IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 5, Ver. VIII (Sep – Oct. 2014), PP 01-05
www.iosrjournals.org

Twin Key Implementation in Aes

Himanshu Gupta
Department of Computer Science, Maharaja Surajmal Institute of Technology
C4E Janakpuri, New Delhi (110058), India

Abstract: *In February 2001, NIST announced that a draft of the Federal Information Processing Standard (FIPS) was available for public review and comment. Finally, AES was published as FIPS 197 in the Federal Register in December 2001. Rijndael's has been standard by the NIST as the Advanced Encryption Standard (AES). This makes the AES essential and necessary for protection of data. We propose to reconfigure the structure of the advanced encryption standard (AES), especially in constant rotation and replaced it with variable rotation using a single key (Twins Key) that can be used for both ciphering and inverse ciphering. We demonstrate that changes can develop twin ciphers which are similar to the original one. The use of single key in AES helps to solve complexity faced during ciphering and deciphering, but it still maintains the same degree of Confusion and Diffusion. Confusion and diffusion make the use of key thus more very complex and very difficult to discover it. The use of a single key also makes this process more time efficient and variable rotation can protect data from continuous tries to attack encryption algorithm.*

Keywords: *AES, Twin key, Encryption, Decryption.*

I. Introduction:

AES is based on a design principle known as a substitution-permutation network and is fast in both software and hardware. Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant of Rijndael's which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. By contrast, the Rijndael's specification is specified with block and key sizes that may be any multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits. AES operates on a 4×4 column-major order matrix of bytes, termed the state, although some versions of Rijndael's have a larger block size and have additional columns in the state. Most AES calculations are done in a special finite field. The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input, called the plaintext, into the final output, called the cipher text. The numbers of cycles of repetition are as follows:

10 cycles of repetition for 128-bit keys.

12 cycles of repetition for 192-bit keys.

14 cycles of repetition for 256-bit keys.

Each round consists of several processing steps, including one that depends on the encryption key itself. A set of reverse rounds are applied to transform ciphered text back into the original plaintext using the same encryption key. The process is explained in Figure 1.

-->High-level description of the algorithm:

1 KeyExpansion—round keys are derived from the cipher key using Rijndael's key schedule.

II. Initial Round

2.1 **AddRoundKey**—each byte of the state is combined with the round key using bitwise XOR.

3 Rounds

3.1 SubBytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.

3.2 ShiftRows—a transposition step where each row of the state is shifted cyclically a certain number of steps.

3.3 MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.

3.4 AddRoundKey

4 Final Round (no MixColumns)
4.1 SubBytes

4.2 ShiftRows
4.3 AddRoundKey

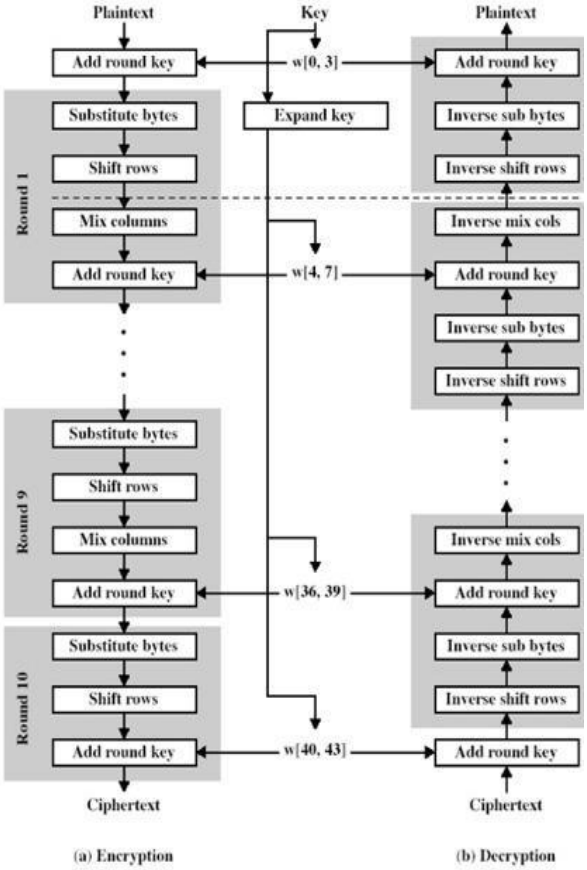

Fig. 1 Different round process

III. Twin Key:

The key plays an important role in rotation for encrypting and decrypting data. The concept of twin key enhances the dynamic property of Algorithm. Twin key is a type of key which is inverse of itself. Reason for developing twin key some constraints need to be satisfied for the dynamic row shifting:

- Both the sender and receiver should have the initial row shifting key as well as inverse with them.
- If we change something in one key and the same change is applied to the inverse key then they still retain the twin keys property, but the change should be specific.

