Available online at http://www.journalijdr.com

IJDR

International Journal of
DEVELOPMENT RESEARCH

ISSN: 2230-9926

International Journal of Development Research
Vol. 06, Issue, 12, pp.10738-10743, December, 2016

Full Length Review Article

ENHANCING SECURITY BY ALTERING ENCRYPTION KEYS FOR SYMMETRIC ALGORITHM

[1,*]Densy John V. and [2]Dr. Agnise KalaRani, X.

[1]Karpagam Academy of Higher Education, Coimbatore, India
[2]Department of Higher Education, Karpagam Academy of Higher Education, Coimbatore, India

ARTICLE INFO

Article History:
Received 17th September, 2016
Received in revised form
22nd October, 2016
Accepted 29th November, 2016
Published online 30th December, 2016

Key Words:
Network security, Encryption, AES, Hash functions, Cryptool, Frequency analysis, XOR encryption algorithm, Key-length.

ABSTRACT

Information security is crucial for all organizations. People are using information technology for storing data in the internet. Now-a-days Cloud Storage and Big Data are common among all kinds of people. Moreover mobile technology is becoming more popular. Therefore new technologies are derived from the existing encryption algorithms in order to resists the attacks from intruders. In this study we are experimenting a new technique of encrypting with two different algorithms and two different encryption keys so that it can be useful for resisting the man-in-the-middle attacks for the information over the internet. The results proved that eaves- dropper cannot determine the key-length to decrypt back to original message. Here we are using AES and XOR for encrypting and key generation is done using hash functions.

Copyright©2016, Densy John and Dr. Agnise KalaRani. *This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.*

INTRODUCTION

Securing data is an important factor in all aspects of our being. Now-a-days information is send through different media which needs to be safe. Information technology is very much concerned about the security aspect of the organization. Latest technologies like mobile computing is becoming an essential part of day- to -day communication. The main advantage of mobile communication is that it is easy to use and handy. They are available with its advanced Operating System like Android or iOS. The architecture of the mobile wireless network is ad-hoc networks which is termed as MANET (Mobile Ad-hoc Network) and hence prone to security issues. The mobile networking is ad-hoc means that it is infrastructure less. As more and more nodes are added to the network it reconfigures itself and detects the nodes and establishes a safe peer to peer communication. The drawback of MANET is less security, has more power consumption, availability and speed. Thus the wireless networks are more prone to security issues than the wired networks (Pramendra Kumar and Vijay Kumar Sharma, 2014; Madhurya *et al.,* 2014; Yang *et al.,* 2004). Some of the security parameters for wireless or wired network are availability, Integrity, Access control confidentiality. There are several security models developed in order to reduce the flaws in the networks.

****Corresponding author: Densy John V.***
Karpagam Academy of Higher Education, Coimbatore, India.

Using the encryption algorithm, Authentication tools, hash function are some of them. The way they implemented it will make them more secure. The wireless LAN (WLAN) is implemented with the protocol IEEE802.11. WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) are some of the other protocols used in wireless networks. WEP is accepted by IEEE that it provides less security while WPA has a set of 802.11i features so that it is more secure. There is a secure protocol RSN (Robust Security Networks) which implements dynamic negotiation of implementing algorithms. All these algorithms use encryption but several security weaknesses are identified by the cryptanalysts (Halil Ebrahim Bulbul *et al.,* Borisov. N *et al*., Fluhrer, S. *et al*., A. Arbaugh. W *et al.,* Stubblefield A. *et al*).

Since the scope of wireless networks are more we need a more secure encryption algorithm to prevent vulnerabilities and to give more privacy in data transmission for each nodes. Cryptography or encryption is the process in which the messages send through the internet are transmitted in a coded form. Though the security parameters are included in the implementation of wireless networks there are vulnerabilities in the existing system. The implementation of security is easily broken with a man-in-the–middle attack, spoofing MAC address, Access Points to intercept the wireless traffic, crashing the Access Points by Denial of Service (DoS) and cracking WEP- an existing security algorithm are some of them.

