International Journal of Scientific Engineering and Technology (ISSN : 2277-1581)
Volume No.3 Issue No.10, pp : 1255-1258 1 Oct 2014

# Protect your data in today's world through cryptography

**Kaustubh verma, Shilpi Sharma**
ASET,Amity University, Noida
kaustubhverma@ymail.com , ssharma22@amity.edu

**ABSTRACT**

***Cryptography is one of the principal means for protecting information security. Not only it has the ability to make information confidential, but has also provided digital signature, secret sub storage system security and other functions. Therefore encryption and decryption can ensure the confidentiality of the information as well as the integrity of the information. Hence, what kind of data we choose to be a key, how to distribute the private key and how to save both data transmission keys are very important issues in encryption and decryption algorithm.***

***This paper proposes the guidelines for implementation of password based encryption cryptography. The system outlined in this paper includes an implementation of Data Encryption Standard (DES) and MD5 message digest algorithm by password based encryption (PBE) scheme for data encryption and decryption of a particular file of the existing source. In order to make the task of getting from password to key very time consuming for an attacker, the PBE implementation used in this paper is mixed in a random number known as salt and iterations in order to create a key.***

***Besides all this, this report also discusses the use of the database connectivity which is used for storing the records of all the users who have used this application in the database and retrieving other information already stored in database for encryption and decryption. Along with these techniques discussed till now, java GUI has also been used to make the application more presentable.***

**Keywords: Cryptography, Encryption, Decryption, MD5**

INTRODUCTION

With the introduction of computer, the need for protecting files and other information stored on the computer became evident. In the early days cryptography used to be performed by using manual techniques. Now in the present era two cryptographic concepts had been introduced to make data confidential and secure i.e. encryption and decryption. Encryption is the process of encoding messages in such a way that the hackers cannot read it, but that authorised parties can and decryption is the process of decoding data that have been encrypted into am unreadable format.

Passwords form the central aspect of the security system. They are generally a string of characters to gain access to resources and are usually human memorable that are considered vulnerable in security[1]. In this report we use password based encryption scheme along with DES and MD5 algorithm for encrypting and decrypting the contents which are stored in the files. The technique of generating a secret key from user generated passphrase is called password based encryption. It is typically used in applications where an attacker can repeatedly try to guess the password without being detected. Along with this technique two more methods were introduced to make data secure i.e. DES and MD5 algorithm. Here, DES encryption algorithm is used to encrypt or decrypt the contents of the file and MD5 algorithm is used to convert user given password into keys and maintains data integrity.

While the process of encryption and decryption was being carried out, another technique was being carried out for holding the records of the people who are performing this process. This technique is called database connectivity which is used for storing, retrieving or making changes in the data in the database. For this technique SQL package is used in java.

For making the java application more presentable java GUI has been used. Java GUI illustrates the use of labels, textfields, buttons, fonts etc in this java application.

OVERVIEW

During the entire process the system obtains the detailed information such as the contents of the files, the password of the user is converted into keys with MD5 algorithm and at the same time the contents of the file are being operated according to DES encryption algorithm and password converted the plain text into cipher text. Then the process of decryption is being carried out in the same way but in reverse order i.e. converting the cipher text into plain text.[2]

The technique used in this paper is PBEwithMD5andDES algorithm which is used to encrypt a given message with DES algorithm using a secret key (PBEKey) derived from password with MD5 message digest algorithm. Here, we use this algorithm for password based encrypting some message by using a cipher object which is being created by calling Cipher's getInstance method. To make the data more secure PBEParameterspec (created from salt and iterations) is used for properly initialising the cipher. The cipher text is then initialised by using update and doFinal methods.

Once we have obtained the cipher text and initialised it, then we are ready to use it for encryption and decryption. Here we encrypt and decrypt the contents of the files in order to make the information confidential.

Till now we have discussed the data is being decrypted and encrypted, but this report also holds its use in another way i.e. for storing and retrieving the records of the people who are using this java application. This technique is called database connectivity. In this technique when person is entering his record in the java application then his record is stored in the database. If the person again wants to use this application then he/she can retrieve his/her record if he/she desires and can perform the process of data encryption and decryption.

In addition to all this the java application created in this report also illustrates the use of java GUI in making of labels, textfields, buttons etc to make this application more presentable.

TECHNIQUES AND TECHNOLOGIES

A wide variety of technologies have lately been developed for encrypting and decrypting the data stored in the files. These technologies and the techniques involved in it can be illustrated as follows:

* Strengthening of hash functions using block symmetric key encryption algorithm –

The techniques that are used are MD5, DES algorithms.

