International Journal of Computer Science and Software Engineering (IJCSSE), Volume 4, Issue 3, March 2015
ISSN (Online): 2409-4285 www.IJCSSE.org Page: 80-87

New Security Techniques for Encrypting IP Address and Data Transfer over Wide Area Network through Three Levels

Ako Muhammad Abdullah[1], Miran Hikmat Mohammed[2] and Roza Hikmat Hama Aziz[3]

[1, 2] Faculty of Science & Science Education, Computer Science Department, Sulaimani University, Sulaimani, Iraq
[3] Faculty of Physical & Basic Education, Computer Science Department, Sulaimani University, Sulaimani, Iraq

[1]ako.abdullah@univsul.edu.iq, [2]miran.mohammed@univsul.edu.iq, [3]roza.hamaaziz@univsul.edu.iq

ABSTRACT

Internet is the primary computer miracles among computer users because of viruses separation in all communication devices, and some of these viruses will lead to creating some problems in computer hardware and software. Thus, hackers will have lots of opportunities to hack user's tools. This research is provided a new approach to securing clients IP address at the time they connected to the internet. This operation will be done by using new encryption techniques in three stages. Similarly, the same procedures of encryption will be established for data that will be transferred over the network between clients. Thus, intruders' and hackers may get obstacles to get the real data and IP address that are the central point for hacking.

Keywords: *IPv4, Networking Security, Networks Vulnerability, Computer Viruses, Encryption Message Digest v5, Hash Security, Data Transfer, Wide Area Network.*

1. INTRODUCTION

Nowadays, internet the world has been started to be the main phenomena to be discussed among programmers, hackers, and typical computer users. Thus, software companies begin to produce software that named anti-virus, which become the first solutions has been used to protect viruses and hackers attack clients [3].

In fact, most of these software did not do theirs require action to prevent viruses attacking, but it was the helper to activate the viruses to attack the targets that the anti-virus software are installed on it. For instance, Trojan, Malware, Worm viruses, and so on, that affect the PCs [1].

The main attack will be done based on IP address, this because the computer protocols are used to identify computers on the network in order to be able to communicate with other clients over the WAN network. From this way, hackers will first identify the IP address of the target in order to start attacking and hack all information on it. In addition, there are many researchers that worked how to protect IP address once they connect to the internet for transferring and receiving data over LAN and WAN area network. This idea can be applied by using some techniques for encryption users sensitive information. For example password encryption using MD5 techniques [2].

In our work, we will use three new security techniques in three levels to secure each client IP address that connected to the internet. These techniques are:

First Level: Changing the order of digit for the IP address that means swap the order of octet for the IP address.

Second Level: Converting each number of IP address in each octet to the ASCII code. This by identify each number with the characters.

Third Level: Converting these characters in the second tier to some symbolic characters.

2. BACKGROUND & LITERATURE REVIEW

2.1 Security Architecture

In order to provide a high trust safety in any system, it is required to understand the best using of security techniques the following are the primary structure for the security based on by some investigated developers:

2.1.1 Identity

The meaning of identity is the password of the system should comprise the authentication, authorization and accounting (AAA).

Authentication means the user is either outside or in the system. Whereas, authorizations mean the users are eligible to use part of the system, this can be determent by using username and password. Thus, users must have an account in the system [4].

2.1.2 Secure Connectivity

This technique needs to use some software that gives the users possibilities to access the particular network virtually. Thus, it can be done by using VPN. In addition, users must have an account or must be a member of the system in order to be capable of using the system [5].

2.1.3 Perimeter Security

Many organizations insist on using a model that are more trusty to make a secure access by the users. This action will happen because these days there are lots of internet hacking, viruses, and some other criminal network that let to effect the system [6][7].

2.1.4 Securing Monitoring

This architecture of security discusses the meaning of Intrusion Detection System (IDS) for gaining the best access to the network system by the users. However, it requires that the system users must be controlled under the administrator to investigate every action that can be done on the system [8].