Research Objectives

The objective of this study is to enhance the security of the existing algorithm. The researcher have chosen the symmetric algorithm AES. Encryption is done two times with two different keys so that the man-in-the-middle cannot guess the key or the key length. This research aims at the security of mobile networks and thus it protects the individual mobile devices. Since the communication using this networks are more convenient and fast many people are using this technology. Therefore the target audience under the study is all users who are using mobile devices. It includes professionals in all area like business, education, industry, civil and government. It is clear that the above study consists of people in all areas so that this is beneficial to the community. Everyone can send the information safe especially the sensitive information like the financial transactions and personal information. Thus the new system will be beneficial all people who are using mobile devices. The study aims the solution to security issues in networking which can be implemented to provide security enhancements to the existing system. The result of the study will be useful for the technical world to improve the security of their system. The scope of the study includes all network users. Since the mobile devices like smart phones are used by all category people irrespective of their age. The study includes the enhancement of the algorithm and does not include the development stage. The perception of the study limits to the enhancement methods in the existing algorithm and not the implementation phase. The readers can view the limitations from the results obtained.

MATERIALS AND METHODS

The wireless technology is used in many organizations like corporate, manufacturing, warehousing, retail, education, finance and healthcare. Most of the organizations use the wired and wireless combination network in the company. The wireless devices are connected to network through wireless access points. Authors Pramendra Kumar, Vijay Kumar Sharma mentions that the wireless networks use a peer-to-peer network system. The nodes themselves will be forwarding the messages and thus it will reach the destination. As more nodes are added to the network the risks associated with the network increases. The media used in wireless network is air. Anyone with right device can access the information transmitted by a node from the medium. Therefore, mobile network is called as an Ad hoc network (Pramendra Kumar and Vijay Kumar Sharma, 2014). According to H. T. Dinh, one of the security issues for wireless network is low bandwidth. The network follow Markov's decision table to distribute bandwidth among the users with respect to their needs. Each node in the network will communicate each other and find the shortest hopping distance. The security issues arise when they share information to hop between the nodes. According to the authors, an account key, friend key and content key are used along with the information send through the network. The devices access the network using different access technologies (Hoang *et al.,* 2013). Traffic analysis is another kind of network vulnerability. The intruder can know about the activities, physical location, and communication protocol of the victim. In eavesdropping the attacker secretly listens to conversation of others. In passive eavesdropping attacker reads the messages passed between the persons while in active eavesdropping the attacker sends his own messages in between their conversation. High jacking and Replay attack are two other attack against the authorization of the owner. Jamming is DoS attack on network availability (Umesh Kumar *et al.,* 2014). The MAC (Media Access Control) address of a node can be changed which is not traceable and the network considers it as a true node. For this network administrator need to check MAC address in NIC. A MAC and IP combination can resolve the problem. An encryption of wireless communication between the Access Points and the nodes can also resolve the problem. All such security methods may affect the speed, throughput of the network (Mohd Izhar and Singh, 2014). Some other protocols like SEAD (Secure and Efficient Ad hoc Distance Vector), SMT (Secure Message Transmission) use MAC (Message Authentication code) or Hash function for authentication. A newer technology is ECC (Elliptic Curve Cryptography) which makes fast and efficient algorithm even though the key length is small (Ram Shringar Raw, 2013; Menezes *et al.,* 2004). To solve security issues in MANETs, IDS (Intrusion Detection System) or Encryption algorithm can be used IDS can be stored in the nodes of original networks and false nodes can be detected. Cryptography uses symmetric or asymmetric keys. In symmetric key the distribution of the key to all nodes will destroy the security of the network. Asymmetric cryptography we need a public and a private key, where the public key of the other node is used to decrypt the messages received by the node. Hence the public key for all nodes is to be stored in every node so that messages from any valid nodes can be decrypted whenever they receive a message (Deepti Ranaut and Madal Lal, 2014). The encryption algorithms used are DES (Data Encryption Standard) which uses 56-bit secret key. DES can be defeated easily by Brute Force attack. AES (Advanced Encryption Standard) which uses 128 –bit, 192- bit or 256-bit length key for encryption. The key distribution problem exists in both algorithms. There are commonly used public key encryption algorithms. RSA (Rivest, Shamir, Adleman) algorithm is commonly used in e-commerce protocols. Its security depends on the difficulty of decomposing large numbers. Diffie-Hellman (DH) algorithm uses discrete logarithmic function which is difficult to crack but captured by man-in-the-middle attack. DSA (Data Signature Algorithm) is also based on discrete logarithms. Hashing functions uses MD-5 message digest algorithm which uses a 128-bit hash value (Deepti Ranaut and Madal Lal, 2014; Stallings, 2011). The above algorithms provide more security but have its own disadvantages. As the mobile network is expanding the need for a better security is inevitable. This research is focused on providing a stronger option for a better security so that the information passed through the network will be safer in the coming days.

