Modified ShiftRow AES with RoundKey

David Setyanugraha(13511003)
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
Jl. Ganesha 10 Bandung 40132, Indonesia
13511003@std.stei.itb.ac.id

Akbar Suryowibowo (13511048)
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
Jl. Ganesha 10 Bandung 40132, Indonesia
13511048@std.stei.itb.ac.id

***Abstract*—This paper present a new encryption scheme as a modification of Advanced Encryption Standard (AES) Algorithm. Advanced Encryption Standard (AES) is symmetric-key block cipher algorithm which now used worldwide. Many kinds of attack have been used to cryptanalysis the AES algorithm. Security is an important aspect of AES algorithm. On that basis, we propose a new modification on AES. The modification is done by utilizing the usage of round key to adjust ShiftRow transformation. Detailed results in terms of security analysis and implementation are given. Experimental results verify and prove that AES modification gives better encryption results in terms of security.**

Keywords: Advanced Encryption Standard (AES), Block Cipher, ShiftRow Transformation.

I. INTRODUCTION

In cryptography, a block chiper is a method of encrypting text on fixed-length groups of bits in which cryptographic key and algorithm are applied to block of data [9]. The modern design of block chipers is based on the concept of an iterated product cipher. [5] Iterated product cipher utilizes the encryption in multiple rounds. Example implementation of this block cipher is called Feistal Network. [4] A block cipher consists of two paired algorithms, encryption and decryption. Encryption is the conversion of electronic data into another form, called ciphertext which cannot be easily understood by anyone except authorized parties. Decryption is the reverse operation of encryption. The decryption of data encrypted with symmetric algorithms is similar to the process used to encrypt data with symmetric algorithms. Many realizations of block ciphers (such as the AES) are classified as substitution-permutation networks. Substitution-permutation networks utilize the usage of Substitution Box and Permutation Box to produce each block of ciphertext output. [11] In 2013, reports show that there is possibility that AES can be broke into. It is the reason why we need new modified AES.

II. AES ALGORITHM

Advanced Encryption Standard (AES) is symmetric block chiper used by the U.S. government to protect classified information and is implemented in software and hardware. [6] The AES algorithm is based on permutations and substitutions. AES algorithm (also called Rijndael) is developed by Joan Daemen and Vincent Rijmen. AES is the winner of Encryption competition standard held by National Institute of Standard and Technology (NIST). Rijndael algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits [2]. Many papers have been published on cryptanalysis of AES. In 2013, Attack have been published that are computationally faster than a full brute force attack and it's proved computationally feasible [3].

The AES algorithm is divided into four different phases, which are executed in a sequential way forming rounds. [8] The encryption is achieved by passing the plaintext into initial round, 9 equal rounds and a final round. The algorithm operates on a state consists of 4x4 array of bytes. The high level description of AES consist of SubBytes, ShiftRows, MixColumns, AddRoundKey.[3] Figure 1 shows the step of AES which is adopted by an animation.

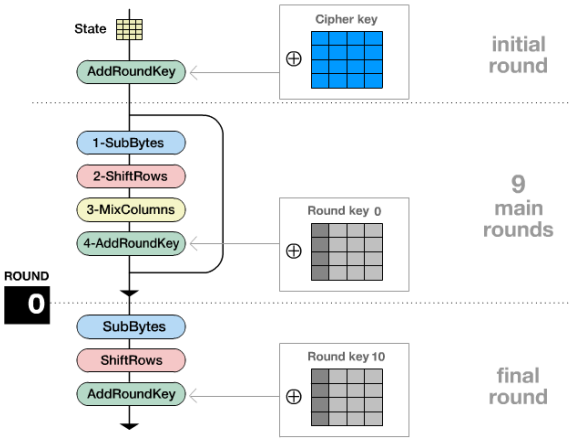

Figure 1 Illustration of Rijndael Animation [4]

A. SubBytes Transformation

In SubBytes Transformation, a substitution table (s-box) is used to construct the chiper text. S-box is constructed by multiplicative inverse and affine transformation.

B. ShiftRows Transformation

In the ShiftRow transformation, the bytes in the last three rows of the State are cyclically shifted over 1, 2 and 3 bytes, respectively. The first row is not shifted. The offset of the left shift only varies from one to three bytes.

C. MixColumns Transformation

MixColumns Transformation takes four bytes of each column of the state combined using an invertible linear transformation. Each column will be multiplied by a fixed matrix which is composed by multiplication and addition of the entries. These MixColumns provided diffusion in the cipher.

