GUPTDOC AN ENTERPRISE PORTAL FOR CRYPTING WITH AES

Arzoo Misbha[1], Karuna Baswal[1], Madhuri N Simha[1], Rachel Abujam[1], Sowjanya C.M[2]

[1]Student, Dept. of Computer Science and Engineering, JVIT, Bidadi, Karnataka, India
[2]Assistant Professor, Dept. of Computer Science and Engineering, JVIT, Bidadi, Karnataka, India

---***---

Abstract - *Security of data means act of protecting data from actions of unauthorized users. There are many ways that provide security of data. Cryptography is one way to make sure that confidentiality, authentication and integrity of user's data can be secured and privacy can be provided. This paper proposes the encryption and decryption of text files using AES advanced encryption standard which is an effective encryption algorithm in application like internet to provide cyber security. AES or Rejindael is a network security algorithm used in all types of wired and wireless digital communication networks for secured transmission of data between two end user especially over public network.*

***Key Words*: Data security, Cryptography, Encryption, Decryption, AES, Rejindael, Symmetric key.**

1. INTRODUCTION

Cryptography plays a very important role in electronics, computers, and communication system design applications. Communication and transfer of data invariably necessitates the use of encryption. Since sending and reception of data is vulnerable to outside attack, data protection through encryption/decryption is critically important. Cryptography is referred to the translation of data in to a secret code (Encryption) and subsequently secret code back to data (Decryption) for security purpose. In the present scenario almost all the data is transferred over computer networks due to which it is vulnerable to various kinds of attacks.

Encryption is the process of obscuring information to make it unreadable without special knowledge. In the mid-1970s, strong encryption emerged from the sole preserve of secretive government agencies into the public domain, and is now used in protecting widely-used systems, such as Internet e-commerce, mobile telephone networks and bank automatic teller machines. In this paper we have endeavored the problems of authentication and security.

2. EXISTING SYSTEM

- The first, and still most consistently used asymmetric algorithm RSA is named on the three mathematicians who developed it, Rivest, Shamir, and Adleman. RSA today is used in many of software products and possibly used for key exchange, digital signatures, or encryption of small blocks of data. RSA uses a flexible size encryption block and a flexible size key. The key pair is acquired from a very large number, n, that is the product of two prime numbers chosen in accordance to special rules.

- DES was the first encryption standard to be recommended by National Institute of Standards and Technology. Many attacks and methods recorded that exploit the weaknesses of DES, which made it an insecure block cipher. Data Encryption Standard (DES) is a widely used method of data encryption using a private (secret) key that was judged so difficult to break.

- Triple DES, officially the triple data encryption algorithm is a key block, which applies the Data Encryption Standard cipher algorithm three times to each data block. The original DES cipher's key size of 56 bits was generally sufficient when that algorithm was designed, but the availability of increasing computational power made brute-force attacks feasible.

- Blowfish is a symmetric block cipher that can be used as a drop-in replacement for DES or IDEA. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for both domestic and exportable use.

3. PROPOSED SYSTEM

In the proposed system, it uses the efficient algorithm AES. It is a new encryption standard recommended by NIST to replace DES. Rijndael algorithm was selected in 1997 after a competition to select the best encryption standard. It is a symmetric cipher Information Processing (FIPS) Standard Number 197 in 2001 as the federal government approved encryption algorithm.

The National Security Agency has approved 128 bit AES for use up to SECRET level. AES is based upon the Rijndael algorithm, which was invented by Joan Daemen and Vincent Rijmen AES specifies three approved key lengths: 128 bits,192 bits and 256 bits. Brute force attack is the only effective attack known against it,in which the attacker tries to test all the characters combinations to unlock the encryption. AES was designed to have the following characteristics:

i) Resistance against all known attacks.
ii) Speed and code compactness on a wide range of platforms
iii) Design Simplicity

In the proposed system it users 128 bits and overcomes the unauthorized users to destruct data by generating token for individual user allowing them to encrypt and decrypt the text file safely. This proposes an encrypted portal which helps user easily to upload and download files. The user can easily download the file without having to undergo separate process for the decryption.

