Rijndael Algorithm for Multiple File Encryption Development

Bryan L. Guibijar

North Eastern Mindanao State University – San Miguel Campus, Surigao del Sur, Philippines

ABSTRACT

The paper examined the Rijndael Algorithm for multiple file encryption development of College of Information Technology Education in North Eastern Mindanao State University – Main Campus. It is based in waterfall model (SDLC) in which descriptive research was applied to computer science students. Data from the pre-assessment survey and interview were treated by using the weighted mean to determine the level of usability of developed multiple file encryption using Rijndael algorithm. The usability of multiple file encryption to secure different file types from malicious users/hackers. Thus, the developed application is important to protect the files of the students from unauthorized use of their projects/programs submitted.

KEYWORD: *Cipher, Rijndael Algorithm, File management, algorithm, development*

How to cite this paper: Bryan L. Guibijar "Rijndael Algorithm for Multiple File Encryption Development" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-6 | Issue-4, June 2022, pp.1164-1168, URL: www.ijtsrd.com/papers/ijtsrd50258.pdf

IJTSRD50258

INTRODUCTION

File security dramatically raises issue especially in cloud computing which raises concern in confidentiality, data availability and data integrity (Mukhopadhyay, Sonawane, Gupta, Bhavsar, Mittal, 2013). This issues commonly happen in some industry when the employee separated. In fact, IT admin faces felony for deleting files under flawed hacking law (Greenberg, 2016). These leads to catastrophe in file management in an industry that may cause interruption in most of the transaction and affect the growth of the industry. The creation of cryptograph using Rijndael algorithm as key factor to solve the issues (Rouse, 2007). The study aims to provide cryptograph using Rijndael algorithm to enhance all type of file security.

Cloud computing is promising and efficient, but there are many challenges for data privacy and security (Singla, Singh, 2013). According to Rouse (2007), Rijndael algorithm is a new generation symmetric block cipher that supports key sizes of 128, 192 and 256 bits. Thereby, the encryption or decryption of a block of data is accomplished by the iteration of a specific transformation (Kaleigh, 2000). Although, Rijndael Algorithm is selected by the U.S. National Institute of Standards and technology (NIST) as candidate for the Advanced Encryption Standard (AES) (Daemen, Rijmen, 2013). However, several studies revealed the weaknesses of RIJNDAEL (Kaleigh, 2000). Where in fact, according to Hoang and Nguyen (2012), the design uses an iterative looping approach with block and key size of 128 bits.

Encryptions are popularly utilized to protect files from unauthorized users and malwares. Encryption was used to achieve authenticated communication in computer networks (Needham, Schroeder, 1978). In fact, cryptography is necessary when communicating over unreliable medium (Pitchaiah, Daniel, 2012). However, according to Townsend, (2015), the key burned in their C# code, they are doing the encryption but the encryption key is weak and it’s just a password. Which revealed the even using latest programming language will be in vain without the help of the Rijndael Algorithm. With that, National Institute of Standards and Technology (NIST) adopted the Rijndael algorithm as new Advanced Encryption Standard (AES) to replace existing Data Encryption Standard (DES) (Adib, Raissouni, 2012).

Implementation of Rijndael algorithm to enhance all type of file security provides resilient file management especially in cloud computing. Thereby, Cloud Cognitive Authenticator (CCA) proposed provided by the Advanced Encryption Standard (AES) which is the Rijndael algorithm. Thus, enhancing the security issues from unauthorized users and malwares. The study increases the security for confidentiality, data availability and data integrity. It also creates harmonious environment between the civilian users and hackers. In fact, hackers doing may be avoided using the Rijndael algorithm encryption method.

Theoretical / Conceptual Framework

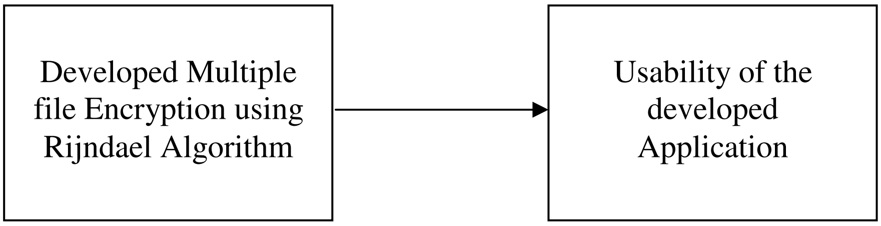
Developed Multiple file Encryption using Rijndael Algorithm
Usability of the developed Application

Figure 1 The Schema of the Study

The schema of this study explains the development of multiple file encryption using Rijndael Algorithm. The Multiple file encryption using Rijndael Algorithm is an application intended to encrypt different file types to avoid file thief, file alter and file damage by a virus. As a result student file security will be strengthen.

