The Implementation of Anti-attack AES Mathematical Model in Library Network Encryption

Yufen Shen
North University
Yanji, 133400, China
yfshen678@126.com

***Abstract*—With the continuous improvement of university library network safety requirements, this paper studies encryption and decryption algorithm analyzing advanced encryption standard AES of the computer, substitution and replacement operation in encryption and decryption process, and key expansion mathematical model. The detailed design of the mathematical modeling process of the algorithm is given, and the whole mathematical modeling process is more thoroughly analyzed. According to the model, library network encryption application is completed. Verified by computer simulation technology, the mathematical model has a good robustness and achieved good results.**

Keywords-AES mathematical model; Library network; Mathematical modeling

I. INTRODUCTION

With the development of computer network, the library service mode continuously develops and completes towards networking. Information resources' electronization and digitization have become main transmission modes. Library business management and literature information service become more and more dependent in the network. But the network resource share increases the network vulnerability and the possibility of network attack. Library network security management is more and more important. Therefore, to guarantee the efficient operation of network security becomes an urgent problem in library informatization and network construction. Currently, AES algorithm is the most secure encryption algorithm available. Based on theory and time, the only effective way to break the algorithm is to force the generation of all possible keys, which will take years in today's fastest system [1 ~ 2]. In our country, with library informatization construction development, library information network construction has become an important national infrastructure. University library network has received high attention of the country. But because China's library informatization construction foundation is weak and starts later, the main security products and technology mainly rely on import at present. Independent technology development is slow, and there are considerable hidden troubles. So it is of great significance to our country's library information security construction that AES algorithm should be studied to form our library network encryption. In this paper, the mathematical modeling of encryption process is carried out and lays the foundation for further study [3 ~ 4].

II. THE ESTABLISHMENT OF THE MATHEMATICAL MODEL IN AES ENCRYPTION ALGORITHM

1) AES algorithm sets each input and output for 128 bits, known as block or group, the number of bits in which is called block length. AES algorithm's password keys are 128 bits, 192 bits or 256 bits. Other input, output and password key length are not allowed in this algorithm.

2) The basic unit of AES algorithm is byte, an 8 bits sequence is seen as a single processing entity. The input, output and password key bit sequence are processed as a byte array. While forming a byte array, per eight adjacent bits in the sequence are divided into a group, constituting a byte. When an input, output or password key is denoted as character a, then the byte array got can be expressed as an or a [n], in which n's range is:

Key length = 128 bits, $0 \leqslant n < 16$; Packet length = 128 bits, $0 \leqslant n < 16$;

Key length = 192 bits, $0 \leqslant n < 24$;

Key length = 256 bits, $0 \leqslant n < 32$;

3)AES algorithm operations are done in the state, and the state is the intermediate result in AES encryption and decryption process. State is composed of four lines of bytes, and each line contains a Nb byte. Nb is equal to block length divided by 32. In AES standard, Nb = 4, State [] denotes state array, and each byte has two pointers: one is its line number r（$0 \leqslant r < 4$）, the other is its column number c（$0 \leqslant c < Nb$）. each byte of the state can be expressed as State [r, c] or Stater，c. 4 bytes in each column of the state array constitute a 32 bit word, that is to say, state is one dimensional array consisting of 32 bit word (column).

4) To AES algorithm, input group, output group and the total length of the state are all 128 bits which are denoted by Nb = 4. Nb value reflects the number of 32 bit word(that is, the number of columns) in the state. The length of the key is denoted by Nk = 4, 6 or 8. Nk's numerical value reflects the number of 32 bit word in password key (that is, the number of columns). Cycle times during the algorithm implementation depend on the size of the key. Cycle times is denoted by Nr, when Nk = 4, Nr = 10; When Nk = 6, Nr = 12; When Nk = 8, Nr = 14. ShiftRows is a substitution operation which conducts cyclic shift to the last 3 line byte

Published by Atlantis Press, Paris, France.

according to different byte offset number, and the first line r = 0 doesn't shift. Other ShiftRows' expression is as follows:

s′r，c= sr，(shift(r,Nb)+c)mod Nb,0＜r＜4 and 0≤c＜Nb

In it, the shift value shift (r, Nb) depends on line number r, such as (Nb = 4), shift (1, 4) = 1; Shift (2, 4) = 2;Shift (3, 4) = 3. Figure 2-3 shows ShiftRows operation.