3.1 Twin Key Structure

Rijndael has been standard by the NIST as the Advanced Encryption Standard (AES). This makes the AES essential and necessary for protection of data. We propose to reconfigure the structure of the advanced encryption standard (AES), especially in constant rotation and replaced it with variable rotation using a single key that can be used for both ciphering and inverse ciphering. The twin key structure with Dynamic rotation makes the ―Shift rows step‖ a stronger encryption stage as compared to others step in AES algorithm.

S_n->	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
K_n-> [	8	9	10	11	12	13	14	15	0	1	2	3	4	5	6	7]

Now to explain the working of twin key structure ,we will use two variables S_n(Serial Number) and K_n(Key value). The structure of the key is such that S_n and $K_{(n+8)\%16}$ have same value. This helps the key to be used for both encryption and decryption. This twin key can have around 2^16 combination and changes are also not fix or in any pattern

We can also change this key with any values but some constraints must be followed:
1. K_n , Key value should be ranging from 0 to 15.
2. The value of S_n should be equal to K(n+8)%16 .

The key is generated by an algorithm which uses three real time variables and a constant number. The three real time variables can be any variable like day, month, year or we can even synchronize our ciphers to hour, minute and second. The constant number is any random number which will provide stability to the formation of key which will help in rotation of state in AES.
Let us consider three real time variables to be r_1 , r_2 and r_3 .We now give the algorithm of generating the twin key:
1. consider Key[] = {8 , 9 , 10 , 11 , 12 , 13 , 14 , 15 , 0 , 1 , 2 , 3 , 4 , 5 , 6 , 7} and constant number = 1234(random).
2. Take integral value of r_1 , r_2 and r_3
3. Now integer i= (r_1 +/- r_2 +/- r_3 +/-constantkey) % 8.
4. Key[i] Key[i+8].
5. for(m=0 to 15)

{

int p = Key[m] row[p] = row[m]

}

3.2 Three Level Key (Dynamic Property)
The major problem in Rijndael's AES is the static property of the key. Now using the three level key structure along with twin key implementation helps in making AES dynamic. The three levels are:
1. Fixed key or static key as in Rijndael method.
2. Twin key .
3. Constant number(Random number).

Fixed key performs the same function as in Rijndael method but now there is only first time that this key is to be exchanged , after that no real key exchange is required. This key can be exchanged by any method because hack of this key will still require an extra to crack the real text.

Twin key structure as explained above is to be synchronized with decrypter using real time coefficients. Both encrypter and decrypter knows what real time coefficients is chosen. Both can generate their own key which will be similar and hence can be used in either encryption or decryption.

Benefit of using a constant number is to maintain the ease of access to the cipher. It will act as endless port numbers, with each number fixed for a particular user. This helps in increasing the range of values that can be used for dynamic AES key.

3.3Benefits of twin key

First of all , it is a key that can be changed easily unlike Rijndael method, as the change is to be made in self's method only ,the change at other site will be done automatically according to synchronization. It is easy to form a dynamic key because our new row shifting key can afford changes. As, they are same or twins and after any change can retain their properties (means twins property).Even a small change in the key brings a huge change in the text.

IV. Comparison Of Twin Key Aes With Rijndael Aes:

For comparing the rotation in Rijndael AES and Twin Key AES, we have used the SAC (Strict Avalanche Criterion) test. The **strict avalanche criterion** (**SAC**) is a generalization of the avalanche effect. It is satisfied if, whenever a single input bit is complemented, each of the output bits changes with a 50% probability. The SAC builds on the concepts of completeness and avalanche and was introduced by Webster and Tavares in 1985.

The impact of twin key structure can be measured by an Strict Avalanche Criteria (SAC) that is clear if, when an input is changed slightly (flipping a single input bits) the output changes, as shown in the following tables.