Cyber Security Theory, according to Kuusisto (2013), that the study on the key concepts and terms of cyber security and presents the physical world and the cyber world framework. It also refers about the society and uses of the model to analyse the results of two limited media survey about cyber-related newspaper. It also added that the media survey indicate strong need to organize the cyber world.

RESEARCH DESIGN AND METHODS

The study is a descriptive type of research in which survey questionnaire and interview was applied to the students of College of Engineering, Computer Studies and Technology (CECST) to find out the level of usability of the *developed multiple file encryption using Rijndael Algorithm* after utilizing the developed apps. The survey instrument was validated by IT experts two from College of Engineering, Computer Studies and Technology and two outsource.

The data collected were tabulated and analysed. Appropriated statistical tool were employed in the data analysis. Mean was used to determine the usability of developed multiple file encryption using Rijndael Algorithm.

Round Transformation

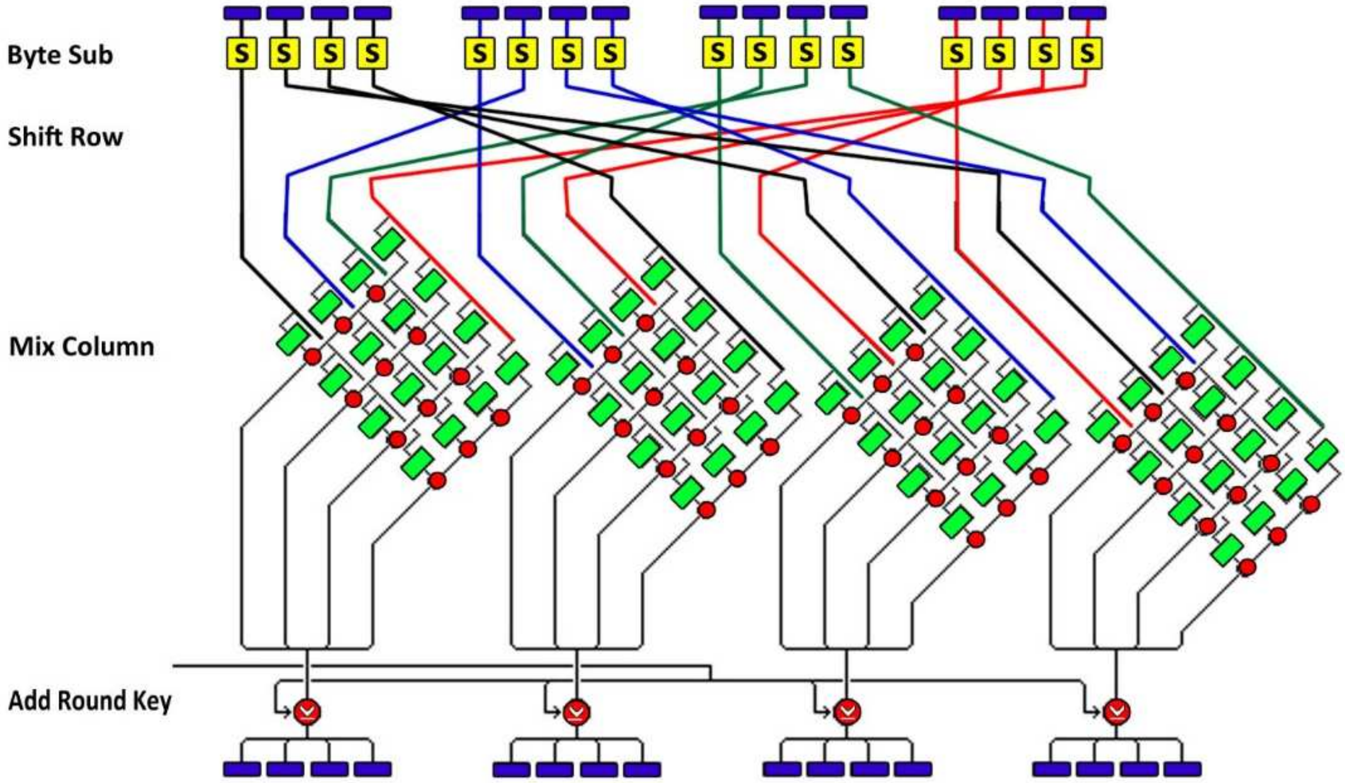

Figure 2 Rijndael Algorithm Round Transformation

Figure 2 - According to the creator of Rijndael Algorithm the round transformation is broken into layers and this layers are the linear mixing layer, which provides high diffusion over multiple rounds. The non-linear layer which are basically application of the Rijndael S-box and the key addition layer which is simply an exclusive or of the round key and the intermediate state. Each layer is designed to have its own well-defined function which increases resistance to linear and different cryptanalysis.

