International Journal of Computer Science and Engineering Open Access
Research Paper Volume-2, Issue-2 E-ISSN: 2347-2693

Network Security and Methods of Encoding and Decoding

Sharmeen kaur[1*], Raveena Singh[2] and Shivya Gagneja[3]

[1*] Computer Science & Engineering, Punjab Technical University, India, bhatt.sherry53@gmail.com
[2] Computer Science & Engineering, Punjab Technical University, India, raveenasingh07@gmail.com
[3] Computer Science & Engineering, Punjab Technical University, India, shivya12@gmail.com

www.ijcaonline.org

Received: 28 Jan 2014 Revised: 10 Feb 2014 Accepted: 20 Feb 2014 Published: 28 Feb 2014

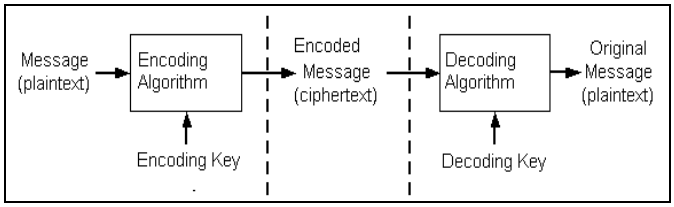
***Abstract*—** Network Security is the most vital component in data protection because it is responsible for protecting all information passed through computers containing network. Network Security refers to all hardware and software functions, characteristics, features, accountability, measures, access control, and administrative and management policy required to provide an acceptable level of protection for Hardware and Software, and information in a network. Here we are focusing on the technique of Quantum Cryptography which uses the law of quantum physics for unconditionally secure data communications. This is an improvement because the cryptography currently in use, known as conventional cryptography, is dependent entirely on the difficulty level of a mathematical equation. To write this paper we have studied about Network Security and methods of encoding and decoding in detail. Hereby we are presenting our work on the enhancement of cryptography using various encoding and decoding approaches. The proposed algorithm has a better speed compared with other encoding algorithm. Nevertheless, the proposed algorithm improves encoding security by inserting the symmetric layer. The proposed algorithm will be useful to the applications which require the same procedure of encoding and decoding. This paper makes a comparison between classical cryptography and quantum cryptography and outlines the increased security level provided by quantum cryptography.

***Keywords*—** Network security, Encoding, Decoding, Cryptography, Quantum Cryptography

I. INTRODUCTION

Transferring messages securely has been a major aspect for the world of computers. Network Security is a method to protect network and data transfer over wireless network. It protects its availability, privacy, authentication, non-repudiation and integrity. Network security is the main aspect of protected data transmission over unreliable network. Network security is a challenging issue of data communications today that touches many areas including protected communication channel, strong data encoding method and in order to maintain the database trusted third party is required. Many businesses secure themselves from the internet attacks by means of firewalls and encoding method. We use different methods for encoding and decoding such as eavesdropping, viruses, worms, Trojans, phishing, IP snopping attacks, denial services. Therefore, it is necessary to apply effective encoding/decoding methods to enhance network security.

The main feature of the encoding/decoding program implementation is the generation of the encoding key. Cryptography is the method that allow information to be sent in a protected form in such a way that the only receiver able to retrieve this information. Presently continuous researches on the new cryptographic algorithms are going on. However, it is a very difficult to find out the specific algorithm, because we already know that they must consider many factors like: security, the features of algorithm, the time complexity and space complexity.



Security Services:
If we are taking about security of information then following services come in mind.

- Confidentiality (privacy)
- Authentication (who created or sent the data)
- Integrity (has not been altered)
- Non-repudiation (the order is final)
- Access control (prevent misuse of resources)
- Availability (permanence, non-erasure)

II. INTERNET ARCHITECTURE AND VULNERABLE SECURITY ASPECTS

Fear of security breaches on the Internet is causing organizations to use protected private networks or internet. The Internet Engineering Task Force (IETF) has introduced security mechanisms at various layers of the Internet

Corresponding Author: *Sharmeen Kaur*

Protocol Suite. These security mechanisms allow for the logical protection of data units that are transferred across the network. The security architecture of the internet protocol, known as IP Security, is a standardization of internet security. IP security, IPSec, covers the new generation of IP (IPv6) as well as the current version (IPv4). Although new methods, such as IPSec, have been developed to overcome internet's best-known deficiencies, they seem to be insufficient .IPSec is point-to-point protocol, one side encrypts, the other decrypts and both sides share key or keys. IPSec can be used in two modes, namely transport mode and tunnel modes. IPSec contains a gateway and a tunnel in order to secure communications. The current version and new version of the Internet Protocol are analyzed to determine the security implications. Although security may exist within the protocol, certain attacks cannot be guarded against. These attacks are analyzed to determine other security mechanisms that may be necessary.

