IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 22, Issue 6, Ser. I (Nov. – Dec. 2020), PP 39-44
www.iosrjournals.org

Using AES Algorithm Encryption and Decryption of Text File, Image and Audio in Openssl and Time Calculation for Execution

Nikhil Anand
(School of Electronics Engineering, VIT University, Chennai, India)

Abstract: *Cryptography is used to secure and protect data during communication. It is helpful to prevent unauthorized person or group of users from accessing any confidential data. Encryption and decryption are the two essential functionalities of cryptography [4].A message sent over the network is transformed into an unrecognizable encrypted message known as data encryption. At the receiving end, the received message is converted to its original form known as decryption [2].Encryption is a process which transforms the original information into an unrecognizable form. This new form of the message is entirely different from the original message. That's why a hacker is not able to read the data as senders use an encryption algorithm. Encryption is usually done using key algorithms. Decryption is a process of converting encoded/encrypted data in a form that is readable and understood by a human or a computer. This method is performed by un-encrypting the text manually or by using keys used to encrypt the original data.*

Key Word*: Cryptography; AES algorithm; Encryption and Decryption; Openssl tool; Security; Integrity.*

Date of Submission: 10-12-2020 Date of Acceptance: 25-12-2020

I. Introduction

The Advanced Encryption Standard (AES) is a symmetric block cipher chosen by the U.S. government to protect classified information. AES is implemented in software and hardware throughout the world to encrypt sensitive data. It is essential for government computer security, cyber security and electronic data protection. The National Institute of Standards and Technology (NIST) started development of AES in 1997 when it announced the need for an alternative to the Data Encryption Standard (DES), which was starting to become vulnerable to brute-force attacks. NIST stated that the newer, advanced encryption algorithm would be unclassified and must be "capable of protecting sensitive government information well into the 21st century." It was intended to be easy to implement in hardware and software, as well as in restricted environments -- such as a smart card -- and offer decent defenses against various attack techniques.AES was created for the U.S. government with additional voluntary, free use in public or private, commercial or noncommercial programs that provide encryption services. However, nongovernmental organizations choosing to use AES are subject to limitations created by U.S. export control.

II. Methods

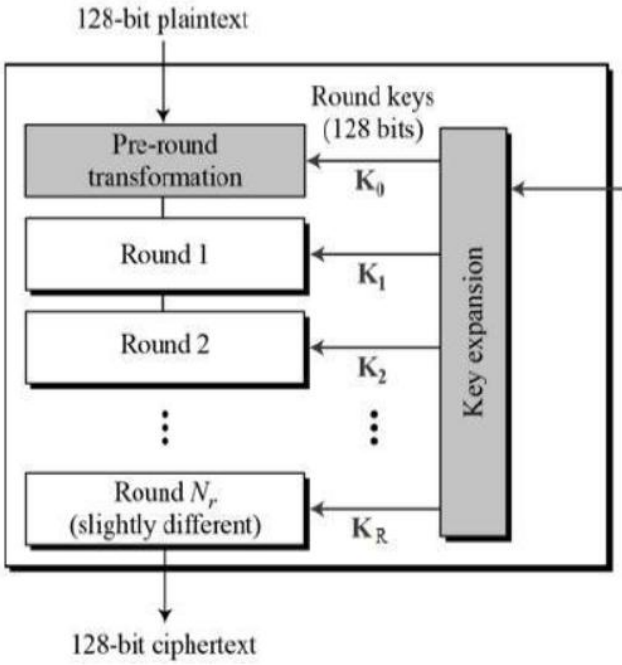
How AES encryption works

AES includes three block ciphers: AES-128, AES-192 and AES-256.

AES-128 uses a 128-bit key length to encrypt and decrypt a block of messages, while AES-192 uses a 192-bit key length and AES-256 a 256-bit key length to encrypt and decrypt messages. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128, 192 and 256 bits, respectively.