Application Data Flow Diagram

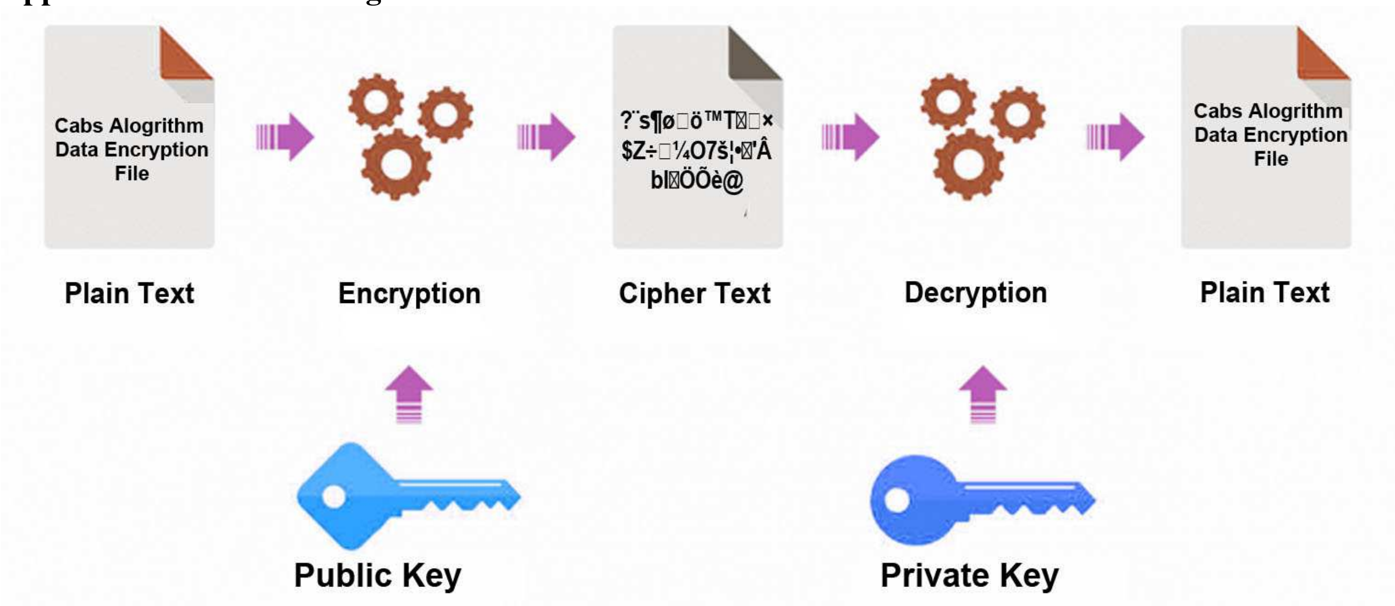
Cabs Alogrithm Data Encryption File
?¨s¶ø□ö™T⊠□× $Z÷□¼O7š¦•⊠'Â bl⊠ÖÕè@
Cabs Alogrithm Data Encryption File
Plain Text
Encryption
Cipher Text
Decryption
Plain Text
Public Key
Private Key

Figure 3 Application Data Flow Diagram of the Study

Figure 3 – As illustrated in the data flow diagram of the study, the file/s (Plain Text) was process using Public Key. Under Encryption is the application of the Rijndael Algorithm in which encrypting the file/s to hide the originally contain/form by substituting special character and the like to protect from malicious users. Cipher Text label is the output of the encrypted file/s that is not readable by human language or natural language. Decryption process is the process to return the file/s into its original contain/form.

