Custom Replacement and Shifting of Encryption Key for Modified AES Algorithm

Radhika Desai
CMPN- Thakur college of engineering and technology

Kiran Bhandari
Associate Professor
CMPN- Thakur college of engineering and technology

Veena Kulkarni
Assistant Professor
CMPN- Thakur college of engineering and technology

Abstract—Today's world is moving fast towards virtualization and cloud, hence it becomes very important for the organizations to encrypt the critical data. This application provides this facility by enhancing the AES algorithm by adding custom encryption settings in the algorithm. Any known algorithm has a probability of being cracked. So hence we here proposed a configurable algorithm that allows user to modify the algorithm each time he encrypts text. The algorithm uses AES and adds some custom configurable steps in the system where user may modify the encryption process as needed. In this application more steps of encryption are added in order to make the data impossible to decipher by attackers.

Keywords- AES algorithm; Accounting information, Security, Encryption

I. INTRODUCTION

Web Applications form an integral part of our day to day life. The number of attacks on websites and the compromise of many individuals secure data are increasing at an alarming rate. With the advent of social networking and e-commerce, web security attacks such as phishing and spamming have become quite common. The consequences of these attacks are ruthless.

Hence, providing increased amount of security for the users and their data becomes essential. SQL injection can be used for unauthorized access to a database to penetrate the application illegally, modify the database or even remove it. For a hacker to modify a database, details such as field and table names are required.There are some algorithms to prevent the SQL injection attacks.

II. LITERATURE REVIEW

1. AES algorithm

AES is an encryption algorithm collected by the United States National Institute of Standards and Technology (NIST) in January 1997. The criteria made by NIST are divided into three major items to compare the candidate algorithms: (1) safety, (2) cost, (3) algorithm implementation.

The minister of the United States Department Commerce announced that the Rijndael algorithm won on October 2nd, 2000. NIST released AES standard officially in 2001 [1]. Rijndael algorithm is easy to realize with high security and strong flexibility, so it became the best option of AES.

2. The structure of AES algorithm

The Advanced Encryption Standard (AES) is a128-bit block cipher with a 128-, 192- or 256-bit secret key, called AES-128, AES-192, AES-256. AES algorithm is composed of three parts, AddRoundKey, encryption and decryption. The relationship of block length (Nb), key length (Nk) and the rounds (Nr) is shown in Table 1.

Table 1. Relationship of Nb, Nk and Nr [2]

Variant	Nb(32b)	Nk(32b)	Nr
AES-128	4	4	10
AES-192	4	6	12
AES-256	4	8	14

3. *The process of AES algorithm*

The information needed to encrypt is called plaintext. Each round function consists of SubBytes, a nonlinear 8×8 S-box byte substitution; ShiftRows, a cyclic shift of each row by different byte offsets; MixColumns, a linear combination of all 4 bytes in the same column; and AddRoundKey, an exclusive-OR (XOR) of the data block with the round key.

Each round is identical except that an extra AddRounKey is added before the first round and MixColumns is excluded from the last round [2]. As an example, Figure 1 presents a pictorial illustration of overall AES-128 encryption process, which consists of 10 such round functions.

One noteworthy feature of this structure is that it is not a Feistel structure. Recall that, in the classic Feistel structure, half of the data block is used to modify the other half of the data block and then the halves are swapped.AES instead processes the entire data block as a single matrix during each round using substitutions and permutation.

The key that is provided as input is expanded into an array of forty-four 32-bit words, w[i]. Four distinct words (128 bits) serve as a round key for each round.

Four different stages are used, one of permutation and three of substitution:

• Substitute bytes: Uses an S-box to perform a byte-by-byte substitution of the block. The forward substitute byte transformation, called SubBytes, is a simple table lookup AES defines a 16X16 matrix of byte values, called an S-box that contains a permutation of all possible 256 8-bit values.

• ShiftRows: A simple permutation. The **forward shift row transformation**, called ShiftRows. The first row of **State** is not altered. For the second row, a 1-byte circular left shift is performed. For the third row, a 2-byte circular left shift is performed. For the fourth row, a 3-byte circular left shift is performed

•MixColumns: The forward mix column transformation, called MixColumns, operates on each column individually. Each byte of a column is mapped into a new value that is a function of all four bytes in that column.