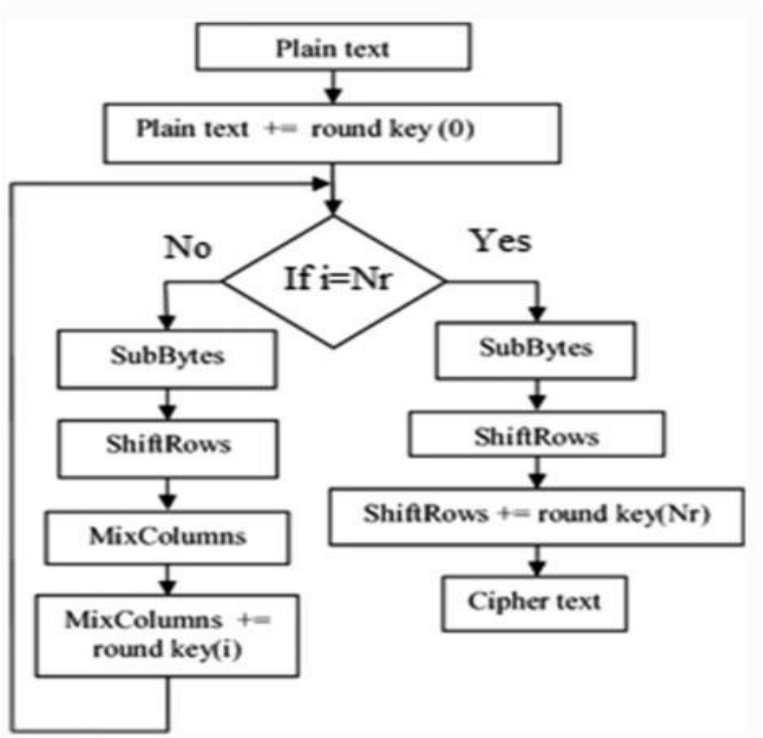
Symmetric, also known as *secret key* , ciphers use the same key for encrypting and decrypting, so the sender and the receiver must both know -- and use -- the same secret key. The government classifies information in three categories: Confidential, Secret or Top Secret. All key lengths can be used to protect the Confidential and Secret level. Top Secret information requires either 192- or 256-bit key lengths.

There are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. A round consists of several processing steps that include substitution, transposition and mixing of the input plaintext to transform it into the final output of cipher text.



R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size



OPENSSL

Openssl is a robust, commercial-grade, and full-featured toolkit for the Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocols. It is also a general-purpose cryptography library. For more information about the team and community around the project, or to start making your own contributions, start with the community page.

Encryption of text file

Commands:

time openssl aes -256-cbc –a –iter 1024 –in index.php –out encrypt.enc : This command is used for encrypting the given file.

time openssl aes -256-cbc –a -d –iter 1024 –in encrypt.enc –out decrypt.decry : This command is used to decrypt the encrypted file

Encryption and decryption of images

Commands :

time openssl aes-256-cbc –a –iter 1024 –in pic_original.bmp –out encrypt.enc : This command is used for encryption of original image.

time openssl aes-256-cbc –a -d –iter 1024 –in encrypt.enc –out decrypt.decry : This command is used for decrypting the encrypted image file.

Encryption and decryption of audio

Commands:

time openssl aes-256-cbc –a –iter 1024 –in audiofile.mp3 –out encypt.enc : This command is used for encryption of audio information

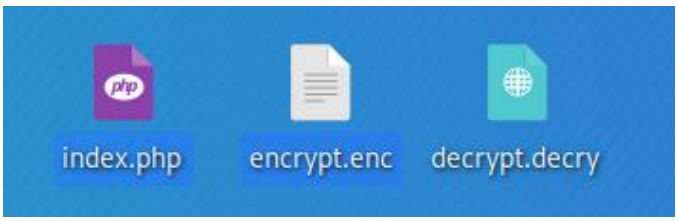
time openssl aes-256-cbc –a -d –iter 1024 –in encrypt.enc –out decrypt.decry : This command is used for decryption of audio information.

III. Result and Discussion

Text File

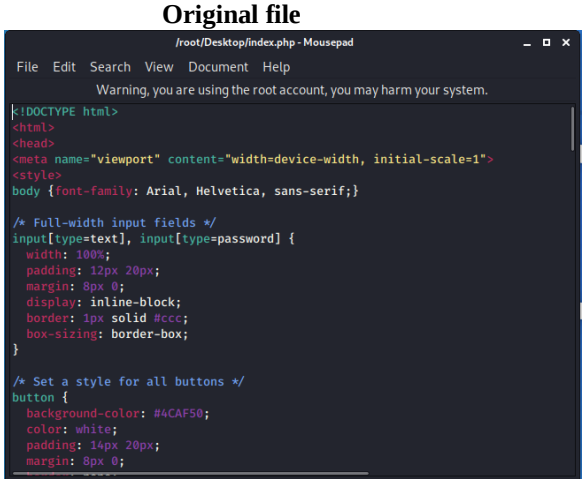
The original text file is encrypted and decrypted using the command and also time for execution is also calculated.

```
root@kali:~/Desktop# time openssl aes-256-cbc -a -iter 1024 -in index.php -out encryp.enc
enter aes-256-cbc encryption password:
Verifying - enter aes-256-cbc encryption password:

real    0m4.927s
user    0m0.011s
sys     0m0.000s
root@kali:~/Desktop# time openssl aes-256-cbc -a -d -iter 1024 -in encryp.enc -out decryp.decry
enter aes-256-cbc decryption password:

real    0m2.435s
user    0m0.011s
sys     0m0.000s
root@kali:~/Desktop#
```