Research Methodology

Enhancing the algorithm can be done using many methods. In this research we are finding out the 'best' available networking security encryption and compare it with the updates to the algorithm. From the studies done in the past, it is obvious that AES algorithm is stronger than the DES and other symmetric algorithm. In this we use XOR and AES to encrypt the same message twice so that the security can be doubled. Key-length of AES is 16 bytes (128-bits) and represented as Hexa-decimals. The study uses AES algorithm which is also called Rijndael developed by two cryptographers. It is very powerful algorithm which is used in many encryption algorithms and wireless protocols. There are two phases for the encryption. In the first phase, encryption is done using the AES and XOR

using the same key. In the second phase after the encryption with AES a hash function is used to encrypt with a second key.

Frequency analysis: Finds the frequency of the appearance of a letter or group of letters. Corresponding graph representing the frequency of each of the characters will appear. If the graph contains the representation of a set of characters, which can be used as a reference point, the distance between the character set and frequency of alphabets can be considered as the key length.

Autocorrelation: it is the index of similarity between different sections of the document. It helps to find the cycle length for the automatic analysis of the encryption by Exclusive –OR used in this study.

RESULTS AND DISCUSSION

In this study we use two methods to encrypt data. In the first method we same key for both encryption whereas in the second method we use two different secret keys to encrypt the same message. Thus we prove that by using the second method we confuse the intruder or eavesdropper not to find the original message by guessing the key or even the key-length. Cryptanalysis of encrypted messages are done with the help of CRYPTOOL.

Comparing the encryption keys used in encrypting the message

The research analyses the output obtained by encrypting the text file using a key generated by the hash function MD5. In this procedure we analyze after encrypting first using the XOR and then using AES and try to find the decrypting key.

PHASE1

Step1: Key generation is done using the cryptographic tool for a selected text.

Step 2: Encrypt using the key generated. Here we are using the same key for XOR and AES encryption. 5F 4D CC 3B 5A A7 65 D6 1D 83 27 DE B8 82 CF 99

Step 3: AES encryption using the same key 5F 4D CC 3B 5A A7 65 D6 1D 83 27 DE B8 82 CF 99

Step4: Cryptanalysis. Autocorrelation and frequency analysis are done to analyze the changes in the encrypted message. The derived key length is found which shows that deriving the original message is not possible by cryptanalysis.

The derived key length is 7. We get a different key length than the original even though we are using the same key with different encryption algorithm.