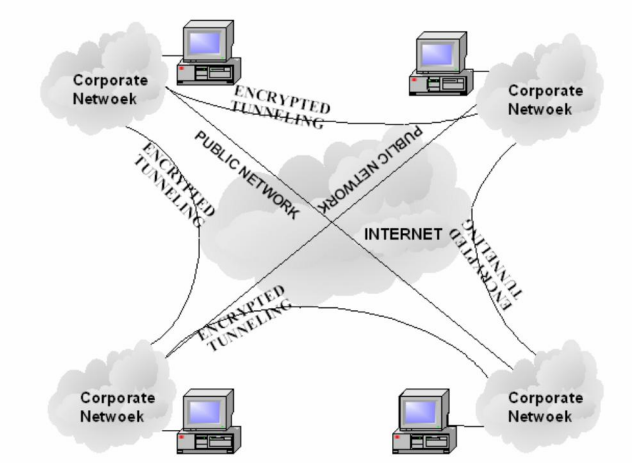

Fig. 1. Network Architecture Encryption

2.2 Threats

Networks (Private and Public) are more likely to be attacked by some people who are willing to access systems in unauthorized way through using some hacking tools or using programming techniques that compile to attack networks. It is important to study every point of security issues in network systems intensively to provide a security environment and protection for user's data when they are on the way for transferring between network users. Usually, it could be required to ask security professional people to test System Bridge and ports before the system become use widely [8].

2.2.1 IP Attacks

Hackers are those people either a part of the system or out of the system. First group are using attacking techniques to get into the system ineligible way. In this way, it can be denied by the system administrator because every network system users have a range of accessibility in a part of the system action, and grant and revoke can do this. Whereas, the second group is more dangers than the first group because there are working outside of the system, and they are not member of the organization. Action that can be done by this group is to hack the system completely and maybe for stealing sensitive data.
The key for hacking by a professional hacker is IP address, on private and public networks, because IP address is the identification for any client that enter to the LAN and WAN networks. Thus, scribblers detect the Internet Protocol address for specific users and use their on attacking techniques such as some software (IP Scanning Software) that are specific for hacking [9].

2.2.2 Viruses

In the computer world, there are thousands of software that IBM PC and Macintosh can invade those computer systems that can perform different actions between harmful and useful. For instance, deleting files or destroying hard disk is the type of dangers that can be cost by the software though software can cause some popping messages it cannot be dangers. Moreover, some software when they are installed, they caused to affect the computer system with viruses such as Trojan Horses and Worms. These viruses are some programs that are categorized as viruses because it works on deleting some important files that are operating system main files that run Windows.

Viruses should be treated quickly by some anti-viruses software because it is the way to open the door for hackers to attack users' computer. Thus, some software that comes with viruses will open some sensitive network ports that are the main breach to steal sensitive data from the targeted machine [10].

2.2.3 Network Vulnerability

The meaning of Vulnerability in computer science subjects especially network topics, is the way that gives the hackers full permission to unpermitted network access. Each computer in any network has some ports might be opened to the world. The opening port will happen during the internet connection, this phenomena means that the client who is their PC do not have any security to protect from viruses and attackers [11].

There are three types of attack

- Profile Attack: the attackers they want to attack people's profiles on social and private network. The primary goals of this attack are to change the

personal data for the victim of the system such as changing address, occupation, and some other personal data. Most of the attackers use this method to revenge the client.

- Files Attacking: attacking files is another way to get sensitive information that is either personal information or information that related to some sensitive organization such as police station data and police traffic data monitoring. Also, there are some other attackers' uses their purpose on hacking files to damage the system completely for example changing configuration of some windows files DLL files.
- Attacking Template: this kind of attack requires people who are professional in computer hacking programming and computer security problems. Those sniffer work on getting the absolute operating system versions and releases type in order to detect the correct bridge according to the Windows version. This kind of attack is much more widespread way between attackers that the use to intrude the target [12].

