Cryptographic Algorithm: AES

Saoud Sarwar[1] Shikha Kumari[2] Mahenaz Fatima[3] Almas Zahra[4] Syed Tariq[5]
[1,2,3,4,5]Department of Computer Science
[1,2,3,4,5]Al-falah School of Engg. & technology, Faridabad, India

Abstract — AES is the advanced encryption standard, for encrypting and decrypting data. AES was published by NIST (National Institute of Standards and Technology. AES is a block cipher algorithm described on Federal Information Processing Standard (FIPS). AES was created by two Belgian cryptographers, Vincent Rijmen and Joan Daemen, replacing the old Data Encryption Standard (DES), which grew vulnerable to brute-force attacks due to its 56-bit effective key length. It takes an input block of a certain size, usually 128, and produces a corresponding output block of the same size.

Keywords: AES algorithm (encryption, decryption), ciphers, PKC.

I. MODERN CRYPTOGRAPHIC ALGORITHMS

Cryptographic algorithm is a set of rules that is used to encrypt and decrypt message in a cryptographic system.
Secret Key (Symmetric) Cryptography (SKC): Uses a single key for both encryption and decryption
In cryptography, a cipher (or cipher) is an algorithm for performing encryption and decryption
In a stream cipher the plaintext digits are encrypted one at a time, and the transformation of successive digits varies during the encryption.
Block cipher is a symmetric key cipher which operates on fixed-length groups of bits, termed blocks, with an unvarying transformation.
Public Key (Asymmetric) Cryptography (PKC): Uses one key for encryption and another for decryption
Hash (One-Way) Functions: Uses a mathematical transformation to irreversibly "encrypt" information

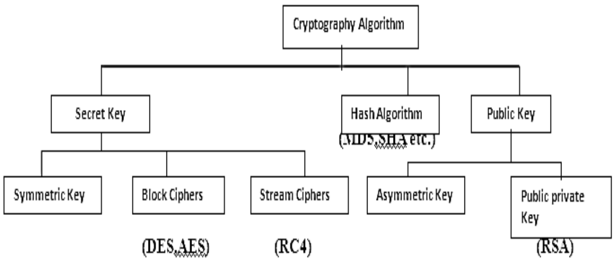


Fig. 1

II. ADVANCED ENCRYPTION STANDARD (AES)

AES is one of the most important block cipher cryptographic technique designed in 1997 after DES was found too weak due to its small key size. Although triple DES (3DES) increased the key size, the process was too slow. AES was called block cipher technique as it works on fixed-length group of bits, which are called *blocks*. It takes an input block of a certain size, usually 128, and produces a corresponding output block of the same size. For transformation, secret key is used as second input. So it is important to know that the secret key can be of any size (depending on the cipher used) and that AES uses three different key sizes: 128, 192 and 256 bits. AES uses no. of rounds, which are fixed depending on key size.
Relationship between no. of rounds and cipher key size Rounds

Key size	No. of rounds(N_r)
128	10
192	12
256	14

Table 1

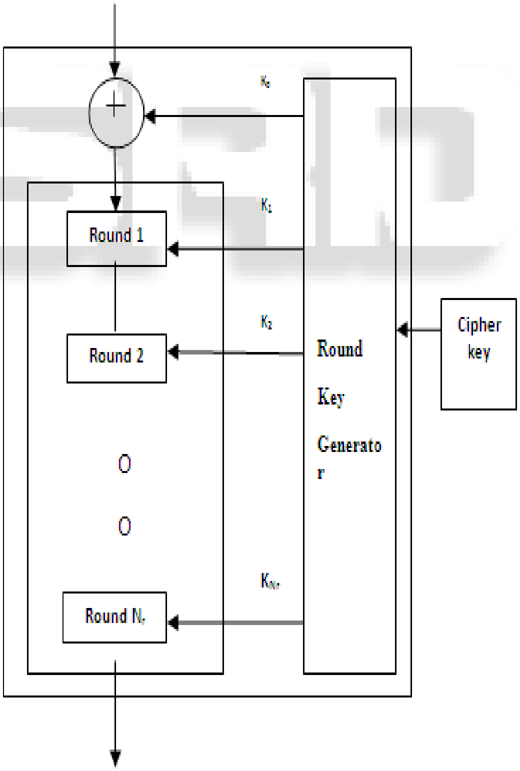


Fig. 2

Each round of AES, except for the last, is a cipher with four operations. The last round of the encryption alone is different in a way that the mixed column operation will not be carried out.

III. STRUCTURE OF EACH ROUND AT ENCRYPTION SITE

One AddRoundKey is applied before first round. Also the third transformation i.e MixColumn is missing in last round.