D. AddRoundKey Transformation

AddRoundKey Transformations combines the subkey with the roundkey using XOR operation. This key is generated in every round.

Some works have been done before in order to make AES become better encryption algorithm. Luminiţa and Mircea-Daniel (2012) proposed modified AES which work on data matrices with exactly 8 rows and a variable number of columns: 6,8,12 and 16. They made this modified AES algorithm based on knowledge that to increase the robustness of the AES algorithm, by using longer encryption keys and larger data matrix.[7] Vandana C. Koradia (2013) also proposed new modified AES. In order to overcome the problem of high calculation, they skip the Mixcolumn step and add the permutation.[12] The most similar researchs to our work came from Seyed Hossein Kamali and Reza Shakerian (2010). They also modified the AES by adjusting ShiftRow Transformation. However, they validate their new modified AES on image encryptions. [10]

III. Proposed AES Algorithm

According to Claude Shannon, good encryption algorithm must provide two properties of operation: Confusion and Diffusion. We proposed the new AES Algorithm in the term of ShiftRow function. In original ShiftRow algorithm, the byte shift is done depends on the row of the blocks. The weakness of this ShiftRow function is in the same pattern of shiftRow. This made easy for the cryptonalysists to break into this algorithm. We modified ShiftRow function by using XOR operation done between every byte in each row of round key. Every row of cipher key will have different kind of shifting depends on the roundkey generated in every round. This increases the complexity of ShiftRow transformation.

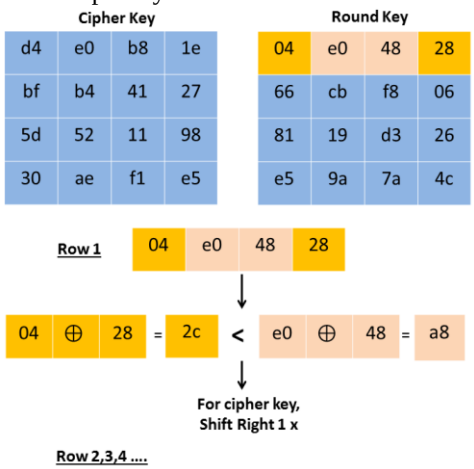

Figure 2. Illustration of ShiftRows function in AES

The pseudocode for the proposed ShiftRows is as follows:

```
procedure modifiedShiftRows(byte[][] state,
byte[][] roundkey) {
        for (every row in roundkey) {
                a : roundkey[1][row];
                b : roundkey[2][row];
                c : roundkey[3][row];
                d : roundkey[4][row];
                if ((a ^ d]) > (b ^ c)) {
                        shiftRight(state,row);
                }
                else if ((a ^ d]) < (b ^ c)) {
                        shiftLeft(state,row);
                }
                else {
                        shiftDouble(state,row);
                }
        }
}
```

Our proposed AES algorithm can be implemented in many programming languages. In this experiment, we implement our new shift row AES algorithm in Java programming languange. Here we provide some changes for our proposed AES algorithm to support encryption and decryption process:

ShiftRow Algorithms (Encryption)

```
private static byte[][] ShiftRows(byte[][] state, byte[][] w, int
round) {
    byte[] t = new byte[4];
    for (int i = 0; i < 4; i++) {
        byte a,b,c,d;
        a = w[round * Nb + 0][i];
        b = w[round * Nb + 1][i];
        c = w[round * Nb + 2][i];
        d = w[round * Nb + 3][i];

        if ((a ^ d) > (b ^ c)) {
            for (int c1 = 0; c1 < Nb; c1++) {
                t[c1] = state[i][(c1 + 1) % Nb];
            }
        }
        else if ((a ^ d) < (b ^ c)) {
            for (int c1 = 0; c1 < Nb; c1++) {
                int z = c1-1;
                if (z < 0) z+=Nb;
                t[c1] = state[i][z % Nb];
            }
        }
        else {
            for (int c1 = 0; c1 < Nb; c1++) {
                t[c1] = state[i][(c1 + 2) % Nb];
            }
        }

        for (int c1 = 0; c1 < Nb; c1++)
            state[i][c1] = t[c1];
    }
    return state;
}
```

