption time. Comparing these three algorithms, RSA takes more time for computation process. The memory usage of each algorithm is considered as memory byte level. RSA takes larger memory than AES and DES. Finally, the output byte is calculated by the size of output byte of each algorithm. The level of output byte is equal for AES and DES, but RSA algorithm produces low level of output byte.

In paper [14], the selected algorithms are AES, 3DES, Blowfish and DES. By using these algorithms the performance of encryption and decryption process of text files is calculated through the throughput parameter. Encryption time is calculated as the total plaintext in bytes encrypted divided by the encryption time. Decryption time is calculated as the total plaintext in bytes decrypted divided by the decryption time. As a result mentioned in the paper [14], it is said that Blowfish algorithm gives the better performance than all other algorithms in terms of throughput. The least efficient algorithm is 3DES.

In paper [15], discuss the performance evaluation of AES and BLOWFISH algorithms, and the parameters are Time consumption of packet size for 64 bit encodings and hexadecimal encodings, encryption performance of text files and images are compared with these two algorithms and calculate the throughput level, Throughput of encryption = Tp/Et

Where;

Tp: total plain text (bytes)

Et: encryption time (second)

The simulation results shows that Blowfish has better performance than AES in almost all the test cases [15].

3. IPSEC Overview

IPsec [16] is a developing standard for providing security at the network layer of the Internet. It facilitates the authentication of the communicating entities, allows them to set up secure IP channels for data exchange, and provides a framework for the employment of different cryptographic algorithms depending on the level of security required by the users and their applications.

IPsec provides two choices of security service through two distinct security protocols: the Authentication Header (AH) protocol [17], and the Encapsulating Security Payload (ESP) protocol [18]. The AH protocol provides support for connectionless integrity, data origin authentication and protection against replays, but it does not support confidentiality. The ESP protocol supports confidentiality, connectionless integrity, anti-replay protection and optional data origin authentication. Both AH and ESP support two modes of operation: transport and tunnel. The transport mode of operation provides end-to-end protection between the communicating end-points by encrypting the IP packet payload. The tunnel mode encrypts the entire IP packet (both IP header and payload) and encapsulates the encrypted original IP packet in the payload of a new IP packet. This fact guarantees that no part of the initial IP packet is exposed to potential threats as the new IP packet is transmitted through intermediate nodes of the network.

IPsec provides an open framework for incorporating a wide range of different cryptographic algorithms for the actual cryptographic task of transforming the original plaintext messages into the transmitted ciphertext. Most ciphering algorithms that are used in conjunction with IPsec are iterative block ciphers. They break the original user data packets into basic blocks of constant size, which are then encrypted independently through a number of encryption rounds. The characteristics of such ciphers depend on the choice of block size, key size and number of rounds. Larger block sizes lead to greater security, but on the other hand reduce the encryption/decryption speed [19]. Similarly, larger keys lead to greater security, but also decrease the encryption/decryption speed. A ‘‘number-of-rounds’’ parameter is usually used for specifying the number of repetitions of the basic encryption process on each basic block of data. In the remaining part of this section, the most prominent ciphering algorithms used in conjunction with IPsec are briefly presented.

4. VPN Encryption Methodologies

In this section, several VPN encryption techniques will be introduced. The problem statement, the main objectives, and the main idea of each methodology will be studied. The most common classification of encryption techniques can be shown in Fig. 1.

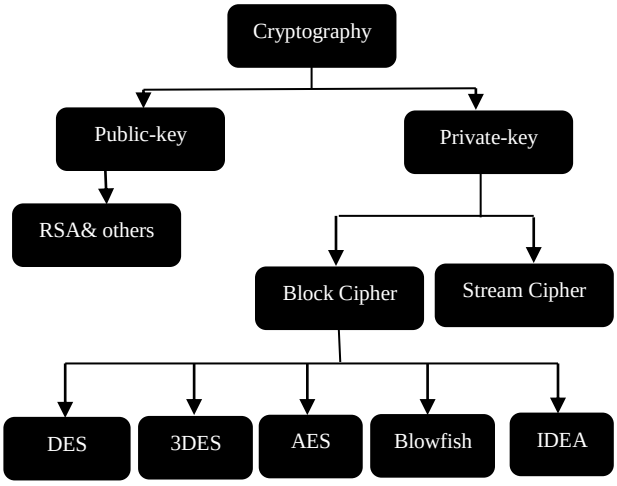

Fig.1 classification of encryption techniques

Stream cipher is one of the simplest methods of encrypting data where each bit of the data is sequentially encrypted using one bit of the key as shown in Fig. 2 [20].In stream cipher, the plain data M is modulated by the random key sequence K. The XOR operation often acts as the modulation operation. The research topic is how to generate the random key sequence [20].