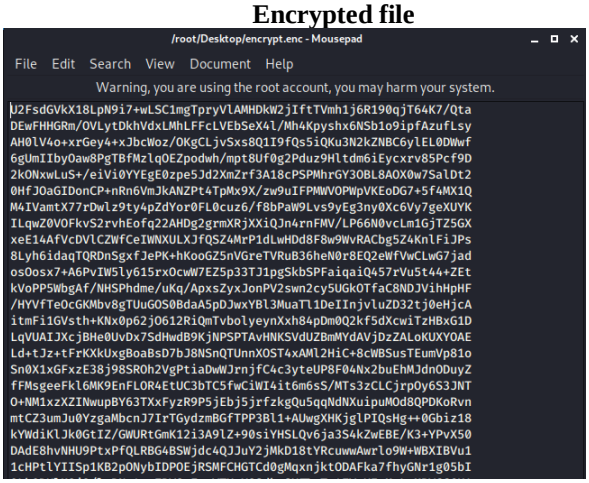


Original is taken which is then converted into encrypted file using AES algorithm. We can see the encrypted file which is not readable and after that the encrypted file is decrypted using the same AES algorithm and by giving the correct key or password we get back the original file

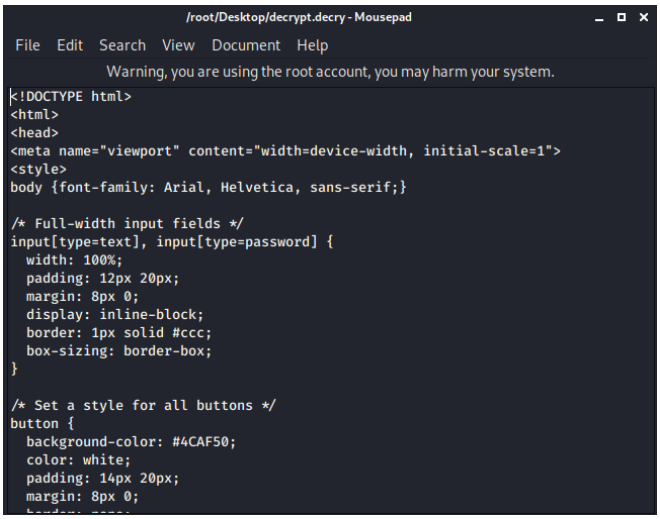
Original file



Encrypted file



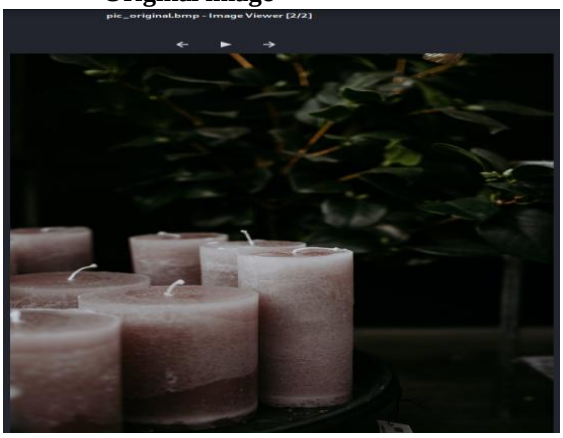
Decrypted file



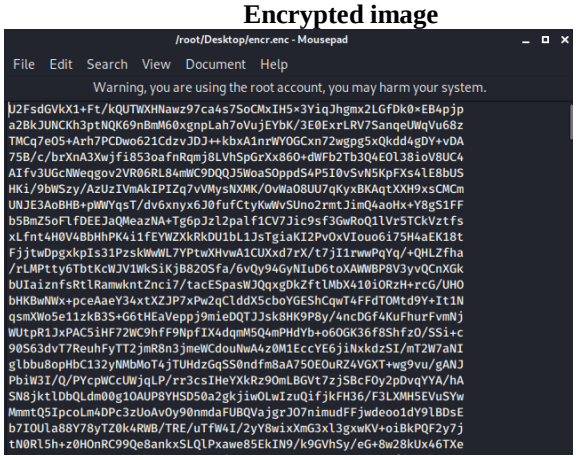
Image

The original image is encrypted to non readable format and then converted back to its original form by decrypting it using AES algorithm and also time of execution is also calculated.