• AddRoundKey: A simple bitwise XOR of the current block with a portionof the expanded key. In the forward add round key transformation, called AddRoundKey, the 128 bits of State are bitwise XORed with the 128 bits of the round key. The operation is viewed as a columnwise operation between the 4 bytes of a **State** column and one word of the round key; it can also be viewed as a byte-level operation.

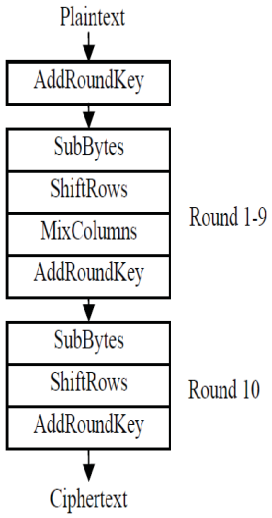

Figure1: The encrypt process of AES-128 [2]

The structure is quite simple. For both encryption and decryption, the cipher begins with an AddRoundKey stage, followed by nine rounds that each includes all four stages, followed by a tenth round of

three stages. Only the AddRoundKey stage makes use of the key. For this reason, the cipher begins and ends with an AddRoundKey stage.

Any other stage, applied at the beginning or end, is reversible without knowledge of the key and so would add no security. The AddRoundKey stage is, in effect, a form of Vernam cipher and by itself would not be formidable. The other three stages together provide confusion, diffusion, and nonlinearity, but by themselves would provide no security because they do not use the key.We can view the cipher as alternating operations of XOR encryption (AddRoundKey) of a block, followed by scrambling of the block (the other three stages), followed by XOR encryption, and so on.This scheme is both efficient and highly secure. Each stage is easily reversible.

For the Substitute Byte, ShiftRows, and MixColumns stages, an inverse function is used in the decryption algorithm. For the AddRoundKey stage, the inverse is achieved by XORing the same round key to the block. With most block ciphers, the decryption algorithm makes use of the expanded key in reverse order. However, the decryption algorithm is not identical to the encryption algorithm.

This is a consequence of the particular structure of AES. Once it is established that all four stages are reversible, it is easy to verify that decryption does recover the plaintext. Figure 1, lays out encryption process. The final round of both encryption and decryption consists of only three stages. Again, this is a consequence of the particular structure of AES and is required to make the cipher reversible.[2]

III. PROPOSED SYSTEM

Today's world is moving fast towards virtualization and cloud, hence it becomes very important for the organizations to encrypt the critical data. This application provides this facility by enhancing the AES algorithm by adding custom encryption settings in the algorithm. Any known algorithm has a probability of being cracked. So hence we here propose a configurable algorithm that allows user to modify the algorithm each time he encrypts text.

-Encryption

- Custom Replacement- As shown in Figure2, in this step the user can select the alphabets with which it wants the alphabets of the plain text to be replaced with. This increases the security as the user gives a unique replacement every time. This replacement is used during registering and login. Every user gives a unique replacement of the password. For eg: password is abcd and the user replaces a with @ sign. So, this replacement is done only for this user particularly. Now, when a different user registers, one will not use the same replacement for the password.
- Shift/ reverse Key- The key that user provides will be added to the left or right and shifting will be done accordingly. For eg: If the user wants a key like 1234abc to be added and shifted accordingly, the algorithm will provide the adding and shifting. The shifting is also customizable. It can be right or left, as specified by the user everytime during registration.
- Replace- In this step the alphabets of the original plain text is replaced by some other alphabet or character in the replacement table and this replacement table is modifiable by the user as desired.
- AES- After replacement, the shifting is done to right or left. Then, using this key AES encryption is done and then sent to the next step for further addition of bits.
- Add Padding Bits- After the AES encryption, some padding bits are added either to the left or right of the encrypted data to get the final encrypted text. The padding bits as well as their addition positions in the cipher text is decided by the user.