In order to make a stream cipher more difficult to crack, one could use a crypto key which varies in length. This would help to mask any discernible patterns in the resulting cipher data [21]. In fact, by randomly changing the crypto key used on each bit of data, one can produce cipher data that is mathematically impossible to crack. This is because using different random keys would not generate any repeating patterns which can give a cracker the clues required to break the crypto key. The main advantage of the stream cipher is that it is faster and more suitable for streaming application but its main disadvantage is that it is not suitable in some architecture [22].

4.1 RC4 Algorithm

RC4 is the most widely used stream cipher in software applications [23]. RC4 is a symmetric key algorithm. The same algorithm is used for both encryption and decryption. It was designed by Ron Rivest in 1987 and kept as a trade secret until it leaked out in 1994. RC4 has a secret internal state which is a permutation of all N = 2n possible n bits words [23-24]. In the algorithm the key stream is completely independent of the plaintext used. It uses variable key length and very quick in software; the way in which keys are generated for use as input to RC4 is its problem [23-25].

The encryption/decryption process as following [23-24]: (i) Create two string arrays, (ii) Initial one array with numbers from 0 to 255, (iii) Fill the other array with the chosen key, (iv) Randomize the first array depending on the array of the key ,(v) Randomize the first array within itself to generate the final key stream , and (vi) XOR the final key stream with the plain data to be encrypted to give cipher data or with cipher data to be decrypted to give reconstruct data [24].

A known attack on RC4 is a distinguisher attack. The goal of this attack is to distinguish output key stream of RC4 from random key stream. For RC4, such distinguishers are practically impossible to avoid given a suitably large key stream so; the way in which keys are generated for use as input to RC4 is its problem. However, in most application this does not cause any security problems since the actual use of RC4 is not intended to be secret. RC4 is very fast in software. However, in hardware RC4 does not operate faster. In certain applications requiring high speed dedicated hardware this may cause some problems [25].

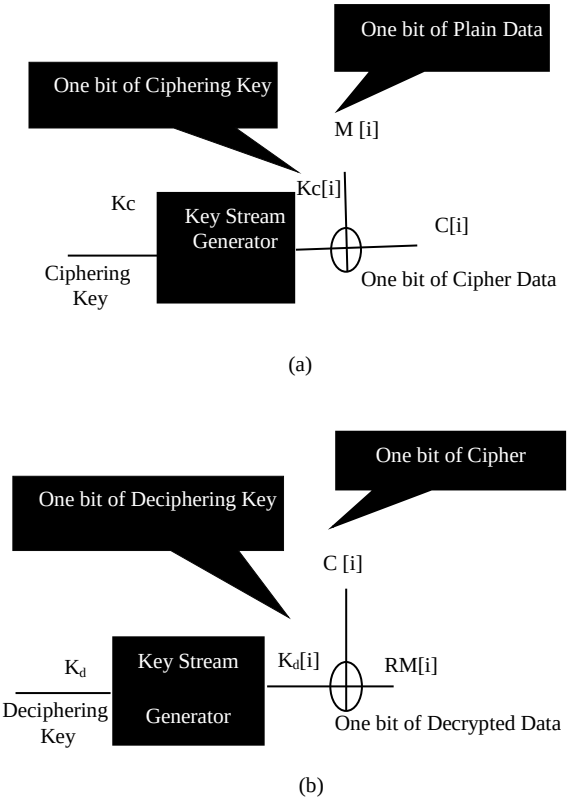

Fig. 2 Stream (a) Ciphering and (b) Deciphering

4.2 Data Encryption Standard algorithm

DES is a block cipher. It encrypts data in blocks of size 64 bits each. 64 bits of plain text goes as the input to DES,

which produces 64 bits of cipher text. The key length is 64 bits. Cryptanalyst can perform cryptanalysis by exploiting the characteristic of DES algorithm but no one has succeeded in finding out the weakness. DES results in a permutation among the 2^64 possible arrangement of 64 bits, each of which may be either 0 or 1. Each block of 64 bits is divided into two blocks of 32 bits each, a left half block L and right half R. The DES [15] algorithm turns 64-bit messages block M into a 64-bit cipher block C. If each 64-bit block is encrypted individually, then the mode of encryption is called Electronic Code Book (ECB) mode. There are two other modes of DES encryption, namely Chain Block Coding (CBC) and Cipher Feedback (CFB), which make each cipher block dependent on all the previous messages blocks through an initial XOR operation [26]. Fig. 3 shows the Encryption Process of DES Algorithm

