Information Protection & Computer Security

Rajendra Kachhwaha
Email: rajendra1983@gmail.com

June 30, 2015

- **Already Covered:**

  1. Security Architecture, Security Attacks, Security Services.

  2-3.Model for Network Security,Basic terms used in Cryptography, Symmetric Cipher Model, Substitution Techniques, Transpositions Techniques.

  4.Block Cipher and Stream Ciphers,Component of Modern Block Cipher, Feistel Cipher Structure, Data Encryption Standard (DES)

  5. Numerical Problems

  6.Triple DES, Block Cipher Modes

- Lecture 7.

  Today's Topic:

  Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES):

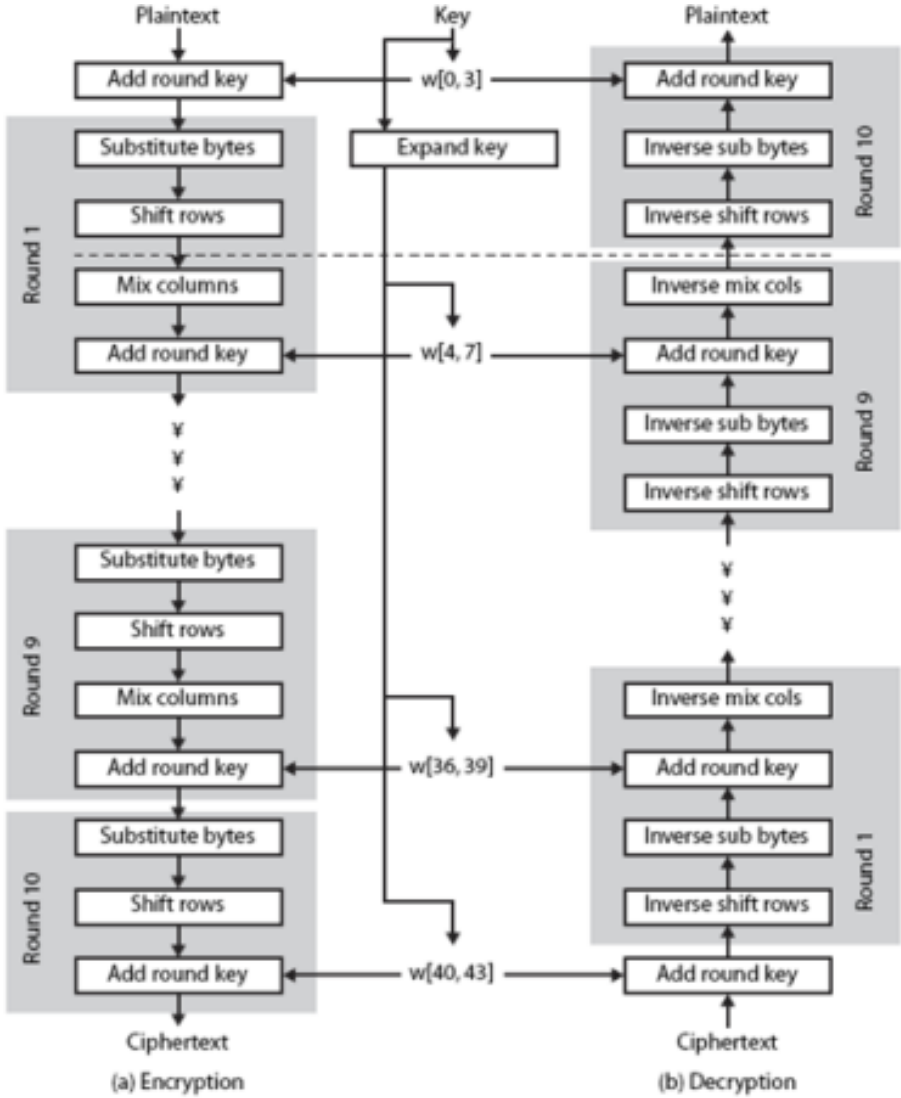
1. AES is based on a design principle known as a substitution-permutation network, combination of both substitution and permutation, and is fast in both software and hardware.
2. Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits.
3. AES operates on a $4x4$ column-major order matrix of bytes.
4. 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 ciphertext. The number 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.
5. Each round consists of several processing steps.

