Encryption Technique for Secure Password Authentication Scheme at Application Layer

Article *in* IOSR Journal of Computer Engineering · July 2017

DOI: 10.9790/0661-1904022325

3 authors, including:

Rajesh Tyagi
Amity University
60 PUBLICATIONS **315** CITATIONS

SEE PROFILE

IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 19, Issue 4, Ver. II (Jul.-Aug. 2017), PP 23-25
www.iosrjournals.org

Encryption Technique for Secure Password Authentication Scheme at Application Layer

Poonam Pandey[1], Prof (Dr.) Rajesh Kumar Tyagi[2], Dr.R.K Bharti[3]
[1]*P.hD Scholar College of Engineering TMU Moradabad U.P, India*
[2]*Director, MSI C-4, Janakpuri New Delhi, India*
[3]*Asst. Professor, Dept CSE BTKIT Dwarahat Almora Uttarakhand India*
Corresponding Author: Poonam Pandey

Abstract: *Password security is the main issue in today's trends. Everything is based on the internet. For securing our data, files etc. we need password .Password should be secure and safe from third party and it must be safe from shoulder suffering attack, for that purpose we design an authentication scheme at application layer. To secure our password we use AES Encryption technique. This Paper shows the design of effective security issue for password by AES algorithm for encryption and decryption. It is based on AES Key Expansion in which the encryption process is a bit wise exclusive or operation of a set of strings and numbers with the 128 bit key which changes for every set of strings.*

Keywords: Authentication, AES algorithm, Encryption, Decryption

---

Date of Submission: 28-06-2017 Date of acceptance: 15-07-2017

I. Introduction

The security and integrity of data is the main concern in today's environment. In the present scenario almost all the data must be secured by password. it is vulnerable to various kinds of attacks. To make the data secure from various attacks and for the integrity of data we must encrypt the data Cryptography is a science or art of storing and transmitting data in an encryption form It is a technique of protecting information by encoding it into an another form. It is an effective way of protecting sensitive data from third party .AES is a symmetric key encryption algorithm. The algorithm was suitable across a wide range of hardware and software systems. The algorithm is relatively simple as well. Advanced Encryption Standard, also known as the Ri-jndael (pronounced as Rain Doll) algorithm is adopted worldwide.AES Algorithm is used to protect our data. The AES Algorithm needs data as input and the other thing it needs is key (encryption key). When we combined these two they are called as input and then feed into Cipher Engine which produces Encrypted data in binary format which called as cipher text. To recover the encrypted data we need to reverse the process in which the cipher text and key is feed into Cipher Engine and we get the original data. This process is called decryption AES is a symmetric block cipher that can encrypt data blocks of 128 bits using symmetric keys. There are 10, 12, 14 rounds for 128,192 and 256 bit keys. Regular rounds are 9,11and 13.Final round is 10th, 12th, 14th. Each round has certain processing involved.

II. Working Of AES Algorithm:

1. SubBytes Transformation:-It uses substitution table which includes nonlinear substitution which operate on each byte of the state.
2. ShiftRows Transformation:- In this step, bytes in each row of the state are shifted cyclically to the left. The number of places each byte is shifted differs for each row. The first row doesn't change.
3. MixColumnsTransformation:- This step operates on the column level. It is equivalent to the multi- plication of matrix at column level. Each column of the state I multiplied with fixed polynomial.
4. AddRoundKeyTransformation:-In this step, the state is combined with roundkey using XOR operation
5. Expansion Key:-In AES algorithm, the sender and receiver uses the same key they know about the key. The AES algorithm remains secure, the key cannot be determined any intruder even if he knows the plaintext and the cipher text. The AES algorithm is designed to use one of three key sizes (Nk).The keys can be 128 bits, 192 bits, 256 bits.128 bits means (16 bytes, 4 words) ,192 bits means (24 bytes, 6 words), 256 bits means (32 bytes, 8 words). These are the key sizes which are supported by AES Encryption. The larger the key the stronger is the encryption. The keys are then expanded via a key expansion routine for use in the AES cipher algorithm.