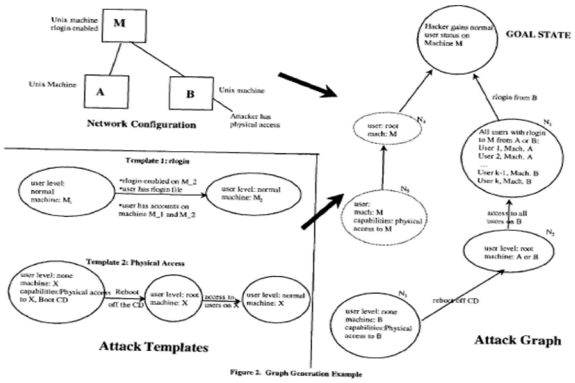

Fig. 2. Attacking Types

2.3 Data Encryption and Decryption

The term encryption can be defined a new technique in the computer worlds to hide sensitive user information such as using username and password. In the case of password, it requires the password must be hidden or coded to some other codes that cannot be understood by the people readily. For instance, a password that consists of numbers, characters, and special characters can be converted to some text that can be known by the computer subject. In addition, some encryption process goes through some levels of encoding data. On each level, the text will encrypt on it is on algorithm. There are many software and programming techniques that work on encrypting data [13]:

2.3.1 Cipher Text

The text can be a cipher by using some techniques of encryption algorithms; this method is worked on the form of data that required going through some process of encryption. There are two types of ciphering:

- Block Cipher

  This type of cipher text algorithm is the simplest type than the other kind which is a stream cipher. This feature of comparing the simplicity due to the working algorithm which divide the plain text into some block of text as it can be seen the following figure. This kind of divide will fit the cipher system in order to produce ciphered text [16].

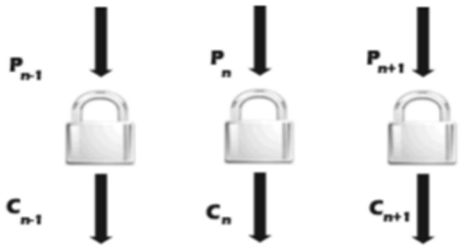

Fig. 3. Block Cipher

- Stream Cipher

  Stream cipher is another type of ciphering text which is relied on two different categories; a Key Stream Generator and a Mixing Function. The first one is based on generating auto encryption data from the original texts. The second one (Mixing Function), is used to generate some methods that can be used to produce some processes that will be used to cipher the texts in the stream way. Also, there are some ideas of this cipher type they think that this algorithm work in the same way as XOR functions. Thus, the meaning of using XOR is that if the text is generated streams of zeroes at the time of converting process to get ones at the end [18].

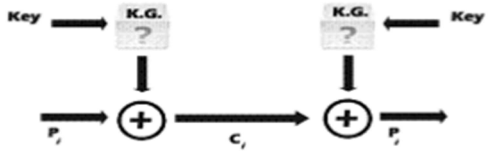

Fig. 4. Stream Cipher XOR

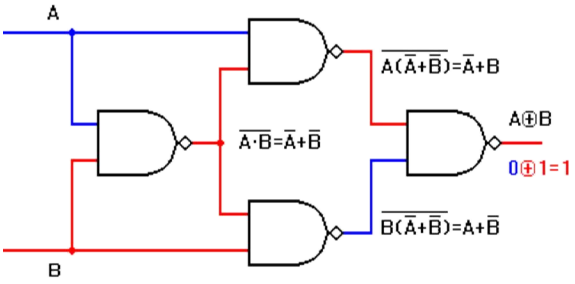

Fig. 5. Logical XOR

2.3.2 Message-Digest Algorithm (MD5)

MD5 is one of the security algorithms that use to encrypt and hide text data from unpermitted users on the network. Thus, it means MD5 is designed to work on hiding text only; the change will be done by each letter of the words. Moreover, this algorithm has been found by Ron Rivest in 1993, and MD5 stand for message digest version 5. It works on encrypting data using 512 bits words; this means that it can produce a security level for hiding IP address [21].

2.3.3 Symmetric Encryption

A symmetric encryption works on a data bit by bit in the network which is peer-to-peer or LAN network between two groups of the system. Moreover, this technique works on a part of the system, and it cannot be used in large area network. It needs to share the idea of encryption between two clients that agree on sharing an encryption which is worked on encrypting data messages before the destination. After that the message will decrypt to original text [14].