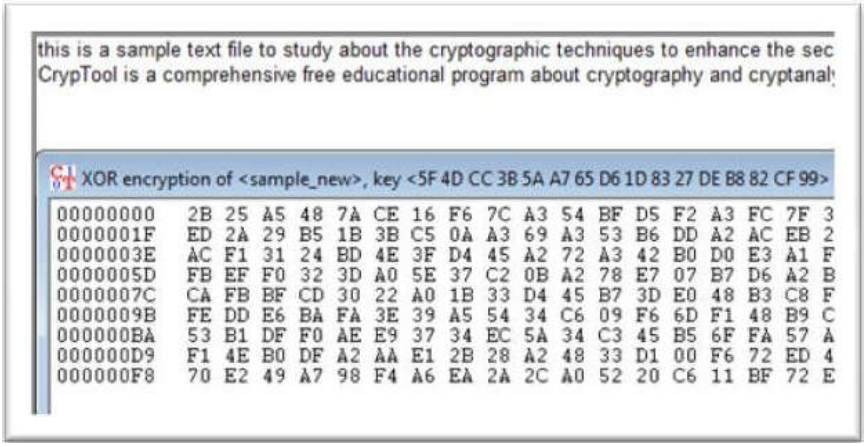


Figure 1. Encrypted message after XOR analysis

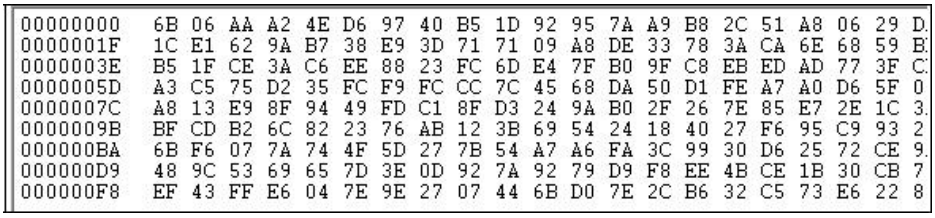


Figure 2. Result: Encrypted message

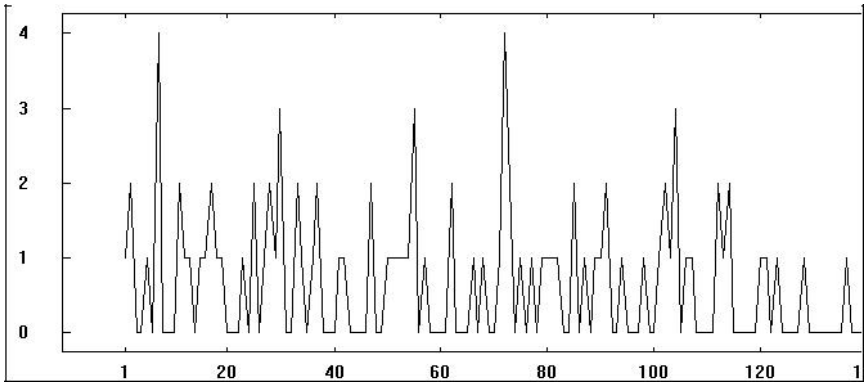


Figure 3. Analysis: Autocorrelation of AES encryption

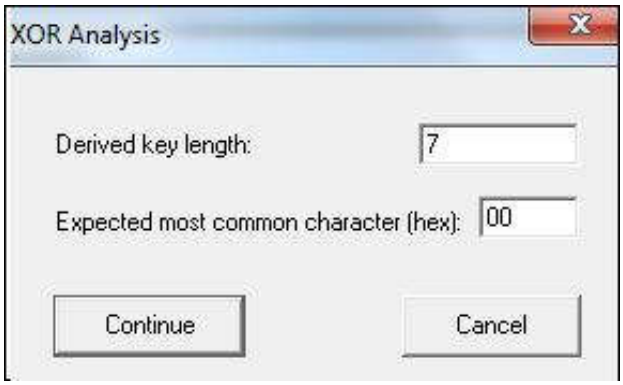


Figure 4. Fig Analysis: Finding the key length

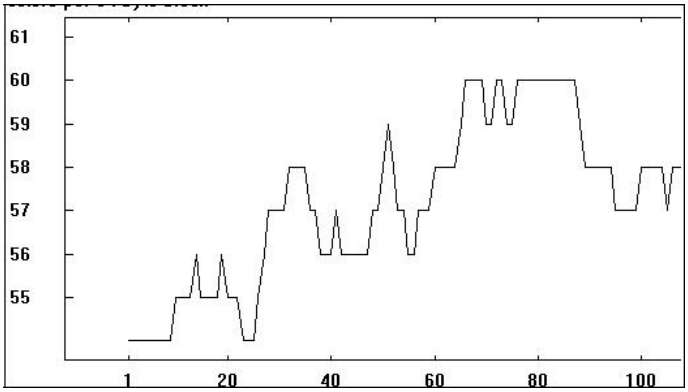


Figure 5. Analysis: Floating frequency

```
00000000   2B 25 A5 48 7A CE 16 F6 7C A3 54 BF D5 F2 A3 FC 7F 39 A
0000001F   ED 2A 29 B5 1B 3B C5 0A A3 69 A3 53 B6 DD A2 AC EB 26 3
0000003E   AC F1 31 24 BD 4E 3F D4 45 A2 72 A3 42 B0 D0 E3 A1 FA 3
0000005D   FB EF F0 32 3D A0 5E 37 C2 0B A2 78 E7 07 B7 D6 A2 BB F
0000007C   CA FB BF CD 30 22 A0 1B 33 D4 45 B7 3D E0 48 B3 C8 F0 A
0000009B   FE DD E6 BA FA 3E 39 A5 54 34 C6 09 F6 6D F1 48 B9 CA E
000000BA   53 B1 DF F0 AE E9 37 34 EC 5A 34 C3 45 B5 6F FA 57 AA D
000000D9   F1 4E B0 DF A2 AA E1 2B 28 A2 48 33 D1 00 F6 72 ED 4B B
000000F8   70 E2 49 A7 98 F4 A6 EA 2A 2C A0 52 20 C6 11 BF 72 ED 5
```