4. SYSTEM ARCHITECTURE

The System Architecture of the File Encryption and Decryption is as shown in the fig 1 .It describes various components and communication between those components. A user as depicted in the system architecture should be authorized to login to the system. The user will communicate with the application server to store the file through a web browser. When the user uploads the file it is encrypted using AES encryption algorithm.

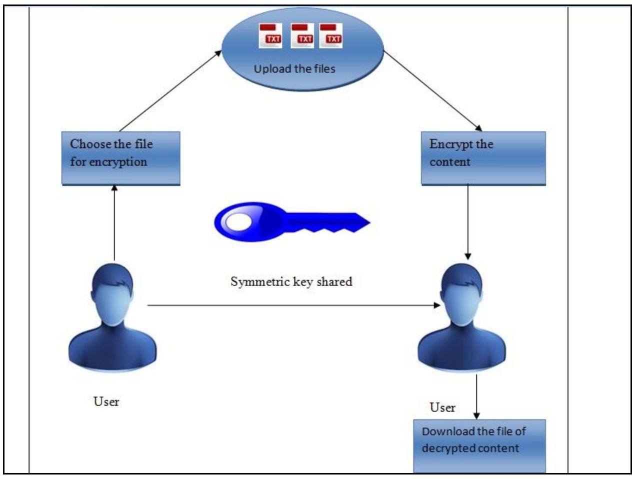


Fig -1: System Architecture

After the user uploads the file for encryption the file is stored which is in cipher text. The user then downloads the file to get back the decrypted text.

5. DISADVANTAGES WITH EXISTING SYSTEM

- DES uses a smaller block size compare to AES.
- Lack of security and authentication for user data.
- DES is breakable while AES is unbreakable.
- Undergoes long procedure for encryption and decryption.
- Use of smaller key length resulting insecure for many applications.

6. ADVANTAGES WITH PROPOSED SYSTEM

- Fast, secure, easy, efficient to use.
- Complete encrypted portal providing secure file encryption and decryption.
- AES is faster in hardware and software.
- AES is asymmetric block cipher where a pair of key is used to encrypt and decrypt the messages so that it arrives securely.
- The AES uses the Rijndael algorithm in combination with symmetrical block cipher as its encrypted method.
- Provide automatic decryption of files.

7. MODULES

The Application Modules are as follows:

7.1 Registration/Login

In this module for the first time login user needs to register with the system to use the application. In the registration page as shown in Figure 4.1 a form will be displayed to the user where valid information needs to be filled in the provided fields with a generated unique user id. A unique user id will be generated for registered users.

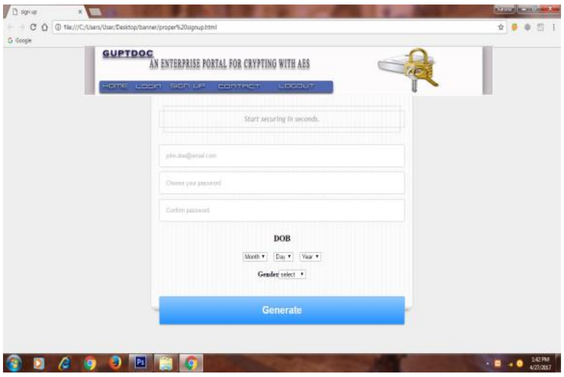


Fig -2: Login/Registration page

All the required fields need to be filled appropriately. Validations are performed on the fields entered. If the information filled in the form is not according to the requirements then condition fails and will be able to determine the reason and prompt error messages to the user for resolving this issue.

Once user clicks the generate button with valid information it needs to be uploaded in database. However, before uploading the user information into the database the application server creates a hash for the password entered by the user .The application server will replace the password entered by the user with the digest created.If the registration is successful, the user is redirected to the login page prompting successful registration.

After filling in all the fields of registration page the user gets a token generated, which will be used to redirect to the login page indicating the successful authentication of the user to encrypt. The token is generated is sent to the users mail.