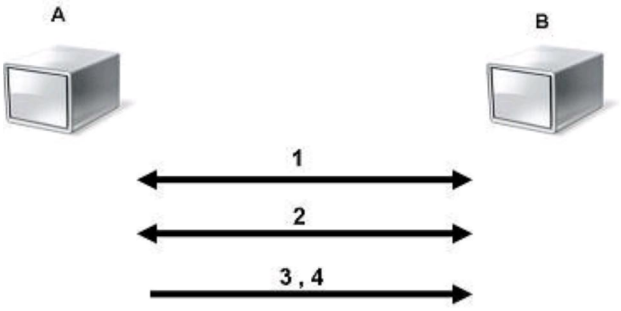

Fig. 6. Symmetric Encryption

2.3.4 Asymmetric Encryption

Asymmetric algorithm encryption based on two pieces one is called public, and another is called private. The first one named public because the network users can do the encryption. Whereas the second one named individual because there will be some hidden encryption technique will be used to encode the data. In addition, this technique requires lots of mathematical operation such as matrixes mathematical operation and statistical operation. Thus, this method is slower than the symmetric technique 1000 times [17].

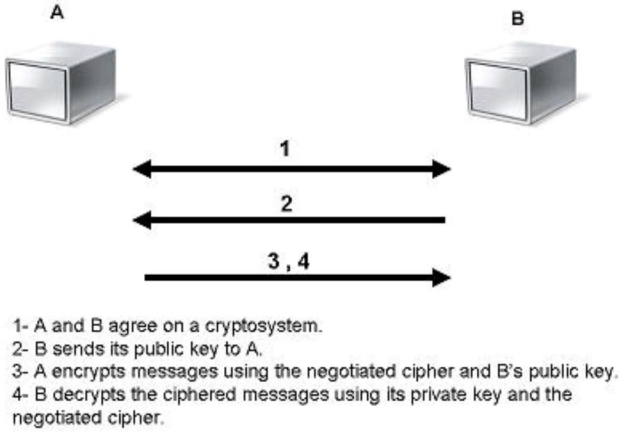

Fig. 7. Asymmetric Encryption

3. Design and Implementation

3.1 Login System Form

As the first stage in the system, users require entering their username and password. This is the first step in the system that is considered security roles for users' profile. Therefore, hackers will not get into the account easily because of the password. In addition, that information of the user will be stored in the database such as First Name, Last Name, Age, User Name and Password.

users

UserID	FirstName	LastName	Age	UserName	Password
1	Miran	Baban	30	MirBaban	100101 110100 111011 010010 110001
2	Ako	Ali	29	AkoAli	110101 110100 110011 110010 110111
3	Roza	Hikmat	29	RozaHikmat	110111 110110 110011 111010 110011

Fig. 8. Users Information

As it is apparent from figure, it can be noticed that the password field is shown as binary digit this means that the password for the system user has been encrypted by using a new proposed security algorithm.

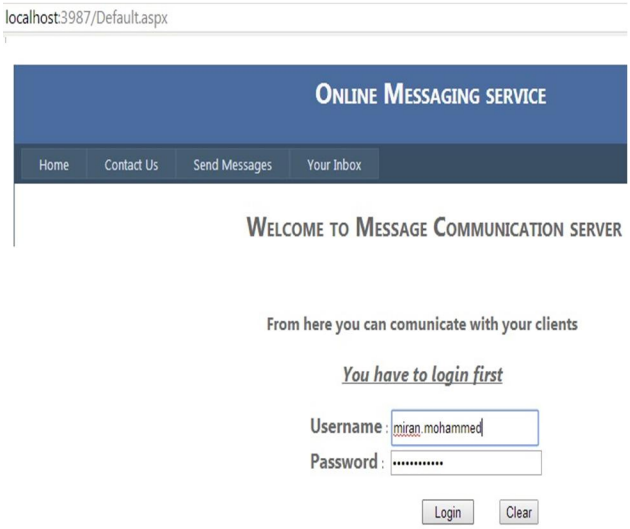

Fig. 9. User Login

3.2 Contact Information

In this page, users can use the following address as it can be seen in the following figure to give any issues that related to this system.