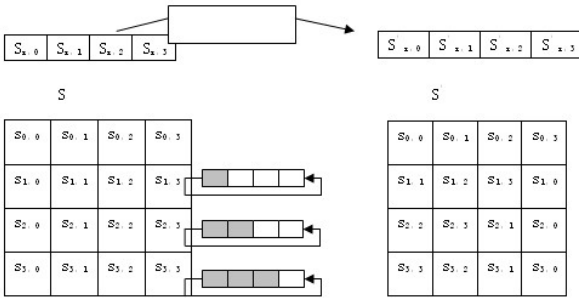

Figure 1. ShiftRows operation

Status before ShiftRows

d4	e0	b8	1e
27	bf	b4	41
11	98	5d	52
ae	f1	e5	30

Status after ShiftRows

d4	e0	b8	1e
bf	b4	41	27
5d	52	11	98
30	ae	f1	e5

Figure 2. ShiftRows () case

III. MATHEMATICAL MODEL OF MIXCOLUMNS

MixColumns perform operations to the state column by column. Each column is processed according to four polynomials. Column is considered to be the polynomial in GF (28) domain, and multiplies the fixed polynomial a (x) given below[10] :

$A(x)=\{03\}x^3+\{01\}x^2+\{01\}x+\{02\}$

This formula can be written as matrix multiplication. Suppose s' (x) = a (x) • b(x),

$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 02\ 03\ 01\ 01 \\ 01\ 02\ 03\ 01 \\ 01\ 01\ 02\ 03 \\ 03\ 01\ 01\ 02 \end{bmatrix} \times \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix}$$

As the result of multiplication, four bytes in one column can be expressed as:

$S'_{0,c}=(\{02\}\cdot S_{0,c}) \oplus (\{03\}\cdot S_{1,c}) \oplus S_{2,c} \oplus S_{3,c}$

$S'_{1,c}= S_{0,c} \oplus (\{02\}\cdot S_{1,c}) \oplus (\{03\}\cdot S_{2,c}) \oplus S_{3,c}$

$S'_{2,c}= S_{0,c} \oplus S_{1,c} \oplus (\{02\}\cdot S_{2,c}) \oplus (\{03\}\cdot S_{3,c})$

$S'_{3,c}= (\{03\}\cdot S_{0,c}) \oplus S_{1,c} \oplus S_{2,c} \oplus (\{02\}\cdot S_{3,c})$

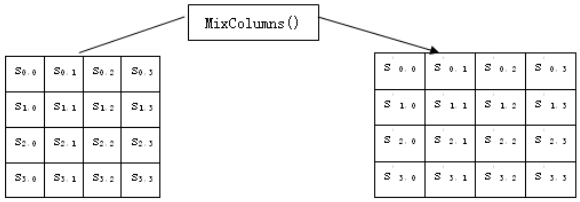

Figure 3. Independent MixColumns operation of each column bytes in the state

Status before ShiftRows

d4	e0	b8	1e
27	bf	b4	41
11	98	5d	52
ae	f1	e5	30

Status after ShiftRows

04	e0	48	28
66	cd	f8	06
81	19	d3	26
e5	9a	7a	4c

Figure 4. MixColumns() case

Figure 3 shows MixColumns' operation process. Figure 4 gives an MixColumns () transformation case.

IV. MATHEMATICAL MODELING OF DECODING

Reverse ShiftRows is reverse transformation of ShiftRows, which conducts cyclic shift to the last 3 line byte according to different byte offset number. The first line r = 0 doesn't shift. 3 lines below respectively cyclic shift Nb - shift (r, Nb) bytes, in which shift (r, Nb)'s shift value depends on the number of lines, such as: shift (1, 4) = 1; Shift (2, 4) = 2;Shift (3, 4) = 3.

Reverse ShiftRows expression is as follows:

$s'_{r,(c+\text{shift}(r,Nb))\bmod Nb} = s_{r,c}, 0＜r＜4$ and $0≤c＜Nb$

Figure 5 shows ShiftRows operation.