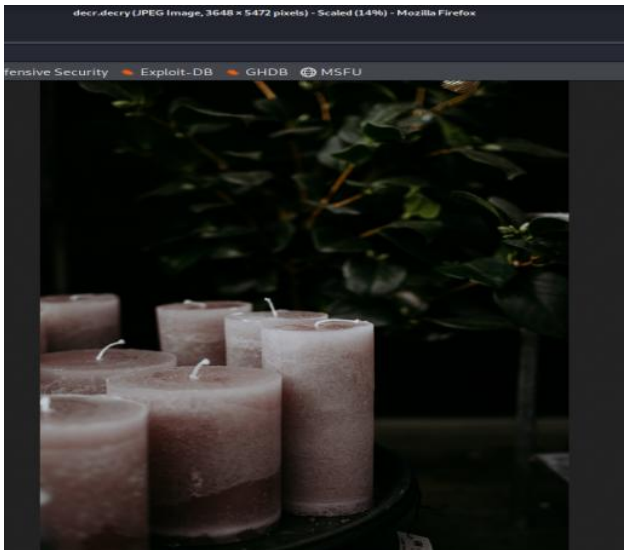
Original image



Encrypted image



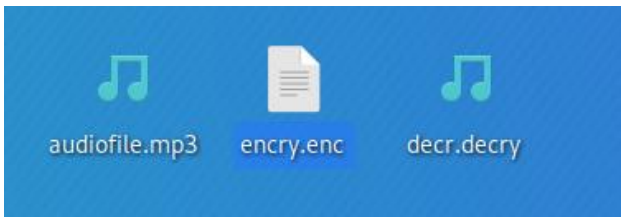
Decrypted image



AUDIO

The original audio file is encrypted and decrypted using the command and also time of execution is calculated.

```
root@kali:~/Desktop# time openssl aes-256-cbc -a -iter 1024 -in audiofile.mp3 -out encry.enc
enter aes-256-cbc encryption password:
Verifying - enter aes-256-cbc encryption password:

real    0m4.196s
user    0m0.004s
sys     0m0.008s
root@kali:~/Desktop# time openssl aes-256-cbc -a -d -iter 1024 -in encry.enc -out decr.decry
enter aes-256-cbc decryption password:

real    0m2.591s
user    0m0.010s
sys     0m0.000s
root@kali:~/Desktop#
```



Time taken for Encryption of text file is maximum followed by image and audio file. Decryption of files took more time compared to encryption.

IV. Conclusion

In this it shows s the successful encryption and decryption of normal text, file and image using AES algorithm in openssl tool. It gives better security against unauthorized access It also give the time consumption for the encryption and decryption to occur. The algorithm guarantees secure end to end transfer of data without any corrupt data. In future the work may be extended to audio and video encryption using openssl tool or different tool and comparing the time required for encryption and decryption.

References

[1]. International journal of Scientific and Engineering Research, Volume 7,Issue 2,February-2016 ISSN 2229-5518
[2]. File Encryption, Decryption Using AES Algorithm in Android Phone
[3]. A novel sensitive image encryption algorithm based on the Zaslavsky chaotic map
[4]. International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 6 Issue 4 April 2007 , Page No. 20915-20919
[5]. W. Stallings, Cryptography and Network Security, 4th Ed, pp. 58-309, Prentice Hall,2005.
[6]. W. Millan, "How to Improve the Nonlinearity of Bijective S-boxes," Lecture Notes in Computer Science, Vol. 1438, pp.181 - 192, Berlin: Springer-Verlag, 1998.

[7]. W. Stallings, Cryptography and Network Security, 4th Ed, pp. 58-309, Prentice Hall, 2005.
[8]. AtulKahate, "computer –based symmetric key cryptographic algorithm " , in cryptography and Network Security , 3th Ed. New Delhi McGraw-Hill , pp.130-141.
[9]. Sourabh Singh, Anurajjain ,(2013, May)."An Enhanced Text To Image Encryption Technique using RGB substitution and AES" , International journal of Engineering Trends and Technology (IJETT) volume -4,issue-5,pp.2108-2112.
[10]. https://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard#:~:text=The%20Advanced%20Encryption%20Standard%20(AES,cybersecurity%20and%20electronic%20data%20protection.
[11]. https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.html
[12]. https://www.openssl.org/
[13]. https://www.gitmemory.com/issue/elasticdog/transcrypt/59/491230983
[14]. http://myhackingjournal.blogspot.com/2016/10/encryption-and-decryption-of-images.html

Nikhil Anand. "Using Aes Algorithm Encryption and Decryption of Text File, Image and Audio in Openssl and Time Calculation for Execution." *IOSR Journal of Computer Engineering (IOSR-JCE)*, 22(6), 2020, pp. 39-44.