InvShiftRow Algorithms (Decryption)

```
private static byte[][] InvShiftRows(byte[][] state, byte[][] w,
int round) {
        byte[] t = new byte[4];
        for (int i = 0; i < 4; i++) {
        byte a,b,c,d;
        a = w[round * Nb + 0][i];
        b = w[round * Nb + 1][i];
        c = w[round * Nb + 2][i];
        d = w[round * Nb + 3][i];
        if ((a ^ d) > (b ^ c)) {
           for (int c1 = 0; c1 < Nb; c1++) {
              t[(c1 + 1) % Nb] = state[i][c1];
           }
         }
         else if ((a ^ d) < (b ^ c)) {
               for (int c1 = 0; c1 < Nb; c1++) {
                    int z = c1-1;
                    if (z < 0) z+=Nb;
                    t[z % Nb] = state[i][c1];
               }
        }
        else {
              for (int c1 = 0; c1 < Nb; c1++) {
                    t[(c1 + 2) % Nb] = state[i][c1];
              }
        }

        for (int c1 = 0; c1 < Nb; c1++)
             state[i][c1] = t[c1];
        }
        return state;
}
```

IV. Experiment and Results

We conduct the experiment on three kinds of text (Short size, medium size and large size). We assume that the key length of 128 bits, which is commonly implemented. Every text is also decrypted successfully. The results of encryption from modified AES can be seen as follows:

Plain Text	Encryption Results
Short size text Before the modern era	e43f 0bdb 7b49 7334 ad3f aa31
Medium size text Before the modern era, cryptography was concerned solely with message confidentiality (i.e., encryption)-conversion of messages fro m a comprehensible form into an incomprehensib le one	e43f 0bdb 7b49 7334 ad3f aa31 0db5 2855 802d 2908 955e 5cb1 a649 2da7 1785 444d 5977 4102 65d5 30b4 d7d9 6557 f045 3f69 c249 526f 61e2 f700 c907 1b4e 94cf a173 2af6 454a b199 c880 68ca fa3c 5732 9cc3 d100 5b15 a516 156f db7b 223f 3426 8a26 d1a1 5928 133d 93d8 5ff5 3fd9 1ad4 00e7 f8d1 647b c523 77b0 29c9 a7c4 4afc 4c3f e5e8 7ece eb73 b380 d64a 539a 33f7 a93d 4b4f a849 4458 1b6b 2879 ed36 a074 0ed5 f22b 56ce a0ea 5a9a 89b1 b0f1 a5bf f743 c82a 51ec 0150 d5eb d073 de83 b43f ba4c 0d0a
Large size text Before the modern era, cryptography was concerned solely with message confidentiality (i.e., encryption)-conversion of messages fro m a comprehensible form into an incomprehensib le one and back again at the other end, rendering it unreadable by interceptors or eavesdroppers without secret knowledge (namely the key needed for decryption of that message). Encryption was used to (attempt to) ensure secrecy i n communicatio ns, such as those of spies, military leaders,	e43f 0bdb 7b49 7334 ad3f aa31 0db5 2855 802d 2908 955e 5cb1 a649 2da7 1785 444d 5977 4102 65d5 30b4 d7d9 6557 f045 3f69 c249 526f 61e2 f700 c907 1b4e 94cf a173 2af6 454a b199 c880 68ca fa3c 5732 9cc3 d100 5b15 a516 156f db7b 223f 3426 8a26 7b47 01ad b1eb a5cd dc92 b42b 57b9 0468 42bc 5758 6d48 6a48 273f 8361 91b8 6761 cc3f e0c8 6247 3bfe e0f0 ca1f b8c4 1947 ee31 8bca 7be4 b6c6 bfe9 a717 f767 b6f6 96df def0 76c4 1021 ce7d 2bc3 56f3 108b 382c 0cd8 54a6 dbd8 5a98 420c 9e4a a85d a046 6217 c9f5 e70f 8572 3f4b 5d26 b3ca 4a5f 3488 0310 972b 141e 8c38 8e8b 003f 662f 13ac 7cb3 91b5 0d6f 8a04 5656 7b6c ee06 c453 75f8 5169 9fff a0f4 54d9 7e9b 114d 6c12 232d a530 546f 0aab bb04 b51f ebda ba3f daa1 cf3f 657d 92e5 5785 202d fc46 117f 89f3 b285 71a7 1d31 d7e2 2fb3 33d4 350f 6983 7d0b 1982 a1fb 5928 645a 1ee5 ae4c 82ca ffa3 5eff 3257 c0db 0db3 ef4d 68b1 ed89 0508 aa61 c7db ab7d 413f c3a5 af18 87fc 5527 0436 edc9 08c4 f50f 570b 60e4 328c 2e26 0c68 7c01 fced 3edc 887b 0bf3 683d e8fd 257e e158 09a8 46ce ad83 80fe d628 7b62 aee6 4a1f a0ba d71a 3f22 4a22 74d7 7557 3feb dbb9 7db5 e804 b287 b4e7 a152 0dda 269f 00fc fe3b b021 c27f 43a7 a822 2aef 7e4e f8e1 403f dff3 a2c7 05bd 4c22 4b4f 720c ed1c 5bbe 2674 0d0a