* Enhancement of DES algorithm with multi state logic –

The technique that is used is DES algorithm.

* Secure file transmission scheme based on hybrid encryption technique –The techniques that are used are Double DES, RSA and MD5 digital algorithms.

* Analysis improved cryptography system using DES with RSA –

The techniques used are DES and RSA algorithms.

* Breaking of simplified DES using a genetic algorithm –

The technique used is a genetic algorithm which is a search algorithm based on natural selection.

* Enhancing the security in Bluetooth communication –

The techniques that are used are Triple DES, RSA and MD5 algorithms.

Of these technologies mentioned above, the technologies which are implemented in this report can be described as follows:

1. Strengthening hash functions using block symmetric key encryption algorithm –

Message integrity is one of the primary requirements in many of the today's network protocols. With the improvement in network speed, higher processing speed is also required for encryption and integration.

This technology discusses usage of encryption algorithm such as DES along with hash function such as MD5 to provide more security to the hash function in terms of improved message integrity. It also discusses the working of MD5 and DES functions and there key features.[3]

2. Enhancement of DES algorithm with multi state logic –

Cryptography usually referred to as the study of secret is nowadays most attached to the definition of encryption. Encryption is the process of converting the data into a form called cipher text that cannot be easily understood by unauthorised people. Decryption is the process of converting the encrypted data back into its original form so it can be understood. It is the easiest and most practical method of protecting data stored or transmitted electronically.

Encryption uses the mathematical algorithm to scramble readable text that cannot be read unless the reader has the key to unlock or convert the information back into readable form. Even a single failure to encrypt the data can result in a security breach with criminal or civil liabilities and irreparable harm to finances and the reputation of the university.[4]

METHODOLOGY

The methodology used in this report illustrates the use of PBEwithMD5andDES algorithm in the process of encryption and decryption. It also discusses the use of database in the process of database connectivity.

These methodologies can be explained as follows:

Encryption process

In the process of encryption the system obtains the contents of the file, converts the password of the user into keys with MD5

algorithm and in the same time converts the plain text into cipher text using DES algorithm

The encryption process can be explained as follows:

1. In the first step, the password of the user is converted into the keys using MD5 algorithm, here we have PBEKey ie password key which is created from the password.

2. In the previous step salt and iterations are used as an additional input to MD5 algorithm that hashes the password and used to defend against dictionary attacks, here we have PBEParameterSpec which is created from the salt and iterations.

3. Then cipher object is being created by calling cipher's getInstance method. This method is used to encrypt some messages in a common way by using PBEwithMD5andDES algorithm.

4. At almost the same time, when the password is converted into keys by using MD5 algorithm, the plain text is converted into cipher text by DES algorithm.

5. The cipher object is being properly initialised using update and doFinal methods. The update method is used as an encryption operation for processing another the data part and doFinal method is one in which the input data that have been buffered during previous update operation is processed, with the padding being applied. Upon finishing this method resets the cipher object to a state it was in when previously initialised via a call to init, i.e. the object is reset and available to encrypt more data.

6. Hence after both MD5 and DES encryption process have taken place, the data is being converted from plain text to cipher text.

Decryption process

The decryption process is just reverse of encryption process in which cipher text is converted back into plain text.

The decryption process can be explained as follows:

1. In the first step, the password of the user is converted into the keys using MD5 algorithm, here we have PBEKey ie password key which is created from the password.

2. In the previous step salt and iterations are used as an additional input to MD5 algorithm that hashes the password and used to defend against dictionary attacks, here we have PBEParameterSpec which is created from the salt and iterations.

3. Then cipher object is being created by calling cipher's getInstance method. This method is used to decrypt some message in common way by using PBEwithMD5andDES algorithm.

4. At almost the same time, when the password is converted into keys by using MD5 algorithm, the cipher text is converted into plain text by DES algorithm.

5. The cipher object is being properly initialised using update and getIV method. The update method is used as a decryption operation for processing another data part and getIV method is used in the context of password based decryption for decrypting back the data.

6. Hence after both MD5 and DES decryption process have taken place the data is being converted from cipher text to plain text.[5]

Database Connectivity process

The database connectivity process is used for storing the data in the database and retrieving the data already stored in the database. The steps for creating the database of a JDBC java application can be written as follows:

1. Import the java sql package.

2. Load and register the driver that connects to the data source name.

3. Then we establish the connection to the database.

4. Once the connection is established, then we use create a statement object.

5. Using this statement object, SQL statements are being constructed and executed to perform required transactions.

6. After these transactions are made, the query is executed that returns an object of type ResultSet. The ResultSet represents sets of rows that are retrieved from the database.