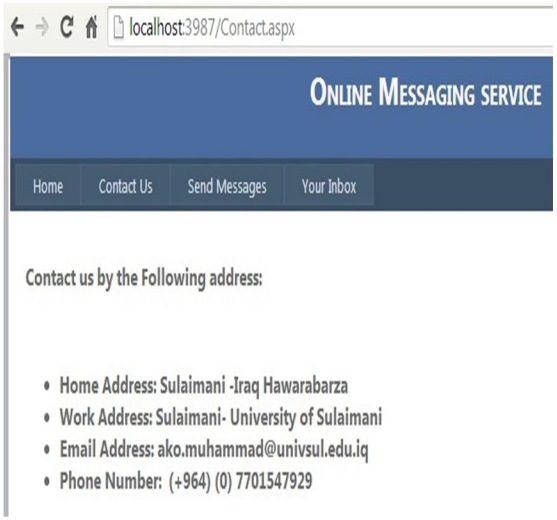

Fig. 10. Contact Information

3.3 Sending Messages

These page users use to send messages to other users that are member of this system. In order to do this process, it required that senders must fill the form of sending messages.

- User Name: In this section, sender must type the username of the receiver that means to send the message too.
- Message Subject: The title for the message should be written in this field.
- Message Details: It is the central part of the system which user sends the message details through using it. The data of the message will be stored in the database before it is received by the receiver. Moreover, the proposed security algorithm will be applied to the data message, and it will be encrypted as shown in Fig. 12.

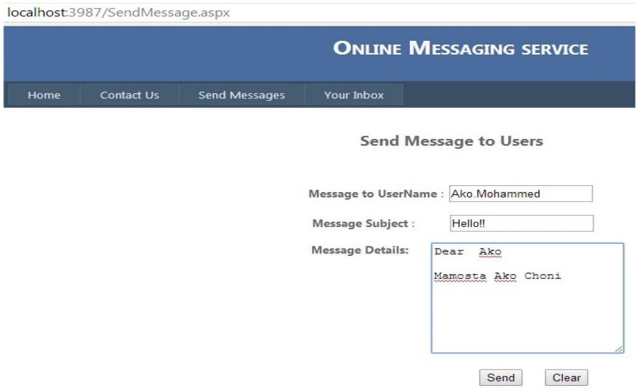

Fig. 11. Send Message to Users

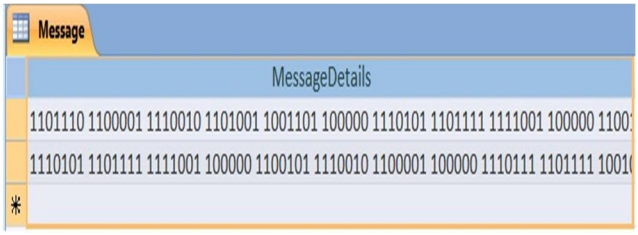

Fig. 12. Encrypted Messages

4. Results and Discussion LING

The goals of our new proposed system are to provide an environment for secure communication between system users. In addition to the level of security, we created a three-level of encrypting IP address for each user enter to the network.

4.1 Securing IP Address

IP address is the main system problem that hackers may attack any system through using it. Consequently, this is the main reason that led us to think about a new algorithm which comprises of three levels.

- Reversing the data (IP Address order) for instance 192.168.1.28 to 28.1.168.192
- Converting each number to ASCII Code and Binary number for example 28 =. 1C
- Then to binary= 11100.

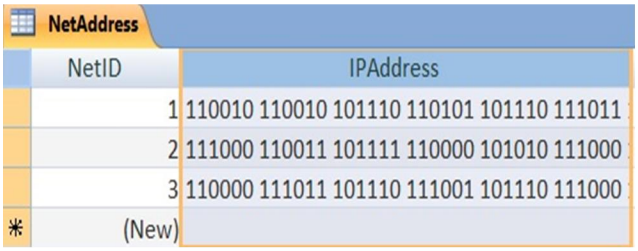

Fig.13. IP Encryption

4.2 Messages Encryption

Messages are the personal part of the system which users want to send to other personally and hidden from the hackers and the other people. In order to do this for the user, we came to account to use the same propose security algorithm that we applied to the IP address can be used for data messages as well. Thus, as well as IP address we encrypted messages over the network before it is received at its destination. As it can be seen the following figure.