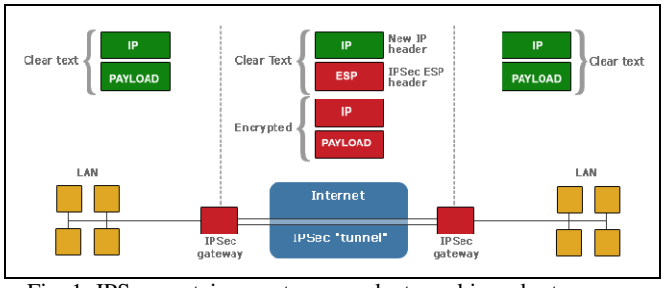


Fig. 1: IPSec contains a gateway and a tunnel in order to secure communications.

III. ATTACK METHODS AND SECURITY TECHNOLOGY

Common attack methods and the security technology will be briefly discussed. Not all of the Methods in the table above are discussed. The current technology for dealing with attacks is understood in order to comprehend the current research developments in security hardware and software.

Computer Security attributes	Attack Methods	Technology for Internet Security
Confidentiality	Eavesdropping, IIacking, Phishing, DoS and IP Spoofing	IDS, Firewall, Cryptographic Systems, IPSec and SSL
Integrity	Viruses, Worms, Trojans, Eavesdropping, DoS and IP Spoofing.	IDS, Firewall, Anti-Malware Software, IPSec and SSL.
Privacy	Email bombing, Spamming, Hacking, DoS and Cookies	IDS, Firewall, Anti-Malware Software, IPSec and SSL.
Availability	DoS, Email bombing, Spamming and Systems Boot Record Infectors	IDS, Anti-Malware Software and Firewall.

Intrusion Detection Systems:

An Intrusion Detection System (IDS) is an additional protection measure that helps ward off computer intrusions. IDS systems can be software and hardware devices used to detect an attack. IDS products are used to monitor connection in determining whether attacks are been launched. Some IDS systems just monitor and alert of an attack, whereas others try to block the attack.

IV. SECURITY ISSUES OF IP PROTOCOL IPV6

From a security point of view, IPv6 is a considerable advancement over the IPv4 internet protocol. Despite the IPv6's great security mechanisms, it still continues to be vulnerable to threats. Some areas of the IPv6 protocol still pose a potential security issue. The new internet protocol does not protect against misconfigured servers, poorly designed applications or poorly protected sites. The possible security problems emerge due to the following:

- Header manipulation issues
- Flooding issues
- Mobility issues

Header manipulation issues arise due to the IPSec's embedded functionality. Extension headers deter some common sources of attacks because of header manipulation. The problem is that extension headers need to be processed by all stacks, and this can lead to a long chain of Extension headers. The large number of extension headers can overwhelm a certain node and is a form of attack if it is deliberate. Spoofing continues to be a security threat on IPv6 protocol. A type of attack called port scanning occurs when a whole section of a network is scanned to find potential targets with open services. The address space of the IPv6 protocol is large but the protocol is still not invulnerable to this type of attack. Mobility is a new feature that is incorporated into the internet protocol IPv6. The feature requires special security measures. Network administrators need to be aware of these security needs when using IPv6's mobility feature.

V. ADVANCED CRYPTOGRAPHY FOR BETTER NETWORK SECURITY

In Here we are using symmetric encoding approach. We have already know that symmetric encoding approach is divide in two type one is block cipher symmetric cryptography method and another is stream cipher symmetric cryptography but here we are choosing block cipher type because its efficiency and security. In the proposed method we have a common key between sander and receiver, which is known as private key. Basically private key concept is the symmetric key concepts where plain text is converting into encoded text known as cipher text using private key where cipher text decrypted by same private key into plane text. The encoding key is trivially related to the decoding key, in that they may be identical or

there is a simple transform to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain private information.