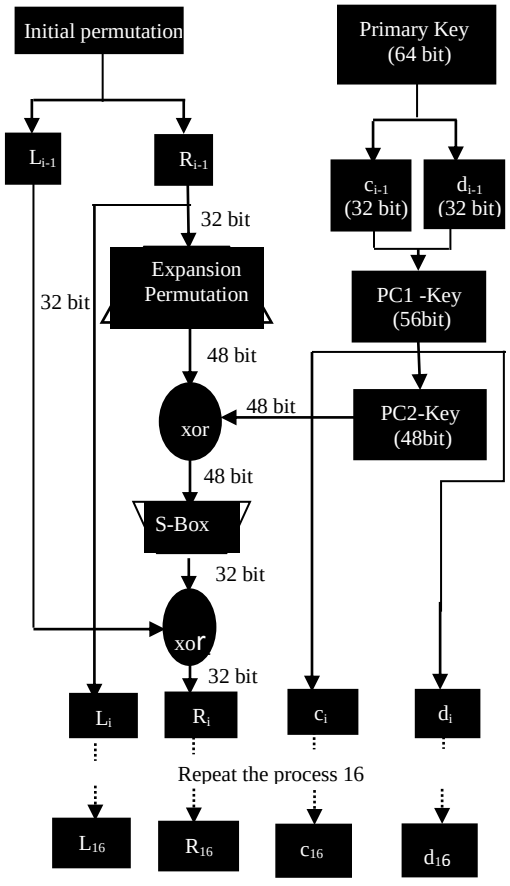

Fig.3 Encryption Process of DES Algorithm

4.3 Triple Data Encryption Standard algorithm

Triple DES (3DES), is no more than a triple repetition of the basic DES encryption: first the data block is DES-encrypted using an initial key, then the encrypted block is decrypted using a second (different) key and then the new block is re-encrypted using the initial key. This process is equivalent to using a larger effective key length of 112 bits. The obvious disadvantage of 3DES is that it runs three times slower than DES on the same platform [27]. Fig. 4 shows the 3DES where k_i is the $_i$th key, p is the original plaintext and C3 is the final cipher text.

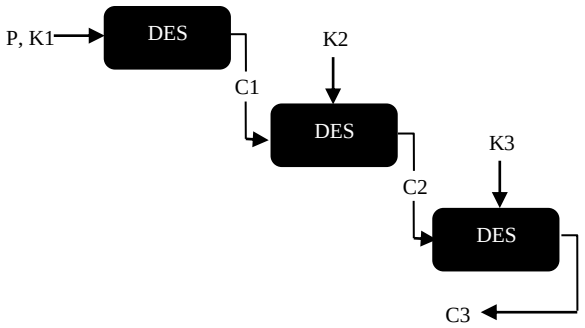

Fig. 4 triple Data Encryption Standard

4.4 Advanced Encryption Standard

The Rijndael algorithm, selected as the algorithm of choice for the new Advanced Encryption Standard (AES), [27-28-29], is one of the newest additions to IPsec. Rijndael is a symmetric block cipher that supports different key and block sizes (128, 192, or 256 bits). The AES standardized version of Rijndael, however, is tied to a fixed block size of 128 bits. The initial block is passed through a round transformation function, which is repeated 10 times (respectively, 12 or 14) under a key length of 128 bits (respectively, 192 or 256). Rijndael combines an increased resistance against attacks with an implementation simplicity and, thus, high execution rate. It has proved to be quite durable against differential, truncated differential, linear, interpolation, and Square attacks, [27-30]. Rijndael is quite versatile as it may also serve as a Message Authentication Code (MAC) algorithm, as a hash function and as a pseudo random number generator. The Message Digest (MD5) [31] and Secure Hash Algorithm 1 (SHA-1), [32], implement so called ‘‘one-way hash functions’’ and are usually used in conjunction with the above cryptographic algorithms for performing authentication. Both of them process input text blocks of 512 bits to generate 128bit and 160-bit hash values, respectively, for the verification of the correct message transfer. Both apply padding to make the plaintext a multiple of 512 bits, but they cannot be directly used as MAC algorithms, as they do not include a secret key. For that reason, they are used in conjunction with keyed-Hashing for Message Authentication (HMAC),

[33]. HMAC is a secret key authentication algorithm that provides a framework for incorporating various hashing functions. The combined HMACMD5 and HMAC-SHA-1 mechanisms are in position to offer data origin authentication and integrity protection services suitable for IPsec.