Figure 6. encrypted message after XOR (step2)

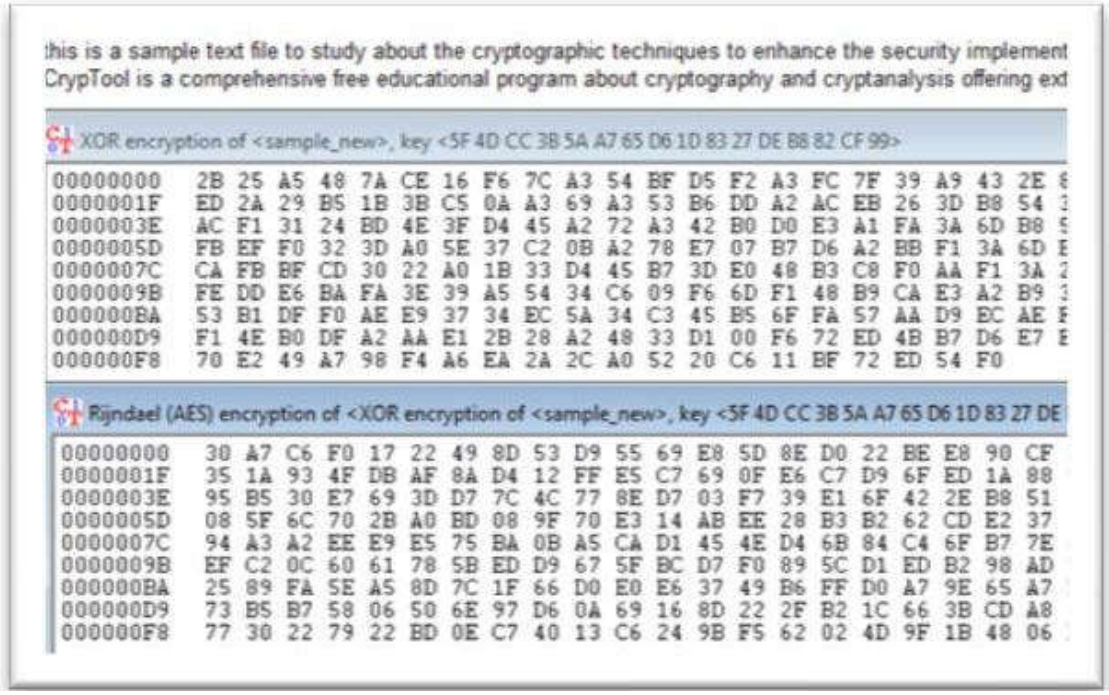


Figure 7. application of AES is done with new password

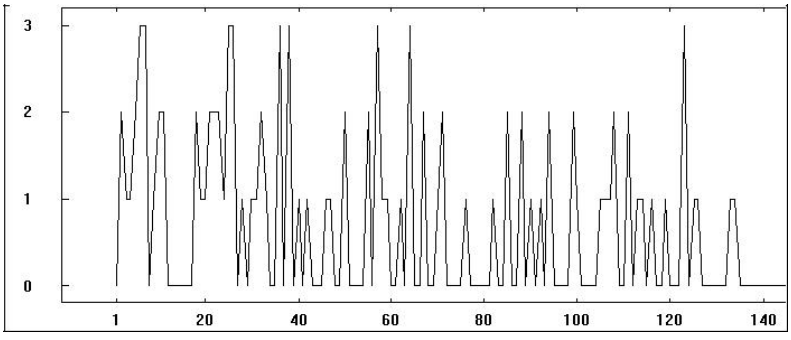


Figure 9. Derived key length: 2

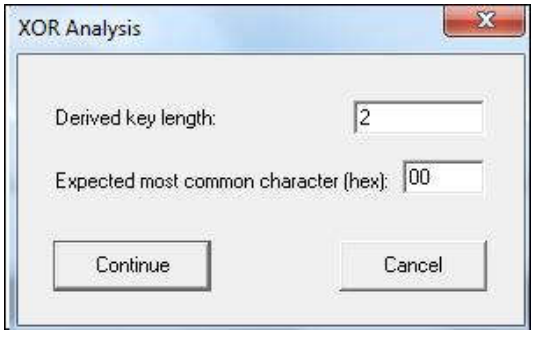


Figure 8. Analysis: Autocorrelation

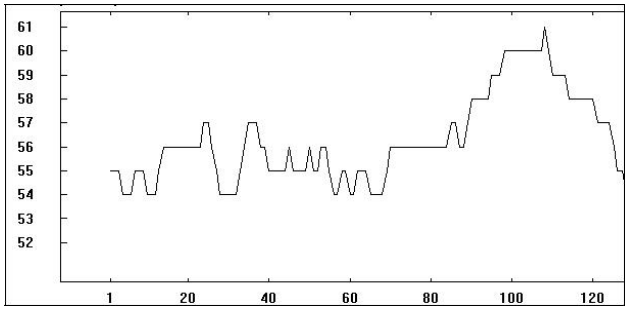


Figure 10. Floating frequency

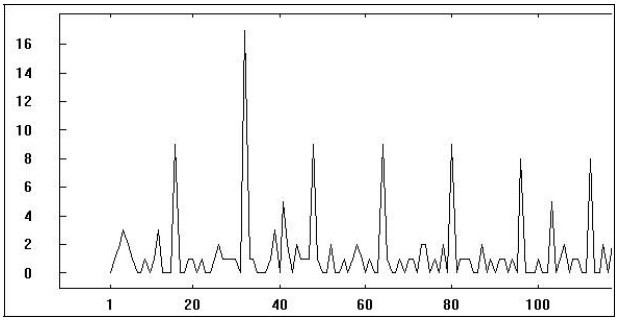


Figure 11. Autocorrelation

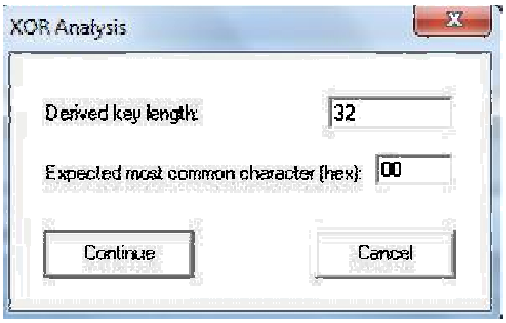
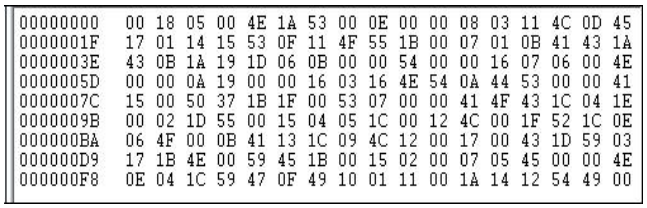


Figure 12. Derived key-length is 32.



00000000	00	18	05	00	4E	1A	53	00	0E	00	00	08	03	11	4C	0D	45
0000001F	17	01	14	15	53	0F	11	4F	55	1B	00	07	01	0B	41	43	1A
0000003E	43	0B	1A	19	1D	06	0B	00	00	54	00	00	16	07	06	00	4E
0000005D	00	00	0A	19	00	00	16	03	16	4E	54	0A	44	53	00	00	41
0000007C	15	00	50	37	1B	1F	00	53	07	00	00	41	4F	43	1C	04	1E
0000009B	00	02	1D	55	00	15	04	05	1C	00	12	4C	00	1F	52	1C	0E
000000BA	06	4F	00	0B	41	13	1C	09	4C	12	00	17	00	43	1D	59	03
000000D9	17	1B	4E	00	59	45	1B	00	15	02	00	07	05	45	00	00	4E
000000F8	0E	04	1C	59	47	0F	49	10	01	11	00	1A	14	12	54	49	00

Figure 13. Intermediate decrypted message by the derived key

The character set of the similar frequency pattern cannot be identified easily by this analysis. Therefore in the phase1 we found that using analysis we cannot retrieve the original message. In phase1 we are using the same key for XOR and AES encryption.

PHASE 2

In this phase we will change the key after the XOR encryption.

Step1: Select the text file to encrypt. Choose the first password. 5F 4D CC 3B 5A A7 65 D6 1D 83 27 DE B8 82 CF 99

Step2: XOR

Step3: Take the second password and apply hash function (MD5) 8E 70 38 3C 69 F7 A3 B7 EA 3F 71 B0 2F 3E 97 31

Step4: Applying AES encryption

Step5: Analysis of encrypted message is done with autocorrelation and frequency analysis.