Encrypt Flow Chart

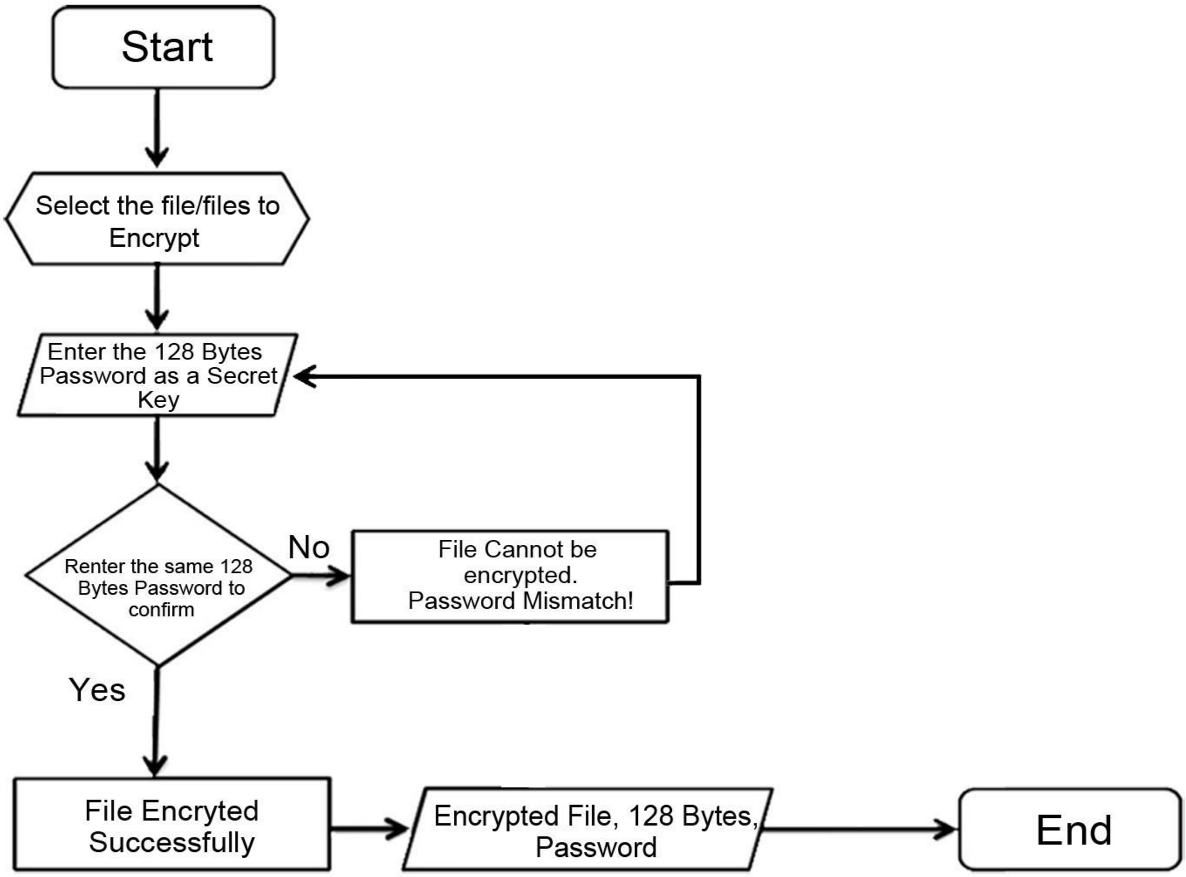
Start
Select the file/files to Encrypt
Enter the 128 Bytes Password as a Secret Key
Renter the same 128 Bytes Password to confirm
No
File Cannot be encrypted. Password Mismatch!
Yes
File Encryted Successfully
Encrypted File, 128 Bytes, Password
End

Figure 4 Encryption Flow Chart of the Study

Figure 4 – Encryption Flow Chart, using the sequential process in encrypting a file. The oval (Terminal) symbol indicate that the flow chart started and ended. The Preparation/ Initialization symbol next to start, it signifies the preparation of the data it is also use to select initial conditions and it is also used to represent instructions or group of instructions that will alter or modify a program's course of execution. The input / output symbol, data are to be read into the computer memory from an input device or data are to be passed from the memory to an output device, in this flow chart it is the input of 128 bytes password as a secret key. The diamond (Decision) symbol, it signifies any decisions that are to be done, two alternative execution paths are possible. The path to be followed is selected during the execution by testing whether or not the condition specified within the outline is fulfilled. The rectangle (Processing) symbol, perform any calculation that are to be done. In decision symbol there are two alternative execution paths the 'Yes' and 'No', if yes the remark is "File Encrypted Successfully", but if no the remark is "File Cannot be encrypted. Password Mismatch!" in this illustration it is password mismatch, but sometimes it can be the file is to large. As the flow near to the end the output was successfully encrypted with password protect to tighten the security of the encrypted file/s.