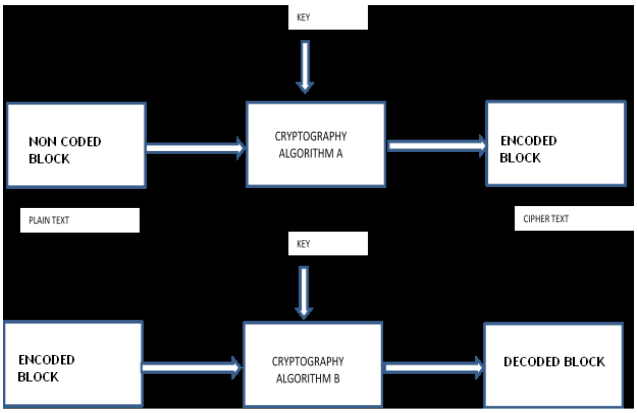


Fig. 2. Basic Concept for Symmetric Cryptography

Reasons for Use of Symmetric Approach for Encoding and Decoding

- The encoding process is simple.
- Each trading partner can use the same encoding algorithm no need to develop and exchange secret algorithms.
- Security is dependent on the length of the key.
- High rates of data throughput.
- Keys for symmetric-key ciphers are relatively short.
- Symmetric-key ciphers can be used as primitives to construct various cryptographic mechanisms.
- Symmetric-key ciphers can be composed to produce stronger ciphers
- Symmetric-key encoding is perceived to have an extensive history.

Proposed Key Generation Steps:

- Select or create any private key of Size 256 X 2 bits or 64 characters.
- Size of selected key will be varying from 128 bits to 512 bits or 16 to 64 characters.
- We can choose any character from 0 to 255 ASCII code.
- Use of 64 * 8 key that means 512 bits in length.
- Divide 64 bytes into 4 blocks of 16 bytes likes Key_Block1, Key_Block2, Key_Block3, and Key_Block4.
- Apply XOR operation between Block1 and Block3. Results will store in new Key_Block13.
- Apply XOR operation between Block2 and Block13. Results will store in new Key_Block213.
- Apply XOR operation between Key_Block213 and Key_Block4. Results will store in new Key_Block4213.
- Repeat Step 7, 8, 9 till (random number / 4).
- Exit

VI. STEPS OF PROPOSED ALGORITHM

- Initially select plane text of 16 bytes (or we can vary from 16 to 64 depend on requirement).
- Initially insert key of size 16 bytes (depend on plane text value)
- Apply XOR operation between key (Key_Block4213) and plain text block (Text_Block). Result will store in Cipher Block1.
- Apply right circular shift with 3 values. Result will store in new Cipher_Block2.
- Apply XOR operation between Cipher_Block2 and Key_Block2. Result will store in new Cipher_Block3.
- Apply XOR operation between Cipher_Block3 and Key_Block4. Result will store in Cipher_Block4.
- Cipher_Block4 is the input of the next round as a plane text block.
- Repeat step 1 to 7 till (Encoding Number / 4).
- Exit.

VII. RESULTS AND COMPARISONS

We are using two parameters for execution time one is encoding value and second is decoding time which is shown in table

1 and table 2 Here I am doing compare execution time of encoding plaintext on different existing cryptographic algorithms with my proposed cryptography algorithm. In each cycle, same plaintexts are respectively encoded by “A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm”, “Effect of Security Increment to Symmetric Data Encoding through AES Methodology” and “Proposed Algorithm (PA)” by copying them. Finally, the outputs of the evaluation system execution time, and measured in numeric form. Actually, for an encoding algorithm, the execution time of encoding not only depends on the algorithm’s complexity, but also the key and the plaintext have certain impact. Result Comparison in Tabular Form: - In this I am going to represent our result in the form of table. After comparison the results that were obtained can be well represented in form of tables. Here, The Proposed Algorithm (with 265bit block size in this thesis) and “A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm” algorithm (with 128-bit block size) and “Effect of Security

Increment to Symmetric Data Encoding through AES Methodology" algorithm (with 128-bit block size) have been implemented on a number of different data files like text, pdf and image varying types of content and sizes of a wide range. But here we are only showing result of text file.

Encoding and Decoding time of Various Text files comparisons shown in table 1 and table 2 respectively.

PLAIN TEXT SIZE	DJSA ALGORITHM	ENCODING THROUGH AES	PROPOSED ALORITHM
1.63 mb	0:1:37	0:1:33	0:01:24
561 kb.txt	0:00:36	0:00:35	0:00:27
185 kb.txt	0:00:16	0:00:14	0:00:07
45 kb.txt	0:00:12	0:00:10	0:00:01
15 kb.txt	0:00:09	0:00:07	0:00:01

Table 1: - Encoding time comparisons of text files.