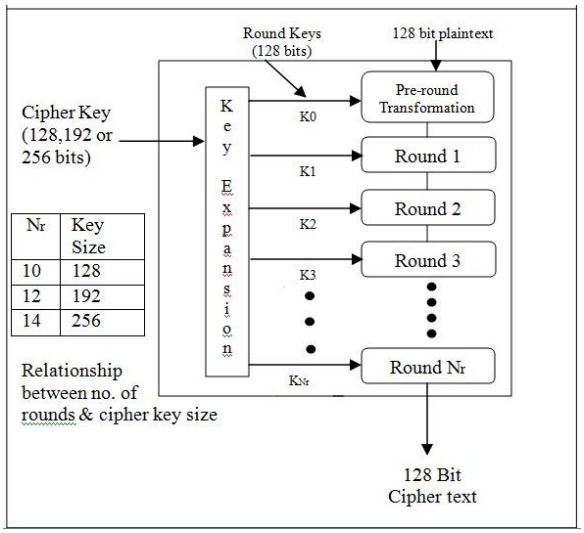

Figure: Structure of AES

III. Implementation

The AES algorithm is based on Key Expansion technique.

AES Key Expansion technique:-

AES Key Expansion is a Pseudo code for AES Key Expansion: The key-expansion routine creates round keys word by word, where every word is an array of four bytes. The algorithm creates 4x(Nr+1) words. Where Nr is the total number of rounds.

The working of algorithm is as follows:-

The first four words are made from the cipher key (initial key). The key is considered as an array of 16 bytes (k0 to k15).

The first four bytes (k0 to k3) become w0, the four bytes (k4 to k7) become w1 etc .

The rest of the words (wi for i=4 to 43) are as follows

If (i mod 4) != 0, wi = wi-1 xor wi-4. and

If (i mod 4) = 0, wi = u xor wi-4.

In the algorithm u is a temporary variable when we rotate word on wi-1 and XOR the result it gives a round constant.

Modifications in AES algorithm for key expansions:-

a) We have made some changes in the above key expansion algorithm process which improves the encryption quality. The R con value is not constant instead it is being formed from the initial key itself, this improves the avalanche effect.

b) Both the s-box and Inverse s-box are used for the Key Expansion process which improves non- linearity in the expanded key and also improves the encryption quality.

c) We do not use the S-box and Inverse S-box as such for this algorithm; instead we perform some circular shift on the boxes based on the initial key.

The following changes are made in the algorithm

1) Formation of Rcon values

Rcon[0]=key[12:15]; Rcon[1]=key[4:7];

Rcon[2]=key[0:3]; Rcon [3]=key[8:11];

2) Using Inverse S-Box for key expansion

The 'temp' value used in the algorithm is formed as

temp = SubWord(RotWord(temp)) XOR InvSubWord(Rcon[i/4]);

Where InvSubWord: InverseSubByte transformation table value

3) Shifting of S-box and Inverse S-box

Sbox _ offset = sum(key[0:15])mod256;

Inv_ Sbox _ offset = (sum(key[0:15])*mean(key[0:15]))mod256;

The initial key is represented as blocks key[0],key[1],..,key[15]. Where each block is 8bits long (8*16=128 bits).

Key Selection Procedure: The sender and receiver are agree for upon a 128 bit key. The key is used for encryption and decryption password. It is base on the symmetric key encryption technique, so they must share same key in a secure manner. The key may be represented in the blocks of k[0],k[1]...k[15]. Where each block is 8bits long (8*16=128 bits).

How to generate Multiple keys:
The sender and receiver can independently generate the keys required for the process using the changes made in the Modified AES algorithm Key Expansion technique.

