AES Password Encryption Technique

Ms. Shalmali Bhoir
Student
Department of Information Technology,
K. J. Somaiya College Of Engineering
Vidyavihar East, Mumbai, India
shalmali.b@somaiya.edu

Ms. Pragati Vaidya
Student
Department of Information Technology
K. J. Somaiya College Of Engineering
Vidyavihar East, Mumbai, India
pragati.v@somaiya.edu

Ms. Pinal Patel
Student
Department of Information Technology,
K. J. Somaiya College Of Engineering
Vidyavihar East, Mumbai, India
pinal.patel@somaiya.edu

Ms. Pooja Ajmera
Student
Department of Information Technology,
K. J. Somaiya College Of Engineering
Vidyavihar East, Mumbai,India
pooja.ajmera@somaiya.edu

Mrs.Sunayana Jadhav
Assistant Professor
Department of Information Technology,
K. J. Somaiya College Of Engineering
Vidyavihar East, Mumbai,India
sunayanavj@somaiya.edu

Abstract-In recent years the cases of hacking have increased at an exponential rate. The Advanced Encryption Standard (AES) is a National Institute of Standards and Technology specification for the encryption of electronic data. It is expected to become the accepted means of encrypting digital information, including financial, telecommunications, and government data. In this paper we explain the importance and the need for encryption and the Advanced Encryption Standard (AES) algorithm for password encryption. Included is a complete AES algorithm.

Keywords- *password encryption, multiple accounts, secret key, cipher text, Advance Encryption Standard*

*****

I. INTRODUCTION

Every project where security is the prime requirement needs some sort of encryption technique to ensure complete security of stored data. For example projects related to security sector of any nation such as arms and ammunitions, navy, police force or any system of a company which deals with data of high level officials or data pertaining to trade secrets etc. Projects related to these fields must ensure guaranteed protection of important data and information along with high level security standards.

The system we are developing is an Enterprise Resource Planning (ERP) System which takes inputs form the user by means of various forms, stores the data collected in the database and generates reports. As per the client's requirement, the system needs to be protected from unauthorized access. The algorithm is used in our ERP system which is based on C# .NET.

Cryptography is a vital part of securing private data and preventing it from being stolen. In addition to concealing the real information stored in the data, cryptography performs other critical security requirements for data including integrity, repudiation, authentication and confidentiality [13].

III. CRYPTOSYSTEM

Cryptosystem is a system or product that provides encryption and decryption. Cryptosystem uses an encryption algorithm which determines how simple or complex the encryption process will be. In encryption, key is a piece of information which states the particular conversion of plaintext to cipher text during encryption, or vice versa during decryption. The larger the key space, the more possible keys can be created. The strength of the encryption algorithm banks on the length of the key, secrecy of the key, the initialization vector, and how they all work together. Depending on the algorithm, and length of the key, the strength of encryption can be measured. Cryptography algorithms are of two types:

A. Symmetric algorithms, which use symmetric keys (also called secret keys) in this algorithm, the same key is used for encryption and decryption.
B. Asymmetric algorithms, which use asymmetric keys (also called public and private keys). In this algorithm, the different keys are used for encryption and decryption.

The traditional method to apply password authentication is via the use of password file stored at the remote server [1]. A client who wishes to enter to the server domain must send its login ID and password to the server. Almost all operating systems protect the password transit through one-way hash functions [2] that securely stores a

II. CRYPTOGRAPHY

Cryptography has its roots in the era of World War II. In the World War II cryptography played an imperative role that gave the allied forces the upper hand, and helped them in winning the war. They were able to dissolve the Enigma cipher machine which the Germans used to encrypt their military secret communications. Plaintext is the original data that is to be transmitted or stored, which is readable and understandable either by a computer or a person. Whereas the Cipher text, which is unreadable, neither machine nor human can make some meaning out of it until it is decrypted.

Cipher text is an art of protecting information by encrypting it into an unreadable form of text. This information can only be read by those who possess the secret key that can decipher (or decrypt) the message into original form.

password. Unfortunately, a simple brute force cracker can break the digest or the hash value of the password in some minutes [3]. For that, it becomes necessary to define another schema to protect the passwords file and the password itselfduring its transport over the connection channel between the client and the server.

IV. TYPES OF CRYPTOGRAPHIC ALGORITHMS

Cryptographic algorithms can be basically divided into two parts viz. Symmetric encryption algorithms and Asymmetric encryption algorithms [4]. These types are also known as Public key algorithms and Private Key algorithm respectively. Further these two types can be divided into subtypes as shown in the figure [5].