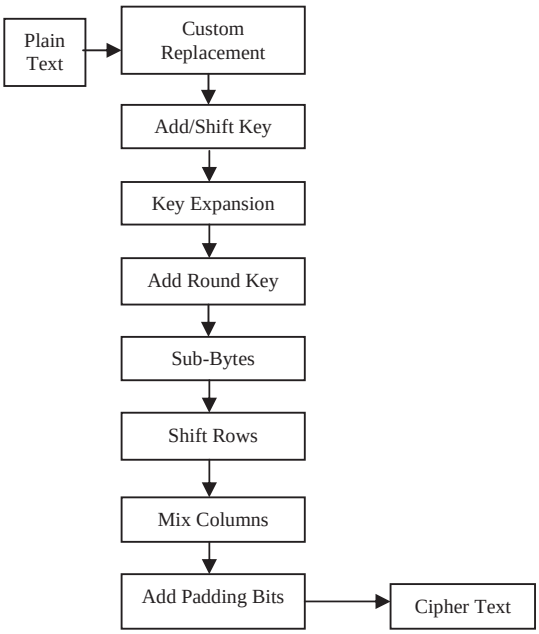

Figure 2: Encryption using proposed system.

Decryption

- Remove Padding Bits- As shown in Figure 3, in this step the padding bits are removed from the cipher text.
- AES Decryption- After the padding bits are removed, the data is decrypted. AES algorithm is used for decryption.
- Shift/ reverse Key- The key will be removed from left or right as specified by the user. The bits are removed and sent to the next step.
- Custom replacement- Once the padding bits are removed, the alphabets are replaced by the corresponding alphabets stored in the user modifiable replacement table. For eg: If the user has replaced a with @, this replacement will be reversed while decryption.

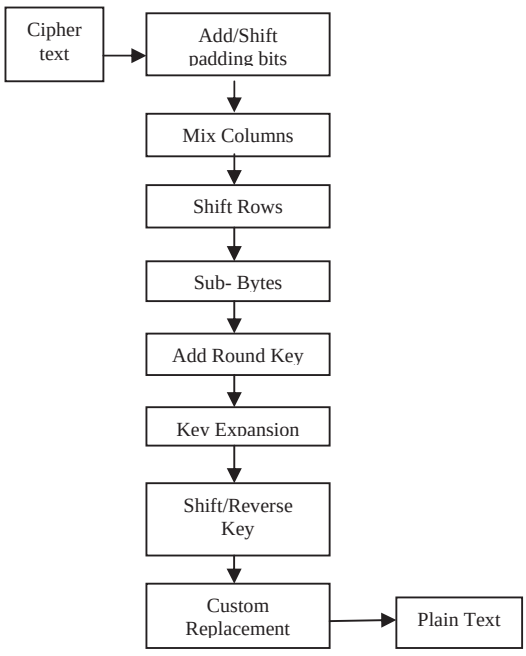

Figure 3: Decryption using proposed system.

IV. ADVANTAGES

- This application makes it difficult to crack the cipher text as the key is only known to the sender and receiver of the message.
- The plain text is also encrypted using AES encryption which makes it more secure and encryption is done faster.
- The original plain text is first replaced with some random characters, the AES encryption is performed on replaced text. Padding bits are then added to this encrypted text. Thus, the cipher text becomes impossible to crack.

V. APPLICATION

This application is very beneficial for sending critical messages over the network as this custom algorithm includes replacement, AES encryption, and padding of extra bits which makes the messages more secure.

VI. CONCLUSION

The proposed system allows user to modify the encryption algorithm each time the encryption is done. So even if the attacker knows the algorithm and the encryption key still it would not be possible to decrypt the cipher text because user may use custom configurations each time while encrypting the text.

REFERENCES

[1] NIST, "Federal Information Processing Standards Publieation197". 2001.

[2] Qing-xiang zhu1, lu li1, jing liu2, nan xu1 "The Analysis And Design Of Accounting Information Security System Based On AES Algorithm" *Proceedings of the Eighth International Conference on Machine Learning and Cybernetics, Baoding*, 12-15 July 2009

[3] Y. Huang, S. Huang, T. Lin, and C. Tsai."A Testing Framework for Web Application Security Assessment" *Journal of Computer Networks*, Volume: 48 Issue: 5, Pp:739-761, 2005.

[4] Amandeep kaur1, Mrs. Shailja Kumari , **"**Secure Database Encryption in Web Applications**"** *International Journal of Advanced Research in Computer and Communication Engineering* Vol. 3, Issue 7, July 2014.

[5] L. Liu, J. Gai," A new lightweight database encryption scheme transparent to applications", *Proceedings of the 6th IEEE International Conference on Industrial Informatics*, 2008.