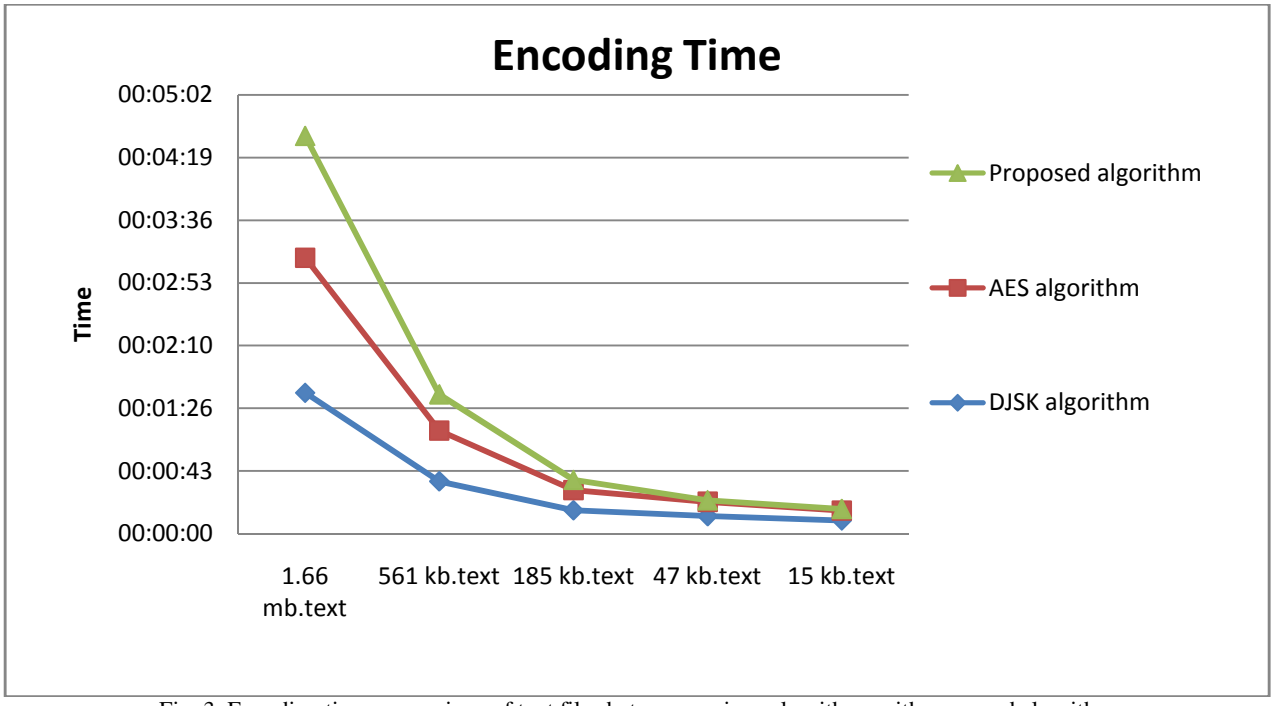


Fig. 3. Encoding time comparison of text files between various algorithms with proposed algorithm

PLAIN TEXT SIZE	DJSA ALGORITHM	ENCODING THROUGH AES	PROPOSED ALORITHM
1.63 mb	0:1:37	0:1:33	0:01:24
561 kb.txt	0:00:36	0:00:35	0:00:27
185 kb.txt	0:00:16	0:00:14	0:00:07
45 kb.txt	0:00:12	0:00:10	0:00:01
15 kb.txt	0:00:09	0:00:07	0:00:01

Table 1: - Decoding time comparisons of text files.