Table 1- One bit plain text change with key constant

(a) AES

Round	Number of bit altered	SAC
1	11	9
2	50	40
3	77	61
4	59	47
5	60	47
6	69	54
7	63	50
8	65	51
9	60	47
10	66	52

(b) Twin Key AES

Rounds	Number of bits altered	SAC
1	53	41
2	66	51
3	59	46
4	69	53
5	70	54
6	65	50
7	66	51
8	71	55
9	63	49
10	68	53

Table 1(a)(b) shows the impact of one bit change in plain text with key constant in AES and twin key AES.

The end result in table 1 demonstrate Avalanche effect SAC is achieved more rapidly in twin key AES than AES in second round with SAC 51%, while the SAC for AES is completed in third round. And total bit altered is 650 in DRAES which is greater than AES with 580 bit altered.

Table 2- One bit key change with

Round	Number of bit altered	SAC
1	36	29
2	63	50
3	66	52
4	55	43
5	72	57
6	65	51
7	54	43
8	63	50
9	63	50
10	66	52

(a)Twin Key AES

Round	Number of bit altered	SAC
1	70	54

2	75	58
3	76	59
4	77	60
5	81	63
6	70	54
7	69	53
8	78	60
9	85	66
10	88	68

plaintext constant (a)AES

Table 2(a)(b) shows the impact of one bit key change with plaintext constant in AES and Twin Key AES. The end result in table 2 demonstrate Avalanche effect SAC is achieved more rapidly in DRAES than AES in first round with SAC 54%, while the SAC for AES is completed in second round. And total bit altered is 769 in DRAES which is greater than AES with 571 bit altered.

V. Conclusion:

With Dynamic rotation for advanced encryption standard DRAES using the Twin key is stronger than rotation that occur in AES, that mean that Rijndael is more secure and physically powerful with twin key structure when compared to Rijndael with constant rotation as publicized from results of Strict Avalanche Criterion(SAC) test.

References

[1] Daniel J. Bernstein, ―Understanding brute force, Department of Mathematics‖, Statistics, and Computer Science (M/C 249) The University of Illinois at Chicago, IL 60607-7045, 2006

[2] Neeraj Kumar, ―Investigations in Brute Force Attack on Cellular Security Based on Des and Aes‖, IJCEM International Journal of Computational Engineering & Management, Vol. 14, October 2011, ISSN 2230-7893

[3] Alex Biryukov, Dmitry Khovratovich, IvicaNikoli_c, ―Distinguisher and Related-Key Attack on the Full AES-256‖,University of Luxembourg falex.biryukov, Dmitry.khovratovich, ivica.nikolic@uni.lug10 August 2009.

[4] EladBarkan and Eli Biham, ―In How Many Ways Can You Write Rijndael?‖, Computer Science Department Technion { Israel Institute of Technology Haifa 32000, Israel ,2006.

[5] Krishnamurthy G N, V Ramaswamy, ―Making AES Stronger: AES with Key Dependent S Box‖,IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.9, September 2008.

[6] Jiqiang Lu1, Orr Dunkelman2, Nathan Keller3, and Jongsung Kim4, ―New Impossible Differential Attacks on AES‖, Volume 5365 of Lecture Notes in Computer Science, pp. 279–293, Springer- Verlag, 2008.

[7] Serge Vaudenay, ―A CLASSICAL INTRODUCTION TO MODERN CRYPTOGRAPHY‖, Springer Science+Business Media, Inc.,2006, ISBN-13: 978-0-387-25464-7.

[8] G. Lokeshwari, Dr. S. Udaya Kumar and G. Aparna ―A CONFIGURABLE SECURED IMAGE ENCRYPTION TECHNIQUE USING 3D ARRAY BLOCK ROTATION**",** International Journal of Engineering Science and Technology (IJEST), Vol. 4 No.01 January 2012.

[9] KonstantinosDrakakis, Senior Member, IEEE, VerónicaRequena, and Gary McGuire, ―On the Nonlinearity of Exponential Welch Costas Functions‖, IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 56, NO. 3, MARCH 2010.

[10] Mohan H. S. and A RajiReddy , ―Performance Analysis of AES and MARS Encryption Algorithms‖, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No 1, July 2011.