The comparison of execution time between classic AES and Modified AES are given below:

Text Categories	Execution Time (ms)	
	Classic AES	Proposed AES
Short-size text	2	2
Medium-size text	4	4
Large-size text	7	8

Compared to classic AES, the execution time for our proposed AES increase slightly, especially for large-size text. It is caused by the IF-validation and XOR operation from roundKey we added in shiftRow transformations. However, if we take a look from security side, our proposed AES has made more difficult for cryptanalyst to break into. The analysis about the security will be provided in next part.

V. Security Analysis

Information security becomes an important issue in every encryption system. Computing technology evolves quickly and all known encryption algorithms have been studied intensively by cryptanalysts to make an efficient attack. Compare to the classic AES, our modified AES provides more security. From the security side, this new modified AES increase the aspect of confusion. In Shannon original definition, confusion means the relationship between the cipher text and symmetric key as complex and involved as possible [1]. The main confusion in shiftRow function comes from the XOR operation done from RoundKey. The generated RoundKey will be also different in each round.

VI. Conclusion and Suggestion

AES is considered as a secure encryption algorithm which is used worldwide. Our modified AES algorithm is more complex than AES algorithm but the encryption time is mostly the same. All main algorithm used in classic AES is maintained, except the shiftRow function. We increase the aspect of confusion for AES with our new shiftRow function. We conducted the experiment using Java programming language. However, our new modified AES could be implemented in different programming languages.

There are also many possibilities that can be made to increase the confusion and diffusion aspect of AES. We suggest some improvements like in mixColumns transformation. Some improvements of our modified AES algorithm will be considered for future works.

VII. References

[1] C. E. Shannon, "Communication Theory of Secrecy Systems" in *Bell System Technical Journal*, 1949.

[2] C. Paar and J. Pelzl, "The Advanced Encryption Standard (AES)," in *Understanding Cryptography*.

[3] D. K. a. C. R. Andrey Bogdanov, "Biclique Cryptanalysis of the Full AES," 2007. [Online]. Available: http://research.microsoft.com/en-us/projects/cryptanalysis/aesbc.pdf. [Accessed 13 03 2015].

[4] E. Zabala, Artist, *Rijndael_Animation_v4_eng.* [Art]. Formaestudio, 2008.

[5] H. C. van Tilborg and S. Jajodia, Encyclopedia of Cryptography and Security, Springer, 2011.

[6] J. P. Christof Paar, "Chapter 4 of "Understanding Cryptography, A Textbook for Students and Practitioners"," in *The Advanced Encryption Standard*, Springer, 2009.

[7] L. S. a. M.-D. FRUNZĂ, "Modified Advanced Encryption Standard," in *11th International Conference on DEVELOPMENT AND APPLICATION SYSTEMS*, Suceava, 2012.

[8] M. Rouse, "Advanced Encryption Standard (AES)," TechTarget, November 2014. [Online]. Available: http://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard. [Accessed 16 March 2015].

[9] M. Rouse, "Block Cipher," January 2006. [Online]. Available: http://searchsecurity.techtarget.com/definition/block-cipher. [Accessed 16 March 2015].

[10] S. H. Kamali, R. Shakerian, M. Hedayati and M. Rahmani, "A New Modified Version of Advanced Encryption Standard Based Algorithm," in *2010 International Conference on Electronics and Information Engineering (ICEIE 2010)*, 2010.

[11] T. W. &. S. P. Cusick, Cryptographic Boolean functions and applications, Academic Press, 2009.

[12] V. C. Koradia, "Modification in Advanced Encryption Standard," *Journal of information, Knowledgr and Research in Computer Engineering*, vol. 2, no. 2, pp. 356-358, 2013.