7.2 Uploading File

In this module, a user can upload text files as shown in fig 3. The text files are encrypted and stored using AES algorithm of 128 bits. While uploading, the user needs to choose the file which is text format and click on encrypt and send button. When the user clicks on encrypt and send button the file is encrypted and the success message is displayed as shown in. The plain text converted to the cipher text is as shown in the fig4. The user can then click on the download file button to get the decrypted file.

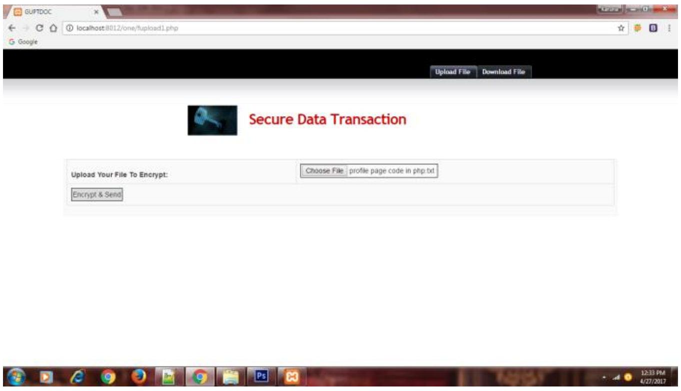
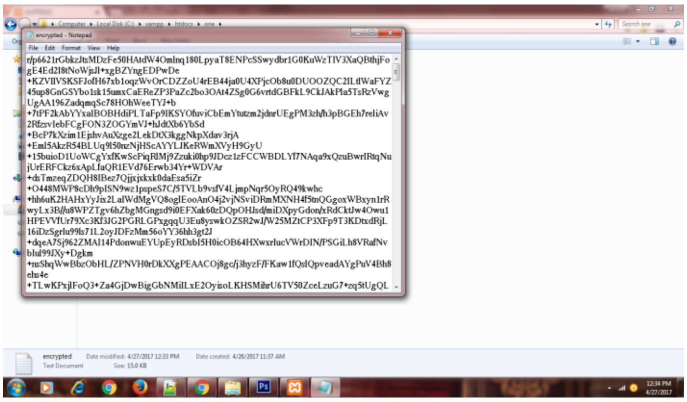