.

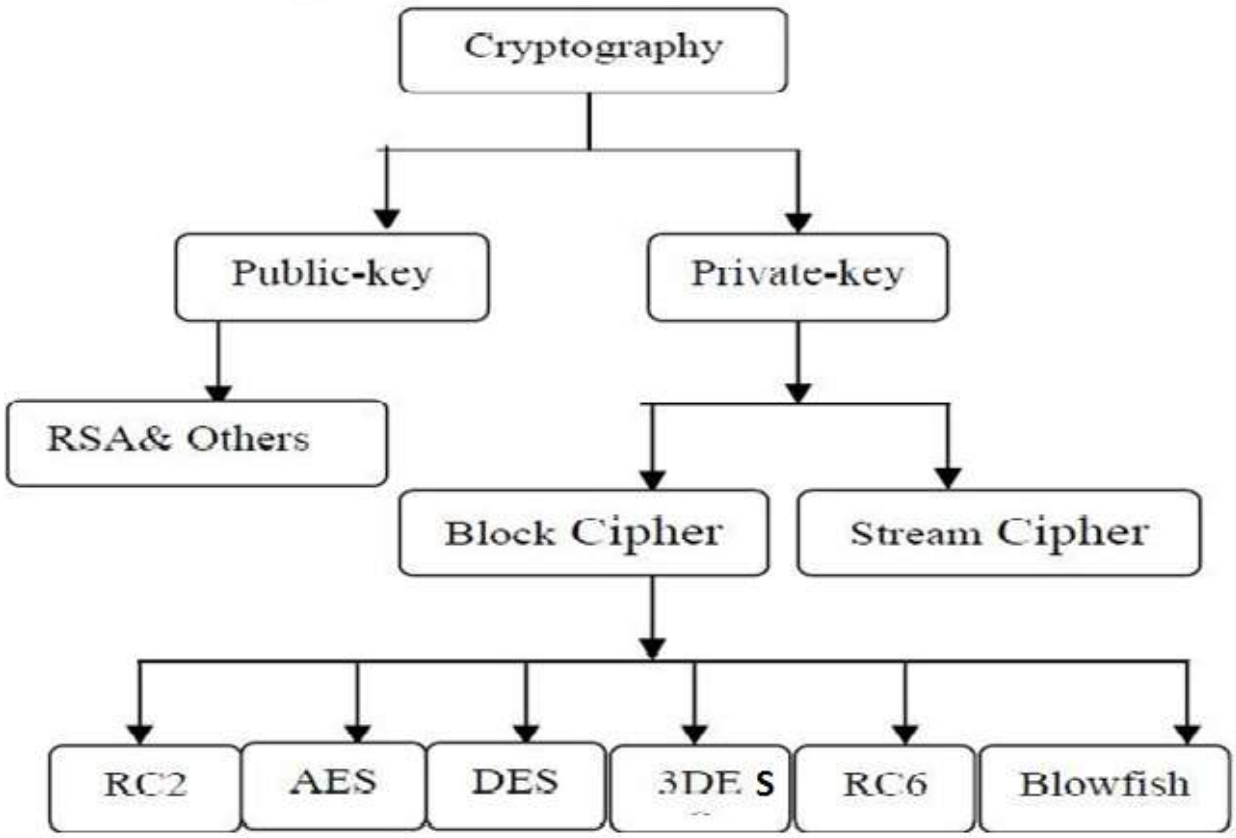

Fig.1 Types of Cryptography Algorithms [6]

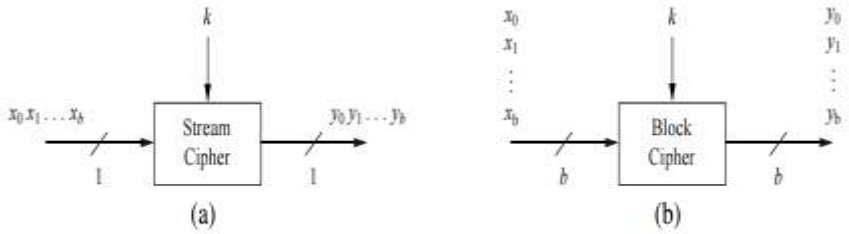

Fig. 2 Encrypting b bits with a stream (a) and a block (b) cipher

- RSA

The Rivest-Shamir-Adleman (RSA) [7] is the best known public key cryptosystem. This system is comparatively slower than many other secret key algorithms.Symmetric cryptography is split into block ciphers and stream ciphers, which are easy to distinguish.[8] Figure 2.2 depicts the operational differences between stream (Fig. 2.2a) and block (Fig. 2.2b) ciphers when we want to encrypt b bits at a time, where b is the width of the block cipher.