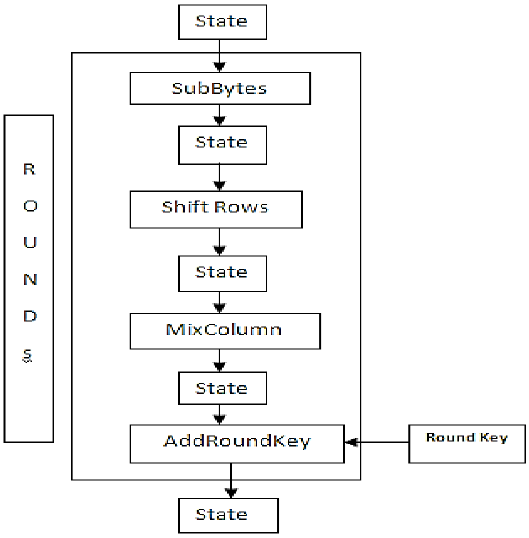
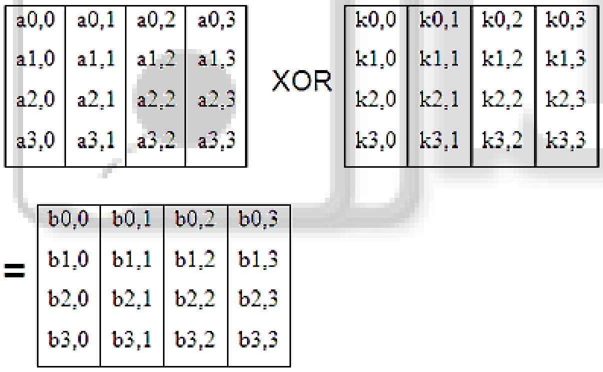


Fig. 3

IV. THE ADDROUNDKEY OPERATION

In this operation, a Round Key is applied to the state by a simple bitwise XOR. The Round Key is derived from the Cipher Key by the means of the key schedule. The Round Key length is equal to the block key length (=16 bytes).

The sub key is added by combining each byte of the State with the corresponding byte of the sub key using bitwise XOR.



a0,0	a0,1	a0,2	a0,3
a1,0	a1,1	a1,2	a1,3
a2,0	a2,1	a2,2	a2,3
a3,0	a3,1	a3,2	a3,3

XOR

k0,0	k0,1	k0,2	k0,3
k1,0	k1,1	k1,2	k1,3
k2,0	k2,1	k2,2	k2,3
k3,0	k3,1	k3,2	k3,3

=

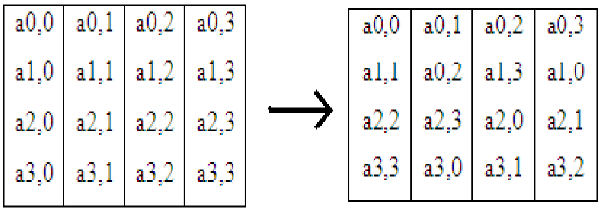
b0,0	b0,1	b0,2	b0,3
b1,0	b1,1	b1,2	b1,3
b2,0	b2,1	b2,2	b2,3
b3,0	b3,1	b3,2	b3,3

Where b(i,j)=a(i,j) XOR k(i,j)

V. THE SHIFTROW OPERATION

In this operation, each row of the state is cyclically shifted to the left, depending on the row index.

The 1st row is shifted 0 positions to the left.
The 2nd row is shifted 1 position to the left.
The 3rd row is shifted 2 positions to the left.
The 4th row is shifted 3 positions to the left.



a0,0	a0,1	a0,2	a0,3
a1,0	a1,1	a1,2	a1,3
a2,0	a2,1	a2,2	a2,3
a3,0	a3,1	a3,2	a3,3

→

a0,0	a0,1	a0,2	a0,3
a1,1	a0,2	a1,3	a1,0
a2,2	a2,3	a2,0	a2,1
a3,3	a3,0	a3,1	a3,2

VI. SUBBYTES OPERATION

The SubBytes operation is a non-linear byte substitution, operating on each byte of the state independently. The substitution table (S-Box) is invertible and is constructed by the composition of two transformations:

1. Take the multiplicative inverse in Rijndael's finite field
2. Apply an affine transformation which is documented in the Rijndael documentation.

Since the S-Box is independent of any input, pre-calculated forms are used. Each byte of the state is then substituted by the value in the S-Box whose index corresponds to the value in the state:

a(i,j) = SBox[a(i,j)] The inverse of SubBytes is the same operation, using the inversed S-Box, which is also pre-calculated.

VII. THE MIXCOLUMN OPERATION

This section involves advance mathematical calculations in the Rijndael's finite field. It corresponds to the matrix multiplication with:

$$\begin{matrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{matrix}$$

And that the addition and multiplication operations are different from the normal ones.

VIII. CONCLUSION

This paper was successfully completed with the explanation of AES algorithm. For the future works of this paper implementation is done on 128 bits. An extra modification to be used for 192 bit and 256 bit key AES.

REFERENCES

[1] AES page available via http://www.nist.gov/Crypto Toolkit.
[2] Computer Security Objects Register (CSOR): http://csrc.nist.gov/csor/.
[3] Cryptography and Network Security, 2nd Edition By Atul Kahate.
[4] J. Daemen and V. Rijmen, AES Proposal: Rijndael, AES Algorithm Submission, September 3, 1999, available at [1].
[5] J. Daemen and V. Rijmen, The block cipher Rijndael, Smart Card research and Applications, LNCS 1820, Springer-Verlag, pp. 288-296.
[6] B. Gladman’s AES related home page http://fp.gladman. plus.com/cryptography_technology/.
[7] A. Lee, NIST Special Publication 800-21, Guideline for Implementing Cryptography in the Federal Government, National Institute of Standards and Technology, November 1999.