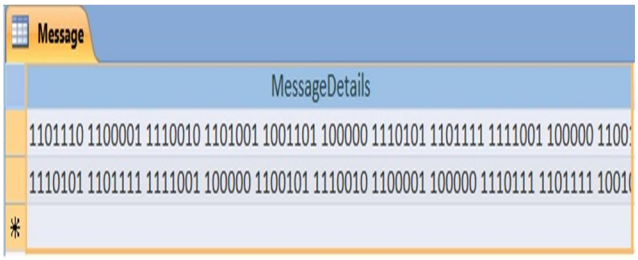

Fig. 14. Message Encryption

The stages for the encrypting data messages are:

- Reversing each text.
- Converting each opposite character to ASCII Code.
- Converting ASCII Code to the binary.

For instance:

- Text “Hi” reverse to iH.
- Converting I to 105 and H to 72.
- Converting 105 to 1101001 and 72 to 1001000.

4.3 Decryption Stage

This is the final stage of our proposed system which works on preserving the encrypted data to its originals shape on the site of the destination users.

For instance:

- Converting the binary number 11100 to 1C.
- Converting 1C to 28.

The receiver will see the messages in decrypted way as shown the following figure.

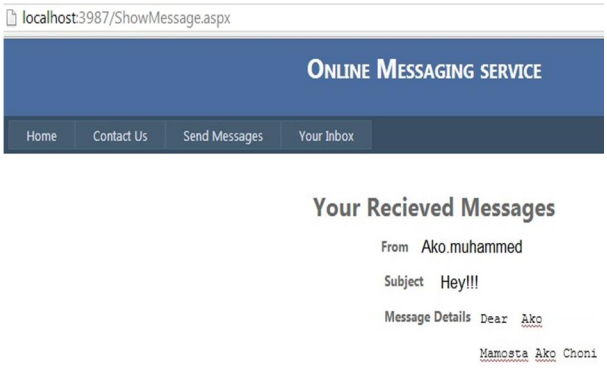

Fig. 15. Decryption Messages

The decryption of the messages will be done by reversing the action of the encryption process.

5. Conclusion

To sum up our proposed system, we conclude that every system that connected to the internet should provide at least a level of security for their users that are member of the system. Also, we have noticed in our work that system should secure the IP address for each user that connected to the proposed system, because hackers when they will tend to hack any system they try to get IP address from each user. Thus, it is a good idea that we proposed a new algorithm for securing IP address. In addition, we concluded that if we secure messages that are stored in the database in the main server which connected users to each other from intruders. Therefore, there are some obstacles face hackers to get the correct messages.

6. Future Work

We already planned to widen our research idea to comprise MAC address. As well as IP address we will apply the concept of this security algorithm on MAC address for each user connected the Wide Area Network.

7. Acknowledgement

We would like to give big thanks, full to the University of Sulaimani that has big roles for our research by providing some facilities. Also, everyone who has given a hand to our project we would like to give them a desired consideration place in our heart.