Decryption Flow Chart

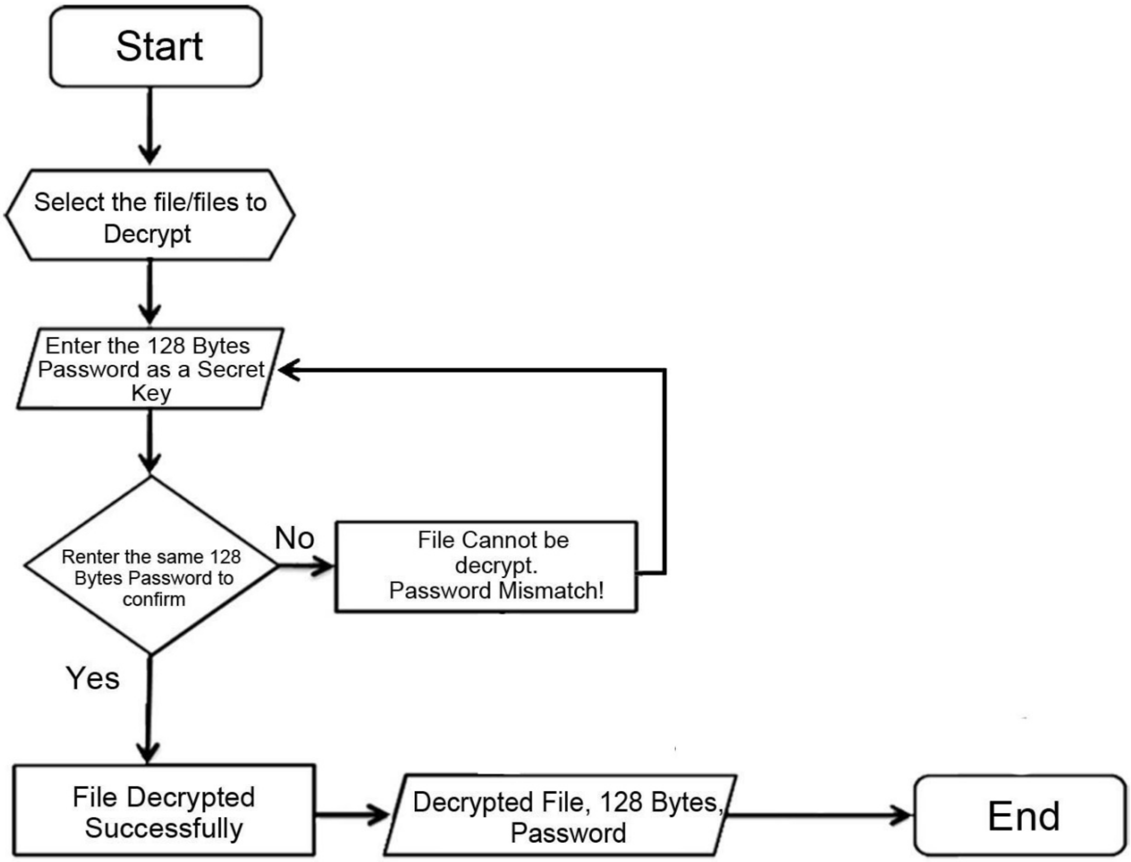
Start
Select the file/files to Decrypt
Enter the 128 Bytes Password as a Secret Key
Renter the same 128 Bytes Password to confirm
No
File Cannot be decrypt. Password Mismatch!
Yes
File Decrypted Successfully
Decrypted File, 128 Bytes, Password
End

Figure 5. Decryption Flow Chart of the Study

Figure 5 – The Decryption Flow Chart of the Study, is the reverse process to return the file/s into the original contain/form. As stated in figure 4, the process is the same from start to initialize the file or selecting the file to be decrypt. Then enter the password and test if the password is correct or incorrect. If not re-enter the password and if correct proceed to successfully decrypt the file/s selected, and finally the original file/s can be read by human or can be read using natural language.