- RC2

RC2 is block cipher that was designed in 1989 by Ron Rivest for RSA Data Security, Inc. RC2 has many interesting and unique design features[9].

- AES

In 1997 the National Institute of Standards and Technology (NIST) initiated the selection process for the successor of DES. One of the submissions was the Rijndael cipher. It is named after its inventors Rijmenand Daemen. On November 26, 2001 this encryption scheme has been standardized as the Advanced Encryption Standard (AES) [10].

- DES and 3DES

The Data Encryption Standard (DES) has been by far the most popular block cipher for most of the last 30 years. Even though it is nowadays not considered secure against a determined attacker because the DES key space is too small, it is still used in legacy applications. Furthermore, encrypting data three times in a row with DES — a process referred to as 3DES or triple DES — yields a very secure cipher which is still widely used today [11].

- RC6

RC6 is an iterative secret-key block cipher designed by Rivest, Robshaw, Sidney, and Yin in 1998. It has variable parameters such as the key size, the block size, and the number of rounds. A particular (parameterized) RC6encryption algorithm is designated as RC6 (*w, r, b*), where *w* is the word size (one block is made of four words), *r* is the number of rounds, and *b* is the number of bytes for the secret key [12].

- BLOWFISH

Blowfish is 64-bit block cipher- used to replace DES algorithm. Ranging from 32 bits to 448 bits, variable-length key is used. Variants of 14 round or less are available in Blowfish. Blowfish is unpatented and license-free. Blowfish is one of the fastest block ciphers developed to date.

V. ADVANCED ENCRYPTION STANDARD (AES) IN DETAIL

AES is a new cryptographic algorithm that can be used to protect electronic data. Specifically, AES is an iterative, symmetric-key block cipher.

- Three block sizes are available : 128, 192, 256 bits
- Three key lengths are available (independent of selected block length) : 128, 192, 256 bits
- The number of rounds varies from 10 to 14 depending on the key length
- Each round consists of 4 functions which are in three 'layers'. The functions are listed below with the layers in the parenthesis
  - ByteStub (Non-linear layer)
  - ShiftRow (Linear mixing layer)
  - MixColumn (Non-linear layer)
  - AddRoundKey (Key addition layer)

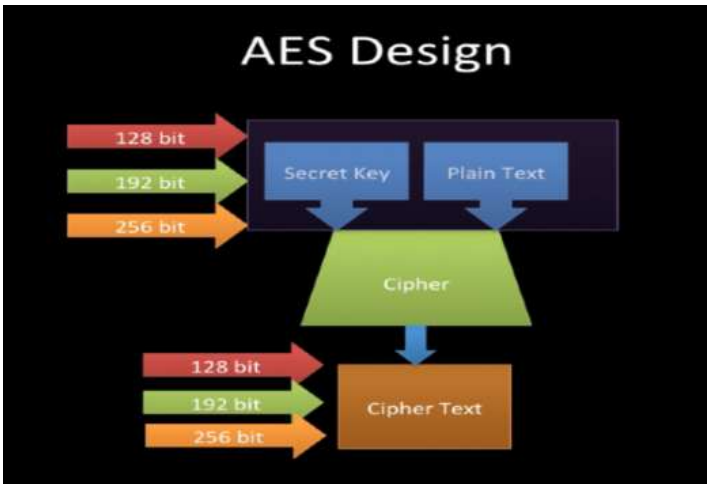

Fig. 3 AES Design

VI. AES ALGORITHM

1. Start
2. Generate a key of length 32 bits and Initialization Vector (IV) of length 16 bits.
3. Create function Encrypt.
4. Take input from the textbox of Password in the form of String.
5. Convert the string into Byte Array.
6. Convert Byte Array into ASCII Encoding.
7. Assign block size to 128 bits and key size to 256 bits.
8. Convert the key and IV generated in step 2 into Byte Array followed by ASCII Encoding.
9. Pad all the required parameters.
10. Change the mode to CBC Cipher Mode. (In CBC mode, before each plain text block is encrypted, it is combined with the cipher text of the previous block by a bitwise exclusive OR operation.)
11. Create a symmetric encryptor object with the current Key property and initialization vector (IV).
12. Transforms the whole plaintext byte array into a new array.
13. Convert the array into the string of 64 bits.
14. End

As mentioned earlier in this paper, unlike public-key ciphers, which use a pair of keys, symmetric-key ciphers use the same key to encrypt and decrypt data. Encrypted data returned by block ciphers have the same number of bits that the input data had. Iterative ciphers use a loop structure that repeatedly performs permutations and substitutions of the input data.