Fig -3: Uploading file



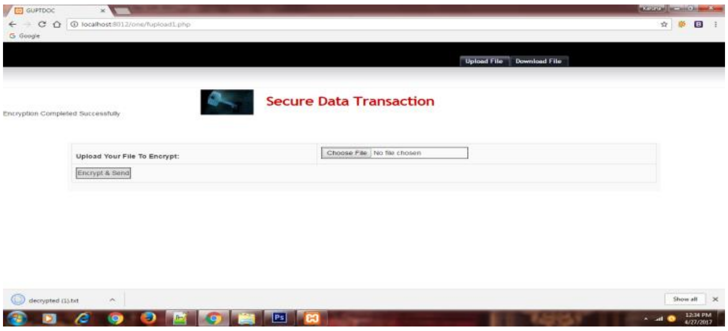
```
r/p6621rGbkzJtsMDzFe50HAtdW4Omlnq180LpyaT8ENPcSSwydbr1G0KuWzTIV3XaQBthjFo
gE4Ed2I8tNoWjsJl+xgBZYngEDPwDe
+KZVIlVSKSFJofH67xb1oqzWvOrCDZZoU4rEB44ja0U4XPjcOb8u0DUOOZQC2ILtlWaFYZ
45up8GnGSYbo1sk15umxCaEReZP3PaZc2bo3OAt4ZSg0G6vrtdGBFkL9CkJAkPla5TsRzVwg
UgAA196ZadqmqSc78HOhWeeTYJ+b
+7tPF2kAbYYxalBOBHdiPLTaFp9IKSYOfuviCbEmYtutzm2jdnrUEgPM3zh/h3pBGEh7reliAv
2RfzsvlebFCgFON3ZOGYmVJ+hJdtXb6YbSd
+BcP7kXzim1EjshvAuXzge2LekDtX3kggNkpXdav3rjA
+Eml5AkzR54BLUq9l50nzNjHScAYYLJKeRWmXVyH9GyU
+15buioD1UoWCgYxfKwScPiqRlMj9Zzuki0hp9JDcz1zFCCWBDLYf7NAqa9xQzuBwrlRtqNu
jUrERFCkz6xApLfaQR1EVd76Erwb34Yr+WDVAr
+dsTmzeqZDQH8lBez7Qjjxjxkxk0daEsa5iZr
+O448MWP8cDh9pISN9wz1pspeS7C/5TVLb9vsfV4LjmpNqr5OyRQ49kwhc
+hh6uK2HAHxYyJix2LalWdMgVQ8oglEooAnO4j2vjNSviDRmMXNH4f5tnQGgoxWBxyn1rR
wyLx3B//u8WPZTgv6hZbgMGngsd9i0EFXak60zDQpOHJsd/miDXpyGdon/xRdCktJw4Owu1
HPEVVfUr79Xc3Kf3JG2PGRLGPxgqqU3Eu8yswkOZSR2wJ/W25MZtCP3XFp9T3KDtxdRjL
16iDzSgrlu99ls71L2oyJDFzMm56oYY36hh3gt2J
+dqeA7Sj962ZMAI14PdonwuEYUpEyRDsbI5H0icOB64HXwxrlucVWrDIN/PSGiLh8VRafNv
bIul99JXy+Dgkm
+nsShqWwBbzObHL/ZPNVH0rDkXXgPEAACOj8gc/j3hyzF/FKaw1fQslQpveadAYgPuV4Bh8
ehs4e
+TLwKPxjlFoQ3+Za4GjDwBigGbNMilLxE2OyisoLKHSMihrU6TV50ZceLzuG7+zq5tUgQL
```

encrypted Date modified: 4/27/2017 12:33 PM Date created: 4/26/2017 11:37 AM
Text Document Size: 15.0 KB

Fig -4: Plain text converted to cipher text

7.3 Downloading File

The User he/she can download the file that was uploaded for encrypting. The user can automatically get the plain text of content without decrypting it. This is because the download file buttons when clicked by the user performs the function of decryption as well as download thereby enhancing the ease of process. The downloaded file is stored in the downloads folder of user along with the encrypted file. The user has the privilege to download the file that was uploaded to encrypt, any time before the expiry of token. The downloading of file is as shown in the fig 5.



Encryption Completed Successfully

Fig -5: Downloading file

7. CONCLUSIONS

Introducing a new approach for encryption and decryption of a text file by using AES which is the proposed system. The proposed algorithm have been tested against different known attacks and proved to be secure against them. It can be considered as a good alternative to some application because of high level of security and average time needed to encrypt and decrypt a data.

REFERENCES

[1] N.S Sai Srinivas, Md.Akramuddin - "Fpga Based Hardware Implementation Of Aes Rijndael Algorithm For Encryption And Decryption" 2016-Iceeot.

[2] Alexandern Uskov, Adam Byerly,Colleen Heinemann- "Advanced Ecryption Standard Analysis With Multimedia Data On Intel Aes-Ni Architecture" 2016-Ijcsa.

[3] P.Srinivas Rao, P.V.Lakshmi Priya, P.C.S Azad, K.Alekhya , K.Ragavendrarao And K.Kishore-"Technique Foe Data Encryption And Decryption "2014 –Ijfgcn.

[4] Roshni Padate, Aamna Patel "Encryption And Decryption Of Text Using Aes Algorithm" 2014-Ijetae.

[5] Gurpreet Kaur, Nishi Madaan "A Comparitive Atudy Of Aes Encryption Decryption"-2014 Ijsr

[6] Abhijith P.S , Dr. Manish Goswami, S.Tadi, Kamal Pandey –"Optimized Architecture Of Aes".