isrjournals

International Journal of Advanced Research in Computer Science Engineering and Information Technology

Volume: 6, Issue: 3,Special Issue: 1 ,Mar,2021 ,ISSN_NO: 2321-3337

Encryption and Decryption Of Unified Payment Interface Using Generation Of Multiple Random S-Box With AES Algorithm

Dr. M. Navaneethakrishnan M.E., Ph.D., Professor of Computer Science Department,
Miss. D. Pamila, Student of Computer Science Department,
Miss. M. Mahalakshmi, Student of Computer Science Department,
Miss. B. Praisy, Student of Computer Science Department,
St. Joseph College of Engineering, Sriperumbudur, Chennai

Abstract

Cryptography is the use of codes and ciphers to protect secrets. AES is used to provide more security also used to prevent attacks. Security is a major problem in recent year. Several researchers for doing their research in information security domain to improve their security through their information sharing. Modern cryptography is achieved by algorithms that have key to encrypt and decrypt information.

This keys convert messages and data into digital gibberish through encryption. In general longer key is, more difficult to Crack the code. In this paper we use AES algorithm to encrypt financial related data as AES uses higher length key sizes.

Key Terms: AES 256 bit key, cipher key, MR S – Box multiple random s – box.

1. Introduction

The aim of our project is to provide security four UPI PIN. Now a days, for maintaining authentication, authorization, integrity of data and security is big challenges for all of us. In general longer key code. So, we have used AES 256 bit key for encryption process.

2. Literature Survey

Process of password transmission encryption using AES 256 and RSA algorithm. Two keys are included. Main key and working key. Main key is responsible for working key. Working

key is responsible for password encryption. This paper improved the AES password transmission encryption process, adopted the method of password adding random number as a key to encrypted password. On this basis in the paper introduced RSA transmission encryption process.

Cloud storage reliability, strong protection and low cost. In data privacy, there is no traditional technical of authentication because une xpected privileges will expose all data. As a result, the delegation can always get an aggregate key of constant Size. This aggregate key can be sent to the others for decryption if ciphertext set are remains confidential.

File encrypting tools like Veracrypt, Axcrypt, Boxcrypt, are place to encrypt files. But they have implemented AES and RSA encryption algorithm. Files are stored in cloud storage systems in plaintext format. Again multiple copies of the files are maintained in multiple locations for faster access and availability. Files are stored in cloud storage systems in plaintext format.

3. System Design

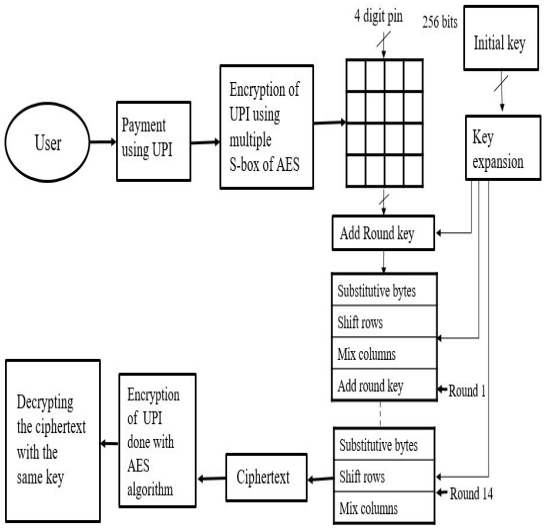
256 Bit encryption is much stronger than 128 bits key. Using AES with 256-bit keys enhances the number of AES rounds that needs to be done for each data block. Multiple Random s-boxes are generated. So, Hackers couldn't find where the data is placed. When user purchases the product from admin's Web page, the user will enter UPI pin and ID. This will be encrypted using AES algorithm and will be stored in payment gateways database. Particularly we focused on how the encryption is done using multiple random s- boxes for providing strong security rather than using single s-box.