The steps for creating the data source name jdbc-odbc connectivity for Microsoft access drivers can be illustrated as follows:

1. Go to the control panel and select administrative tools.

2. Next select the ODBC Data sources (32 bit) icon.

3. Then press "Add" button.

4. Choose the driver for Microsoft Access and then press Finish button.

5. Type the data source name and press the "Select" button for choosing the database file which is already created.

6. Finally press "OK" button to complete the process.[6]

APPLICATIONS

Different areas where this report is useful for data encryption and decryption of files can be described below as follows:

1. It is used in encryption of electronic data.

2. It discourages anyone who can try to read our message that might contain our personal information.

3. DES algorithm used in this report for data encryption or decryption is more useful than the other asymmetric algorithms which makes it beneficial in many areas.

4. It is also used for providing encrypted data storage and proprietary software protection.

5. It is also used by the federal department and other government agencies for cryptographic protection of classified information.[7]

6. MD5 algorithm used in this report can be in the field of electronic discovery.

7. MD5 algorithm is also used in variety of security applications and used to check integrity of files.

8. MD5 digests that have been widely used in the software world is used to provide assurance that the transferred file has arrived intact.[8]

9. It is used in systems such as file encryption tools which are used to ensure data confidentiality. .

10. It is also used in applications that requires encryption and decryption of large amounts of data.

FUTURE WORK

Today's society requires secure data encryption devices to preserve data privacy. Of several encryption algorithms DES and MD5 algorithms have emerged to be most commonly used in varying applications.

The most widely used key cryptographic method i.e. DES algorithm, published in 1977 is still widely used to encrypt or decrypt messages. The requirement of good cryptographic functions are strongest than those in other applications. For this reason cryptographic hash functions make good stock hash functions even functions whose cryptographic security is compromised such as MD5 algorithm.

In spite of the features of these algorithms, security flaws have been detected in it and it is also susceptible to brute force attacks. Hence in order to lessen these defects and make data more secure this report discusses the use of salt and iterations in data encryption and decryption which makes the task of the attacker very time consuming. However other replacement algorithms had also been developed lately such as different variations of DES algorithms such as DoubleDES, TripleDES and AES algorithms that can eliminate such defects and whose products are now available in the marketplace.[9]

Hence this project sees its bright scope in the future as in spite of making data confidential by means of encryption and decryption, it is also used for storing and retrieving the information regarding the people who have used this java application.

In future we can use these techniques in such a way that it can consume less time and power furthermore; we can try to develop strong encryption algorithm with high speed and minimum energy consumption.

CONCLUSION

The main aim of this report is to encrypt or decrypt the contents of the file by means of password based encryption. In addition this report also tells us about the use of database for storing and retrieving information.

This report is used for providing the guidelines for data encryption and decryption of the contents of the particular file by means of password based encryption technique using DES and MD5 algorithms. The password which is used in this technique is used to ensure the confidentiality of the data stored in it. This report also provides guidelines for creating a database.

Even if MD5 and DES algorithms have been susceptible to brute force attacks and different security flaws, in this report we have used salt and iterations to reduce these defects and hence it has proven its worth in various applications.[10]

REFERENCES

i. *Fataftah Ishraq, "Password based cryptography", June 18, 2012.*

ii. *Pachghare V.K.,"Cryptography and information security", PHI Learning private limited, 2009.*

iii. *Purohit Richa, Singh Yogendra, Dr Mishra Upandra and Dr Bansal Abhay "Research paper on strengthening hash functions using block symmetric key encryption algorithm", September-October 2012.*

iv. *Patel Payal, Shah Kruti, Shah Khushbu, "Research paper on enhancement of DES algorithm with multi state logic", May 17, 2014.*

v. *Gupta Raj, "Password encryption decryption using PBE with MD5 and DES algorithm in java", October 14, 2012.*

vi. *Aptech Limited, "A simple approach-Core java", 2010.*

vii. *IBM, "Data Encryption Standard", 1977.*

viii. *Rivest Ronald, "MD5 Algorithm", April 1992.*

ix. *Srinivas N Raghavan, "Cryptography advances into the future", April 28, 2000*

x. *Abadi Martin and Warinschi Bogdan, "Password based encryption analysed".*