RESULTS AND DISCUSSIONS

Table 1 Level of Usability of the Developed Application using Rijndael Algorithm

Indicators	Mean	Adjectival Rating
1. How do you rate the functionality of the apps in terms of performance?	3.03	Average
2. How do you rate the graphical user interface design of this apps?	2.96	Average
3. How do you rate operational performance of this apps?	2.95	Average
4. How do you rate the apps in terms of users-friendliness?	3.00	Average
5. How do you rate the security of the apps?	3.04	Average
Grand Mean	**2.99**	**Average**

Legend: 4.21-5.00-Excellent, 3.41-4.20-Good, 2.61-3.40-Average, 1.81-2.60-Poor, 1.00-1.80-Very Poor

Table 1 shows level of usability of the developed application. It reveals that all indicators are in the level of "*Average*". Thus, respondents give passing rate on the developed application. It implies that the program has need some improvements to gain higher rating other than average rate application. Based in the mean shown in table 1, the graphical user interface design and operational performance is the lesser mean. As the results shows that's the developer must improve the graphical user interface and operational performance of the developed application.

Table 2 Factors level of Concept and Difficult

	YES	NO
1. Do you understand the concept of the developed apps?	99.13%	0.87%
2. Did you encounter any difficulty while using the apps?	2.61%	97.39%

Table 2 shows factors level of concept and difficult. As it is shown in the table among the respondents 99.13% said 'Yes' they understand the concept of the developed application and 0.87% said 'No' they don't understand the concept of the develop application. It is also shown that 2.61% said 'Yes' they encountered difficulty while using the application and 97.39% said 'No' they don't encountered difficulty in using the develop application.

CONCLUSION

This study gets the usability of the Development Multiple File Encryption using Rijndael Algorithm, attempting to give free hassle from malicious users/hackers. In developing multiple file encryption using Rijndael Algorithm, developer must think about the encryption application available in the internet. As claim by Cyber Security Theory, to look into the physical world and cyber world framework and strongly recommend that the media must reorganized the cyber world.

RECOMMENDATION

It is strongly recommended by the author of this research to use the developed application as tool in securing the file/s in your computer. As the researcher recommend to use this application, it is also recommend not to use file encryption / decryption downloaded from the internet. Thus using application that is available to all might be the reason of the file/s corrupt and the file/s is not secure in some ways.

REFERENCES CITED

[1] Daemen, J., & Rijmen, V. (2013). *The design of Rijndael: AES-the advanced encryption standard*. Springer Science & Business Media. Retrieve October 11, 2017 from https://goo.gl/1DZm3n

[2] El Adib, S., & Raissouni, N. (2012). AES encryption algorithm hardware implementation architecture: resource and execution time optimization. *International Journal of Information and Network Security*, *1*(2), 110. Retrieve October 12, 2017 from https://goo.gl/4wJZ2x

[3] Hoang, T. (2012, February). An efficient FPGA implementation of the Advanced Encryption Standard algorithm. In *Computing and Communication Technologies, Research, Innovation, and Vision for the Future (RIVF), 2012 IEEE RIVF International Conference on* (pp. 1-4). IEEE. Retrieve October 11, 2017 from https://goo.gl/eFfQUv

[4] Kaleigh (2000, November 15). Advanced Encryption Standard. File. Retrieve October 10, 2017 from https://goo.gl/jYVZgs

[5] Mukhopadhyay, D., Sonawane, G., Gupta, P. S., Bhavsar, S., & Mittal, V. (2013). Enhanced security for cloud storage using file encryption. *arXiv preprint arXiv:1303.7075*. Retrieve October 10, 2017 from https://arxiv.org/abs/1303.7075

[6] Greenberg, A. (2016, June 03). ANDY GREEN SECURITY. File. Retrieve October 10, 2017 from https://goo.gl/q3Q4gy

[7] Needham, R. M., & Schroeder, M. D. (1978). Using encryption for authentication in large networks of computers. Communications of the ACM, 21(12), 993-999. Retrieve October 11, 2017 from https://goo.gl/dj9SeR

[8] Pitchaiah, M., & Daniel, P. (2012). Implementation of advanced encryption standard algorithm. Retrieve October 12, 2017 from https://goo.gl/7wyzjX

[9] Rauno Kuusisto, Tuija Kuusisto (October 2013). Strategic Communication for Cyber-Security Leadership. Journal of Information Warfare, Volume 12, Issue 3. Retrieve May 22, 2018 from https://goo.gl/ga88Q8

[10] Singla, S., & Singh, J. (2013). Survey on Enhancing Cloud Data Security using EAP with Rijndael Encryption Algorithm. *Global Journal of Computer Science and Technology*. Retrieve October 10, 2017 from https://goo.gl/H9ARHF

[11] Townsend, P. (2015, December 23). Fixing Encryption key management audit failures in Microsoft Windows C# applications. Retrieve October 12, 2017 from https://goo.gl/Z4QDXP