4.5 BLOWFISH

Blowfish is a symmetric block cipher just like DES or IDEA. It takes a variable-length key, from 32 to 448 bits, making it ideal for both domestic and exportable use [34], and encrypts the data 16 times to make it impossible for a hacker to decrypt it [35] . Bruce Schneier designed Blowfish in 1993 as a fast, free alternative to the then existing encryption algorithms. Schneier made no claims about the security of his algorithm, but over the course of time the algorithm has been carefully studied and is now considered to be a strong algorithm .But the only known attacks against Blowfish are based on its weak key classes [35]. Since then Blowfish has been analyzed considerably, and is gaining acceptance as a strong encryption algorithm. Blowfish is a variable-length key, 64-bit block cipher [34]. The algorithm consists of: (i) key Expansion Part; the P-array consists of eighteen 32-bit sub keys: P1, P2... P18 and There are four 32-bit S-boxes with 256 entries, (ii) Data encryption part [36].

4.6 The International Data Encryption Algorithm

The International Data Encryption Algorithm IDEA is one of the strongest cryptographic algorithms. Idea is a block cipher. It works on 64-bit plain text blocks. The key is longer and consists of 128 bits. IDEA is reversible of DES [37] The 64-bit plaintext block is partitioned into four 16bit sub blocks. Four 16-bit key sub-blocks are required for the subsequent output transformation, and it is generated from the 128-bit key. The key sub-blocks are used for the encryption and the decryption [38] IDEA was used in Pretty Good Privacy (PGP).

5. Conclusions

Due to the importance of information security issue, this paper has concentrated on study of different VPN encryption techniques. The main ideas of some VPN encryption techniques have been introduced. In the future, the fusion or mixing between some of these techniques can be applied to get better performance.

References

[1] A.Thomas and G.Kelley," Cost-Effective VPN-Based Remote Network Connectivity over the Internet", Department of Computer Science, University of Massachusetts,100 Morrissey Boulevard, Boston, MA 02125-3393,2002.

[2] W. Bou Diab, S. Tohme and Carole Bassil "Critical VPN Security Analysis and New Approach for Securing VoIP Communications over VPN Networks", WMuNeP"07, pp 92-96.

[3] IP Encapsulating Security Payload, Network Working Group, Request for Comments: 2406, Obsoletes: 1827, Category: Standards Track, @Home Network November 1998

[4] S.Kadry and W.Hassan, "Design and implementation of system and network security for an enterprise with worldwide branches", Journal of Theoretical and Applied Information Technology, School of Engineering, LIU, Beirut, Lebanon ,2008

[5] "Security & Savings with Virtual Private Networks", available:http://tools.netgear.com/media/whitepapers/VPN_Security.pdf. Last Available 19,04,2014.

[6] M. C. Niculescu, Elena Niculescu, and I. Resceanu, "Mobile IP Security in VPNs", 5th WSEAS Int. Conf. on Data Networks, Communications & Computers, Bucharest, Romania, October 16-17, pp:119-124, 2006.

[7] Netgear, Virtual Private networking, 24,santacalara, 4500 Great America Parkway Santa Clara, CA 95054 USA, Available:http://documentation.netgear.com/reference/nld/vpn/pdfs/FullManual.pdf. Last Available: 19.04.2014.

[8] G. Bastian, E.Carter and C.Degu, "CCSP Cisco Secure PIX Firewall Advanced Exam Certification Guide", Cisco Press, 808, Indianpolis, IN 46240 USA, 2005.

[9] O. Elkeelany et al., "Performance analysis of IPsec protocol: encryption and authentication", IEEE Communications Conference (ICC 2002), 2002, pp. 1164–1168.

[10] C. Xenakis, N. Laoutaris, L. Merakos and I. Stavrakakis" A generic characterization of the overheads imposed by IPsec and associated cryptographic algorithms", computer networks, 50(17):3225-3241, December 2006.

[11] S. Miltchev, S. Ioannidis and A. Keromytis, "A study of the relative costs of network security protocols", USENIX 2002 Annual Technical Conference, Monterey, CA, June 2002.

[12] P. Ganesan et al., "Analysing and modelling encryption overhead for sensor network nodes", WSAN'03, San Diego, California, USA, September 2003.

[13]How-Shen Chang, "International Data Encryption Algorithms", 2004.

[14] "Performance Analysis of AES and BLOWFISH Algorithms ", National Conference on Computer Communication & Informatics", School of computer science, RVS college of arts and science, March 07, 2012.

