Advanced Encryption Standard (AES)

Contents

1- Introduction

Among many symmetric cryptographies, Advanced Encryption Standard (AES) [1] is an efficient scheme for both hardware and software implementation. In addition to AES encryption and decryption, there is an increasing demand for different modes of operation to further enhance the security level in the widespread network applications.

2- Algorithm

The AES cryptography is a block cipher that processes data blocks of 128 bits with a cipher key of 128, 192, or 256 bits. A 128-bit data block can be treated as a 4×4 byte array, also known as the State. Figure 1 shows the encryption and decryption procedures in our AES cipher. The encryption and decryption have to be performed by Nr rounds, where Nr = 10, 12, or 14 for cipher key of length 128, 192, or 256 bits, respectively. An AES round function consists of four transformations operating on bytes, rows and columns on the State [1], which are briefly described as follows.

SubBytes(): a nonlinear byte-oriented substitution, also known as S-Box, consisting of a) a multiplicative inverse in finite field GF(28) with irreducible polynomial m(x) = x8 + x4 + x3 + x + 1; and b) an affine transformation over GF(2). The affine transformation can be done by a matrix multiplication and an addition.

ShiftRows(): a cyclic shifting on each row of the State with different number of byte offsets.

MixColumns(): mixing the bytes of each column by multiplying the four column polynomials of the State with a given polynomial modulo x4 + 1 with their coefficient in GF(28). The column polynomial is a polynomial of degree three with the four bytes in that column as its coefficients.

AddRoundKey(): an addition of a round key to the State. The round keys are generated by the key expansion procedure.

Key generation of the AES algorithm consists of the S-Box, AddRoundKey() and RotWord() transformations. The RotWord() performs cyclic shifting of a 4-byte word. Key generation and scheduling of the 192- and 256-bit keys is much more complicated than that of the 128-bit key scheme.

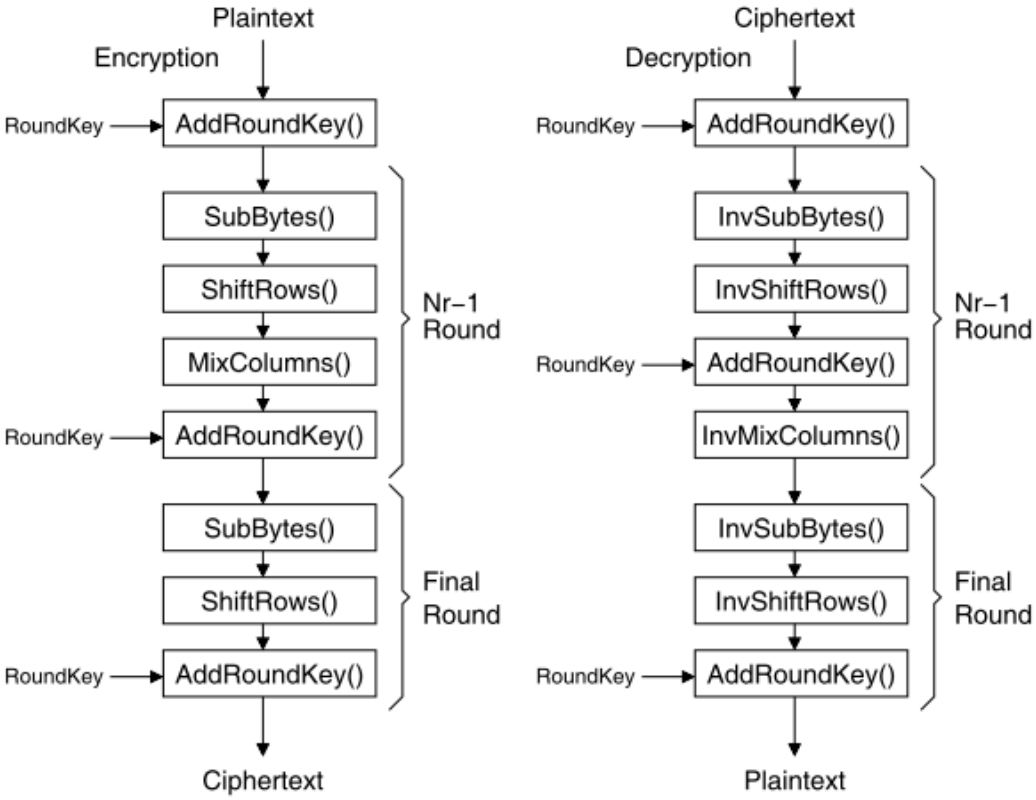

Figure 1 - The procedure of encryption and decryption.

3- References

[1] National Institute of Standards and Technology (NIST), Advanced Encryption Standard (AES), National Technical Information Service, Springfield, VA 22161, Nov. 2001.