The Rijndael algorithm has been selected as the Advance Encryption Standard (AES) to replace 3DES. AES is modified version of Rijndael algorithm. Advance Encryption Standard evaluation criteria among others was:

- Security
- Software & Hardware performance
- Suitability in restricted-space environments
- Resistance to power analysis and other implementation attacks.

AES outperforms 3DES both in software and in hardware. AES has an advantage over other 3DES, DES and RC2 in terms of time consumption and throughput. By design AES is faster in software and works efficiently in hardware. It works fast even on small devices such as

 ISSN: 2321-8169
1529 - 1532

smart phones etc. AES provides more security due to larger block size and longer keys. AES is replacement for 3DES according to NIST both ciphers will coexist until the year2030 allowing for gradual transition to AES.

VII. IMAGES OF IMPLEMENTING AES ALGORITHM

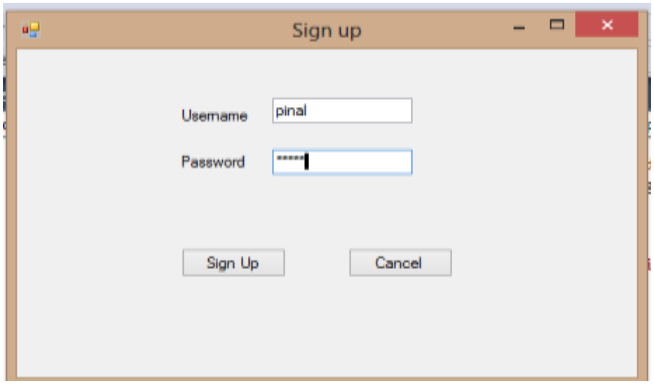

Fig.4 Sign-Up Process for New Account

Fig. 5 Signed-Up Successfully

	username character varying	password character varying
1	abc	123
2	abcd	QnjqL7Qa2lVBsxc
3	abcde	12345
4	abc	123
5	pinal	ytbVHuFmDlb13mU

Fig.6 Encrypted Password in Database

VIII. CONCLUSION

We implemented the AES password encryption algorithm as a measure of high-level security that encrypts the password and helps protect the confidential data. AES technique was adopted because of faster processing speed and better throughput. It provides excellent flexibility in choosing block and the key size which makes it difficult for the hacker to obtain the original password.

REFERENCES

[1] M., Dutreix, .Unix: administration système, AIX, HP-UX, Solaris,Linux., Citations de Ed. ENI, 2003 Ressourcesinformatiques.

[2] Rivest R., "The MD5 message-digest algorithm", RFC1321, April1992.

[3] Bellovin S.M., Merritt M., "Encrypted key exchange: password-basedprotocols secure against dictionary attacks", IEEE Computer SocietySymposium on Research in Security and Privacy, May 1992, May 1992, Page(s): 72 -84.

[4] Barry K. Shelton, "Introduction to cryptography", June 2010.

[5] Mr. Gurjeevan Singh, Mr. AshwaniSingla And Mr. K S Sandha, "Cryptography algorithm comparison for security enhancement in wireless intrusion detection system", International Journal of Multidisciplinary Research vol.1 Issue 4, August 2011, ISSN 2231 5780 .

[6] Abdul D S et al. (2008), "Performance evaluation of symmetric encryption algorithms," IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.12, December.

[7] R.L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Comm. ACM, vol. 21, pp. 120–126, 1978.

[8] Paar, Christof, Pelzl, Jan.,"Understanding cryptography: A Textbook for Students and Practitioners", 2010.

[9] Lars R. Knudsen,Vincent Rijmen,Ronald L. Rivest,Matthew J. B. Robshaw, "On the design and security of RC2", S. Vaudenay (Ed.): Fast Software Encryption – FSE'98, LNCS 1372, pp. 206–221, 1998.

[10] Johannes A. Buchmann, "Introduction to cryptography", 2000.

[11] Prof. Dr.-Ing. ChristofPaarDr.-Ing. Jan Pelzl."The Data Encryption Standard (DES) and Alternatives", 1999.

[12] Helena Handschuh"RC6", 2014.

[13] MilindMathurAndAyushKesarwani"Comparison Between DES, 3DES, RC2, RC6, BLOWFISH AND AES" in Proceedings Of National Conference On New Horizons In IT- NCNHIT 2013.