REFERENCES

[1] Joshi, Milind. J., and Bhaskar Vijayrao Patil. 'Computer Virus: Their Problems & Major At-Tacks In Real Life'. Journal of Advanced Computer Science & Technology 1.4 (2012): n. page. Web.
[2] Hassan, Amir, and Muniza Irshad. 'IP Based Virtual Private Network Implementation On Financial Institution And Banking System.' National Conference on Emerging Technologies (2004): 30-34. Print.
[3] Bontchev, Vesselin. 'Possible Macro Virus Attacks and How To Prevent Them'. Computers & Security 15.7 (1996): 595-626. Web.
[4] Pathan, Amir, and Muniza Irshad. 'IP Based Virtual Private Network Implementation On Financial Institution And Banking System'. National Conference on Emerging Technologies (2004): 30-34. Print.
[5] Walker, J. 'Security, Quality, Standards and Imagination'. ITNOW 48.1 (2006): 26-27.
[6] Song, Fei Fei, and Bin Jie Zhu. 'Design of Perimeter Security Monitor System'. AMM 513-517 (2014): 3593-3596.
[7] Al-Osaimi, Ali. 'Securing Health and Human Rights: Sandwell's Community Health Network'. Medicine, Conflict and Survival 24.sup1 (2008): S94-S103.
[8] Launius, Steven. 'Securing the Network Perimeter Of A Community Bank'. SANS Institute (2009): 1-41.
[9] Heberlein, Todd et al. 'A Network Security Monitor'. IEEE (1990): 296-304.
[10] Takamiya, Ward, and Jocelyn Kasamoto. 'An Introduction To Computer Viruses'. 2000.
[11] Amman, Paul, Duminda Wijesekera, and Saket Kaushik. 'Scalable, Graph-Based Network Vulnerability Analysis'. ACM New York, NY, USA (2002): 217 - 224.
[12] Phillips, Cynthia, and Laura Swiler. 'A Graph-Based System For Network-Vulnerability Analysis'. NSPW '98 Proceedings of the 1998 workshop on New security (1998): 71-79.
[13] Bhati, Sunita, Anita Bhati, and S. Sharma. 'A New Approach Towards Encryption Schemes: Byte – Rotation Encryption Algorithm'. Proceedings of the World Congress on Engineering and Computer Science-USA 2 (2012): 1-5.
[14] Al Tamimi, Abdel-Karim. 'Performance Analysis Of Data Encryption Algorithms'. (2013): 1-13.
[15] Ahmad, Shish et al. 'Comparative Study Between Stream Cipher And Block Cipher Using RC4 And Hill Cipher'. International Journal of Computer Applications 1.25 (2010): 15-21.
[16] Huang, JiaLin, and XueJia Lai. 'What Is The Effective Key Length For A Block Cipher: An Attack On Every Practical Block Cipher'. Science China Information Sciences 57.7 (2014): 1-11.
[17] Lei, Jingsheng. Network Computing And Information Security. Berlin: Springer, 2012.
[18] Paul, Goutam, and Subhamoy Maitra. RC4 Stream Cipher And Its Variants. Boca Raton: Taylor & Francis, 2012.
[19] Ah Kioon, Mary Cindy, Zhao Shun Wang, and Shubra Deb Das. 'Security Analysis Of MD5 Algorithm In Password Storage'. AMM 347-350 (2013): 2706-2711.
[20] Alam Hossain, Md. 'Cryptanalyzing Of Message Digest Algorithms MD4 And MD5'. International Journal on Cryptography and Information Security 2.1 (2012): 1-13.
[21] Prakash, Sankalp. 'An Efficient Implementation Of PKI Architecture Based Digital Signature Using RSA And Various Hash Functions (MD5 And SHA Variants)'. IOSR-JCE 15.6 (2013): 27-33.

AUTHOR PROFILES:

Ako Muhammad Abdullah is Deputy and Assist Lecturer of Computer Science Department in the Faculty of Physical & Basic Education at the Sulaimani University - Kurdistan Region – Iraq. He got BSc in Mathematics and Computer from Sulaimani University, 2007 and MSc in Computer Science from Glyndwr University, United Kingdom, 2012. His main areas of research interest are Network Performance, Multimedia and Web Design. In 2014, he published some papers. Ako M. Abdullah received his Cisco Career Certifications/ Cisco Certified Network Associate-CCNA1, CCNA2, CCNA3 and CCNA4 from United Kingdom in 2012.

Miran Hikmat Mohammed Baban, received BSc degree in computer science from University of Sulaimaniyah in 2007, at Iraq-KRG, and MSc degree also in Advance computer science from the University of Hertfordshire in England-London at 2012.

Roza Hikmat Hama Aziz was born in Sulaimani, Kurdistan Region-Iraq. She received the BSc from Sulaimani University, Kurdistan Region, Iraq, in 2007 and MSc in Computer Science from Glyndwr University, United Kingdom, in 2012. Currently, she is working as assist lecturer of Computer Science Department, Faculty of Physical & Basic Education, University of Sulaimani, Kurdistan Region, Iraq. Her main areas of research interest are Database, Mobile Application, and Web Design. In 2014, she published some research papers. Roza H. Hama Aziz received her Cisco Career Certifications/ Cisco Certified Network Associate-CCNA1, CCNA2, CCNA3 and CCNA4 from United Kingdom in 2012.