Encryption
Encryption is done by the AES encryption process, where we take 16 character in each span. For both its Cipher and Inverse Cipher, the AES algorithm uses a round function that is composed of four different byte- oriented transformations: SubBytes , ShiftRows, MixColumns and AddRoundKey

Decryption
The decryption process is just opposite of encryption, and we use Inverse SubByte Transformation. Data that we get encrypted and decrypted using AES Algorithm. Improve encryption quality. AES-128 offers a sufficiently large number of possible keys, decryptio and encryption by AES Algorithm is less than the time required by DES Algorithm. the algorithm is suitable for data encryption in real time applications.

IV. Conclusion

In this paper we have use AES Technology for secure password authentication scheme at application layer. By using AES our password will be more secure than other existing technologies.

References

[1] P.Karthigaikumar, Soumiya Rasheed, Simulation of Image Encryption using AES Algorithm IJCA Special Issue on Computational Science - New Dimensions & Perspectives NCCSE, 2011, 166-172.
[2] Ahmad Salameh Abusukhon, "Block Cipher Encryption For Text-To-Image Algorithm" International journal of Computer Engineering & Technology (IJCET), Volume 4, Issue 3, 2013, pp. 50 - 59, ISSN Print: 0976 – 6367, ISSN Online: 0976 – 6375.
[3] J. V. Gorabal and Manjaiah D. H, "Image Encryption Approach for Security Issues" International Journal of Information Technology and Management Information Systems (IJITMIS), Volume 5, Issue 2, 2010, pp. 59 - 64, ISSN Print: 0976 – 6405, ISSN Online: 0976 – 6413.
[4] B.Subramanyan, Vivek.M.Chhabria, T.G.Sankar babu, Image Encryption Based on AES Key Expansion, 2011 Second International Conference on Emerging Applications of Information Technology 978-0-7695-4329-1/11 $26.00 © 2011 IEEE DOI 10.1109/EAIT.2011.60, 217- 220
[5] About AES – Advanced Encryption Standard, Copyright 2007 Svante Seleborg Axantum Software AB.
[6] Dhanya Pushkaran and Neethu Bhaskar, "AES Encryption Engine For Many Core Processor Arrays For Enhanced Security" International journal of Electronics and Communication Engineering &Technology (IJECET), Volume 5, Issue 12, 2014, pp. 106 - 111, ISSN Print: 0976- 6464, ISSN Online: 0976 –6472.
[7] Priyanka Chauhan and Girish Chandra Thakur, "Efficient Way of Image Encryption Using Generalized Weighted Fractional Fourier Transform with Double Random Phase Encoding" International Journal of Advanced Research in Engineering & Technology (IJARET), Volume 5, Issue 6, 2014, pp. 45 - 52, ISSN Print: 0976-6480, ISSN Online: 0976-6499.
[8] Prof. Maher K. Mahmood and Jinan N. Shehab, "Image Encryption and Compression Based on Compressive Sensing and Chaos" International journal of Computer Engineering & Technology (IJCET), Volume 5, Issue 1, 2014, pp. 68 - 84, ISSN Print: 0976 – 6367, ISSN Online: 0976 – 6375.
[9] M. Bellare, J. Kilian and P. Rogaway, \ The security of cipher block chaining", Advances in Cryptology { CRYPTO'94 Proceedings, Lecture Notes in Compute Science Vol. 839, Y. Desmedt, ed., Springer-Verlag, 1994. pp. 341-358.
[10] Bleichenbacher, D., \Chosen Ciphertext Attacks against Protocols Based on RSA Encryption Standard PKCS #1", Advances in Cryptology - CRYPTO'98 Proceed-ings , Lecture Notes in Computer Science Vol. 1462, H. Krawczyk, ed., Springer Verlag, 1998, pp. 1{12.

IOSR Journal of Computer Engineering (IOSR-JCE) is UGC approved Journal with Sl. No. 5019, Journal no. 49102.

Poonam Pandey. "Encryption Technique for Secure Password Authentication Scheme at Application Layer." IOSR Journal of Computer Engineering (IOSR-JCE) 19.4 (2017): 23-25.