[15] T. N. T. Zhang, " A study of DES and Blowfish encryption algorithm", Tencon IEEE Conference, 2009.

[16] S. Kent and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[17] S. Kent and R. Atkinson, "IP Authentication Header", RFC 2402, November 1998.

[18] S. Kent and R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, November 1998.

[19] W. Stallings, "Network Security Essentials: Applications and Standards", Prentice-Hall, 2000.

[20] M. Y. Rhee, "Internet Security Cryptographic Principles, Algorithms and Protocols", Seoul National University, Republic of Korea,ISBN: 0470852852 , 2003.

[21] J. Buchmann, "Introduction to cryptography"; 2nd edition, springer, ISBN: 038721156, 2004.
[22] L. Martin, "Introduction to Identity- Based Encryption", ISBN: 1596932384, Febuary 1, 2008.
[23] A. Mousa and A. Hamad, "Evaluation of the RC4 Algorithm for Data Encryption,",PalTel Company, Nablus, Palestine, International Journal of computer Science and Applications,vol.3,No.2 2006.
[24] D. C. Wyld , M. Wozniak ,and N. Chaki, ",Advances in Network Security and Applications";1st edition, Communications in Computer and Information Science , Springer, ISBN: 9783642225390 , August 30, 2011.
[25] Y. Yao, J. Chong, and W. Xingwei," Enhancing RC4 algorithm for WLAN WEP protocol" ,Sch. of Inf. Sci. & Eng., Northeastern Univ., Shenyang, China, ISBN: 9781424451814 ,July 1,2010.
[26] S. Pavithra and E. Ramadevi "Throughput Analysis of Symmetric Algorithms" Int. J. Advanced Networking and Applications Volume:04 Issue:02 Pages: 1574-1577 (2012)
[27] E. Danielyan, "Goodbye DES, Welcome AES", Cisco The Internet Protocol Journal 4 (2) (2001) pp15–21.
[28] S. Frankel, R. Glenn, S. Kelly, The AES-CBC Cipher Algorithm and Its Use with IPsec, RFC 3602, September 2003.
[29] National Institute of Standards and Technology (NIST), Advanced Encryption Standard (AES), Federal Information Processing Standard (FIPS) publication 197, November 2001. Available from: <http://csrc.nist.gov/publications/ fips/fips197/fips-197.pdf>.
[30] R. Phan, Impossible differential cryptanalysis of 7-round Advanced Encryption Standard (AES), Information Processing Letters 91 (1) (2004) 33–38.
[31] R. Rivest, The MD5 Message-Digest Algorithm, RFC1321, April 1992.
[32] D. Eastlake, P. Jones, US Secure Hash Algorithm 1 (SHA1), RFC 3174, September 2001.
[33] C. Madson, R. Glenn, The Use of HMAC-MD5-96 within ESP and AH, RFC 2403, November 1998.
[34] S. Wikipedia ,"Feistel Ciphers: Data Encryption Standard, Blowfish, Kasumi, Tiny Encryption Algorithm, Camellia, Xxtea, Khufu and Khafre, Feistel Cipher", Books LLC, Wiki Series, ISBN: 9781156816967, August 2011.
[35] T. Gonzalez,"A Reflection Attack on Blowfish", Journal of Latex Class Files, Vol. 6, No. 1, January 2007.
[36] T. Nie and T. Zhang,"A Study of DES and Blowfish Encryption Algorithm ",Commun. & Electron. Eng. Inst., Qingdao Technol. Univ., Qingdao, China , ISBN: 9781424445462,2009.
[37] B. Schneier, " Description of a New Variable Length Key, 64-Bit Block Cipher (Blowfish) Fast Software Encryption", Cambridge Security Workshop Proceedings (December 1993), Springer-Verlag, 1994, pp.191-204
[38] William Stallings, cryptography and network security, pearson prentice hall, 2006, 4th edition.

Mohamed Abd-El-Azim received the PhD degree in Electronics and Communications Engineering from the Faculty of Engineering-Mansoura University-Egypt by 2006. After that he worked as an assistant professor at the electronics & communications engineering department until now. He has 60 publications in various international journals and conferences. His current research interests are in multimedia processing, wireless communication systems, and field programmable gate array (FPGA) applications.

Ahmed El-Feki received the M.S of Engineering degree from department of communication and electronics- faculty of engineering- Mansoura University, Egypt, in 2013,He served as a communication and control engineer in north delta electric distribution company from 2003 till now . He has 4 publications in various international journals and conferences. His current research interests are in multimedia processing, wireless communication systems.