Similarity between the sections of the document from the output shown in figure 8 cannot be determined using the Autocorrelation. In the frequency analysis (figure10) distance between the character set and frequency of alphabets can be considered as the key length. From the given output the frequency of alphabets cannot be identified by an intruder. It is the index of similarity between different sections of the document. It helps to find the cycle length for the automatic analysis of the encryption by Exclusive OR. XOR analysis is done but the key-length derived will not match with the original message. The key-length derived from autocorrelation will also produce a different value. Analysis XOR using the previous key will not derive back the original message. Figure below shows the output after the decryption with the XOR. This explains that the man-in-the-middle will not be able to derive the key-length or the key and thus the original message is not retrieved.

Conclusion

The frequency analysis and the derived key using XOR analysis of the Cryptool are taken as the output where the parameters show different values than the previous encryption procedure. This proves that the man-in-the-middle attack can be minimized with the above technique. When the packets forward from one network to another the change in keys will be implemented to avoid the hackers or intruders to attack the network easily. This technique can be implemented in MANETs where risk of security is found. The results shows that when a message is encrypted using two different keys it will make the information more secure. We can extend the technology to other complicated encryption algorithms to implement more security in the network.

REFERENCES

Deepti Ranaut, Madal Lal, 2014. "A review on Security Issues and Encryption Algorithms in Mobile Ad hoc Networks", *International Journal of Science and Research (IJSR),* Vol 3 Issue 6, June pg. 146-148

Halil Ebrahim Bulbul, Ihsan Batmaz, Mesut Ozel, Wireless Network Security: Comparison of WEP (Wired Equivalent Privacy) Mechanism, WPA (Wi-Fi Protected Access) and RSN (Robust Security Network) Security Protocols.

Borisov. N., Goldberg, I., Wagner, D., Intercepting Mobile Communications :The Insecurity of 802.11. http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf

Fluhrer, S., Mantin, I., Shamir, A., Weaknesses in the Key Scheduling Algorithm of RC4. http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pd f

A. Arbaugh,W., Shankar N., Justin Wan,Y.C., Your 802.11 Wireless Network Has No Clothes. http://www.cs.umd.edu/~waa/wireless.pdf

Stubblefield A., Ioannidis J., D. Rubin A., Using the Fluhrer, Mantin, and Shamir Attack. to Break WEP. Revision 2, August 21,2001, AT&T Laboroties and Rice University. http://www.uninett.no/wlan/download/wep_attack.pdf

Hoang, T. Dinh, Chonho Lee, Dusit Niyato and Ping Wang 2013. "A survey of Mobile cloud computing: Architecture, Application and Approaches", *Wireless Communications and Mobile Computing,* 13:1587-1611

Madhurya, M., B. Anandakrishna, T. Subhakshini, 2014.

Implementation of Enhanced Security Algorithms in Mobile Adhoc Networks I. *J. Computer Networks and Information Security,* 2, 30-37

Menezes, S. Vanstone and D. Hankerson, 2004. "Guide to elliptic curve cryptography", Springer Professional Computing (Springer, New York).

Mohd Izhar and Dr. V.R. Singh, 2014. "Network Security Vulnerabilities: Malicious node attack" *International Journal of Scientific and research Publications*, Volume 4, Issue &, July.

Pramendra Kumar, Vijay Kumar Sharma, 2014. Contemporary exploration of Wireless Network Security issues and Design challenges for an Enterprise network, *International Journal of Engineering, Management and Sciences*, Volume-1, Issue-3 March.

Ram Shringar Raw, Manish Kumar, Nayhay Singh, "Security challenges, Issues and their solutions for VANET", *International Journal of Network Security and its Applications (IJNSA),* Vol.5, September 2013

Stallings W. 2011. "Cryptography and network security Principle and Practice", 5th Edition, Prentice Hall, PP 149-174, 192-206, 266-290, 300- 317, 362-374

Umesh Kumar, Sapna Gambhir, 2014. "A literature Review of Security Threats to Wireless Networks" *International Journal of Future Generation Communication and Networking*, Vol. 7 No. 4, pp. 25-34

Yang, H, H. Y. Luo, F. Ye, S. W. Lu and L. Zhang, 2004. "Security in mobile Ad hoc networks: challenges and solutions", *IEEE Wireless Communications,* PP. 38-47

****