Architecture diagram shows the relationship between different components of the system. This diagram is very important to understand the overall concept of the system. They are heavily used in the engineering world in hardware design, electronic design, and software design and process flow diagram.

isrjournals

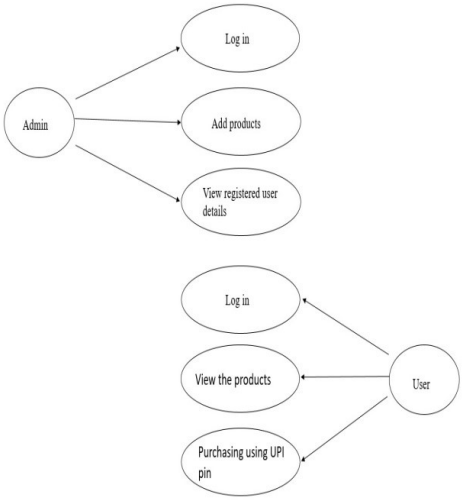
International Journal of Advanced Research in Computer Science Engineering and Information Technology

Volume: 6, Issue: 3,Special Issue: 1 ,Mar,2021 ,ISSN_NO: 2321-3337



Four keys are given to each round in terms of words. Fourteen rounds are performed for AES 256 algorithm in fourteenth round the final cipher text is obtained. This is the encrypted form of UPI PIN if we want to decrypt.

If the PIN and ID is matched then it will show valid credentials otherwise it will show invalid credentials.



When user enters the UPI PIN and ID it will be encrypted and will be stored in payment gateways database. When user again enters the UPI PIN and ID it will decrypt the data.

4. Implementation

AES is a symmetric encryption algorithm. AES was designed to be efficient in both hardware and software, and supports a block length of 128 bits and key lengths of 128, 192 and 256 bits.

STEP 1

Input : 4-digit pin and key.

Output: cipher text.

Method:

Initial key is added to 4 digit pin before the round function begins.

Add round key:

4 digit pin + initial key = 4×4 cypher text

STEP 2

SUBSTITUDE BYTES:

Input : 4×4 cipher text.

Output : 4×4 ciphertext from S-box.

Method:

Step 1: Using 16×16 S-box each element in the matrix is mapped to corresponding byte.

STEP 3

SHIFT ROWS

Input : 4×4 ciphertext from substitute bytes.

Output : 4×4 ciphertext from shift rows.

Method:

Step 1: Row 0 – Shift left 0 byte

Step 2: Row 1 – Shift left 1 bytes

Step 3: Row 2 – Shift left 2 bytes

Step 4: Row 3 – Shift left 3 bytes

STEP 4

MIX COLUMNS

Input : 4×4 ciphertext shift rows.

Output : 4×4 ciphertext from mix columns.

Method:

Step 1 – A predefined matrix is used.

Step 2 – Each column in the matrix is multiplied by predefined matrix to get a new column.

STEP 5

ADD ROUND KEY

Input : 4×4 cipher text from predefined matrix, key.

Output: 4×4 cipher text from add round key.

METHOD:

Step 1: 4×4 ciphertext + Add round key = 4×4 ciphertext.

Step 2: This cyphertext is given to next round.

Generate Multiple Random S-Box Algorithm

Void generate multiple random s-box (byte [32] key)

{

Byte rindex, cindex;

Byte SC = get shift count (key);

Byte s-box = generate primary s-box();

For(int i=0;i<32;i++);

{

Get proper index (key[i], out rindex, outcindex); x

```
    Shift row (rindex, SC, s-box);
    Shift column (cindex, SC, s-box);
        Swap (rindex, cindex, s-box);
}
}
```

Conclusion and Future Enhancement

In our paper, we focused to provide security for UPI PIN. We have generated one algorithm for this process. Multiple random s-box algorithms are generated. To applying this algorithm for encryption process enables hackers could not find where the data is placed. This multiple random s-box is enhanced is future as a dynamic multiple random s-box. Where multiple random s-boxes are changed automatically.

References

[1] K. Tiri et al., "Prototype IC with WDDL and differential routing-DPA resistance assessment," in Cryptographic Hardware and Embedded systems. Berlin, Germany: Springer- Verlag, 2005, pp. 354-365.

[2] A. Moradi, A. Poschmann, S. Ling, C. Paar, and H. Wang, "Pushing the limits: A very compact and a threshold implementation of AES,"in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2011, pp, 69-88.

[3] F. -X. Standard, O. Pereira, Y. Yu, J,-J. Quisquater, M. Yung, and E. Oswald, "Leakage resilient cryptography in practice," in Towards Hardware - Intrinsic Security. Berlin, Germany: Springer-Verlag, 2010, pp, 99-134.

[4] Y. Dodis and K. Pietrzak, "Leakage resilient pseudorandom functions and side-channel attacks on Feistel networks," in Proc. 30th CRYPTO, 2010, pp, 21-40.

[5] S. Faust, K. Pietrzak, and J. Schipper, "Practical leakage-resilient symmetric Cryptographic Hardware and Embedded Systems. Berlin, Germany: Springer-Verlag, 2012, pp, 213-232.