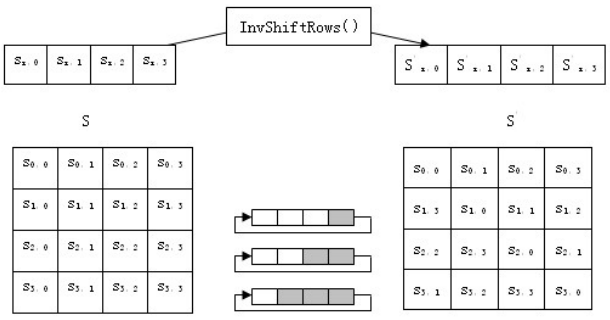

Figure 5. Reverse ShiftRows operation

V. EXPERIMENTS AND RESULTS

This paper takes a university library network file encryption as an experimental object to test the algorithm. The process is as follows:

A. The file encryption design

File encryption operation: first, click the "browse" button, and call OnBFile () function. Define an object of the

CFileDialog type in the function (CFileDialog class is to open and save a universal Windows' file operations dialog box). Choose encrypt files from "open dialog box"; then click "file encryption" button and call OnBFileEn () function. The function defines the pointer to the file for reading and writing files, and use file operation function to get the length of the file. According to the radio button value (namely key length value), define a Aes class object and call the corresponding encryption function. Thus a file's encryption operation is implemented.

Figure 6 is the contents of encrypted a.txt.en file.

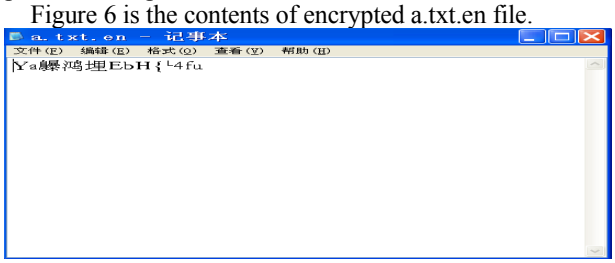

Figure 6. Contents of encrypted file.

B. *File decryption design*

For file decryption, the files in edit box (IDC_EFile) can be directly decrypted, or click the "browse button " and choose the files to be decrypted. Then click "file decryption" button, and call OnBFileDe () function. The function defines the pointer to the file and call fopen, fseek, ftell, fread and fwrite file operation function to open files, change files' location pointer, get file length, read files and write files. Finally call the corresponding decryption function according to the radio button value (key length value).

Documents after decryption are distinguished with suffix.en.de.

Documents after decryption are a.txt.en.de, Figure 7 is the contents of a.txt.en.de, the same contents of a.txt.

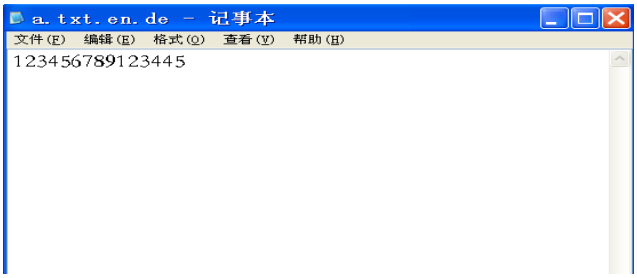

Figure 7. Contents of a.txt.en.de

VI. CONCLUSION

This paper studies encryption and decryption algorithm analyzing advanced encryption standard AES, substitution and replacement operation in encryption and decryption process, and key expansion mathematical model. The detailed design of the mathematical modeling process of the algorithm is given, and the whole mathematical modeling process is more thoroughly analyzed. Verified by computer simulation technology, the mathematical model has a good robustness and achieved good results.

REFERENCES

[1] Deng Kebo,liu zhong Energy-Efficient Area Coverage in Wireless Sensor Networks with Adjustable Sensing Ranges[J].Journal of Electronics& Information Technology 2009.31(10):2305-2309

[2] M A Fischler, R C Bolles. Random sample consensus: a paradigm for model fitting with applications to image analysis and automated cartography[J]. Communication of ACM, 1981,24(6): 381-395.

[3] Chi H P, Lin R L, Chen J F. Simplified flux linkage model for switched reluctance motors[J]. IEE Proceedings of Electrical Power Application, 2005, 152(3): 577-583.

[4] Soares F, Costa Branco P J. Simulation of a 6/4 switched reluctance motor based on Matlab/Simulink environment[J]. IEEE Transactions on Aerospace and Electronic Systems, 2001, 37(3): 989-1007