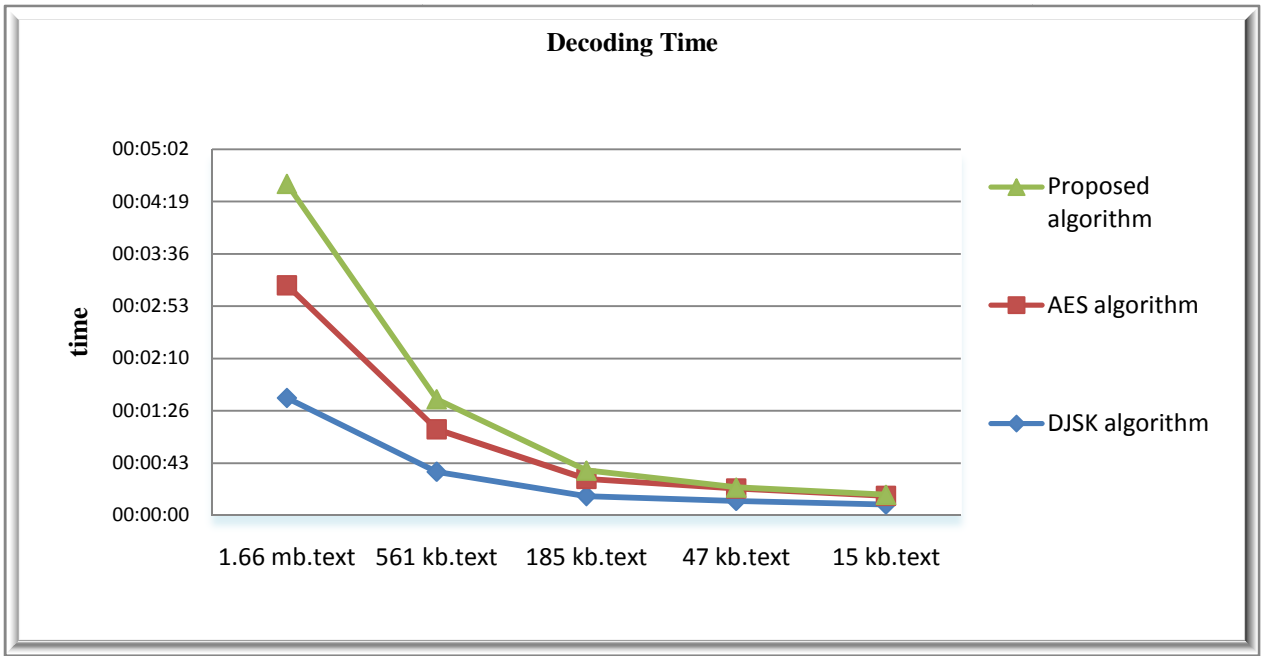


Fig. 4. Decoding time comparison of text files between various algorithms with proposed algorithm

VIII. CONCLUSION

From the result it is clear that "proposed technique" yield better result as compared to "DJSA symmetric key algorithm". Thus this algorithm can be used for security reasons. This method will take less time if the file size is large. The important thing of our proposed method is that it is almost impossible to break the encoding algorithm without knowing the exact key value. We state that this encoding method can be applied for data encoding and decoding in any type of public application for sending confidential data.

ACKNOWLEDGMENT

I would like to express the deepest appreciation to my committee chair Professor Rajwinder Singh, who has shown the attitude and the substance of a genius. He continually and persuasively conveyed a spirit of adventure in regard to teaching. Without his supervision and constant help this dissertation would not have been possible.

I would also like to thank the proof readers, honorable teachers, fellow students, supportive friends and family and my supervisor Mr. Himanshu Kakkar.

REFERENCES

[1] Dripto Chatterjee, Joyshree Nath, Suvadeep Dasgupta, Asoke Nath "A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm" published in 2011 International Conference on Communication Systems and Network Technologies, **978-0-7695-4437-3**/11 $26.00 © **2011** IEEE.

[2] Simmonds, A; Sandilands, P; van Ekert, L (**2004**) Ontology for Network Security Attacks". Lecture Notes in Computer Science. Lecture Notes in Computer Science **3285**, pp.**317–323**.

[3] A Role-Based Trusted Network Provides Pervasive Security and Compliance - interview with Jayshree Ullal, senior VP of Cisco.

[4] Dave Dietrich, Network monitoring/Intrusion Detection Systems (IDS), University of Washington.

[5] Sanchez-Avila, C. Sanchez-Reillol, R, ―The Rijndael block cipher (AES proposal): A comparison with DES‖, **35**th International Conference on Security Technology **2001**, IEEE.

[6] Symmetric key cryptography using random key generator,A.Nath, S.Ghosh, M.A.Mallik, Proceedings of International conference on SAM-**2010** held at Las Vegas(USA) **12-15** July, **2010**, Vol-**2**,P-**239-244**.

[7] By Klaus Felten "An Algorithm for Symmetric Cryptography with a wide range of scalability" published by **2**nd International Workshop on Embedded Systems, Internet Programming and Industrial IT.