Advanced Encryption Standard (AES):

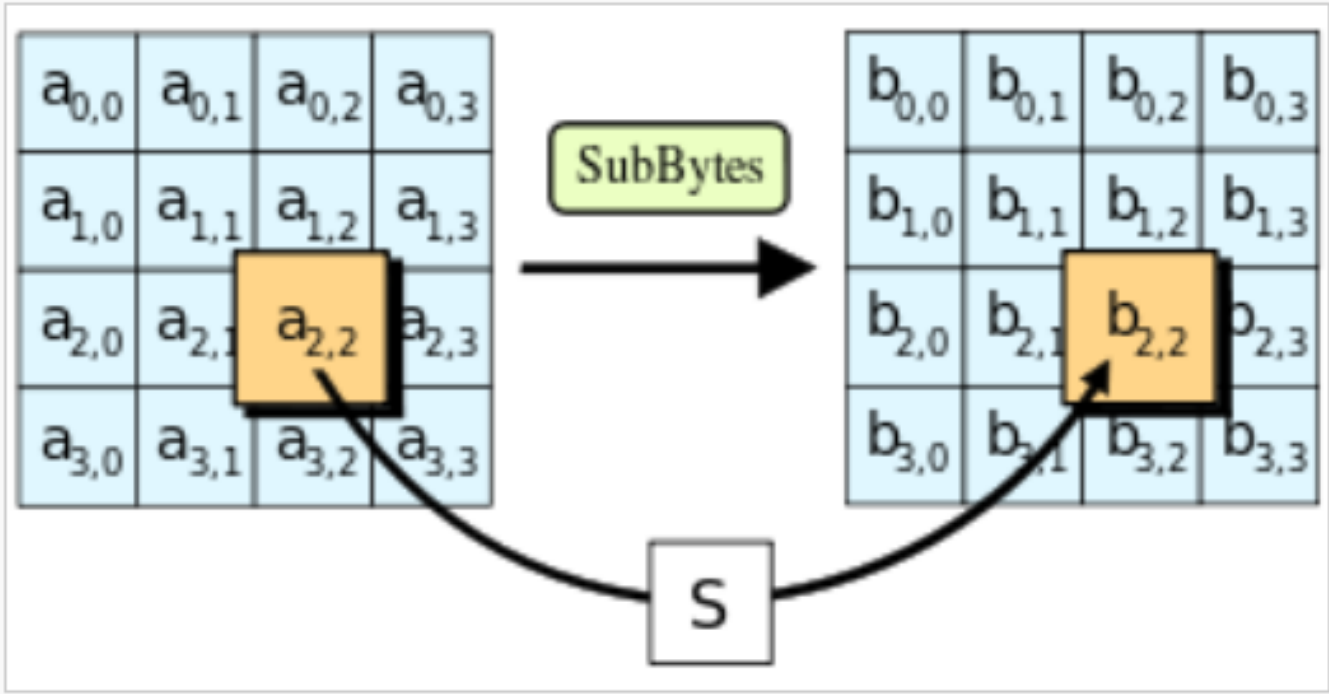
High-level description of the algorithm

1. KeyExpansions-round keys are derived from the cipher key using Rijndael's key schedule.
2. InitialRound-AddRoundKey-each byte of the state is combined with a block of the round key using bitwise xor.
3. Rounds
   - SubBytes-a non-linear substitution step where each byte is replaced with another according to a lookup table.
   - ShiftRows-a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
   - MixColumns-a mixing operation which operates on the columns of the state, combining the four bytes in each column.
   - AddRoundKey
4. Final Round (no MixColumns)
   - SubBytes
   - ShiftRows
   - AddRoundKey.

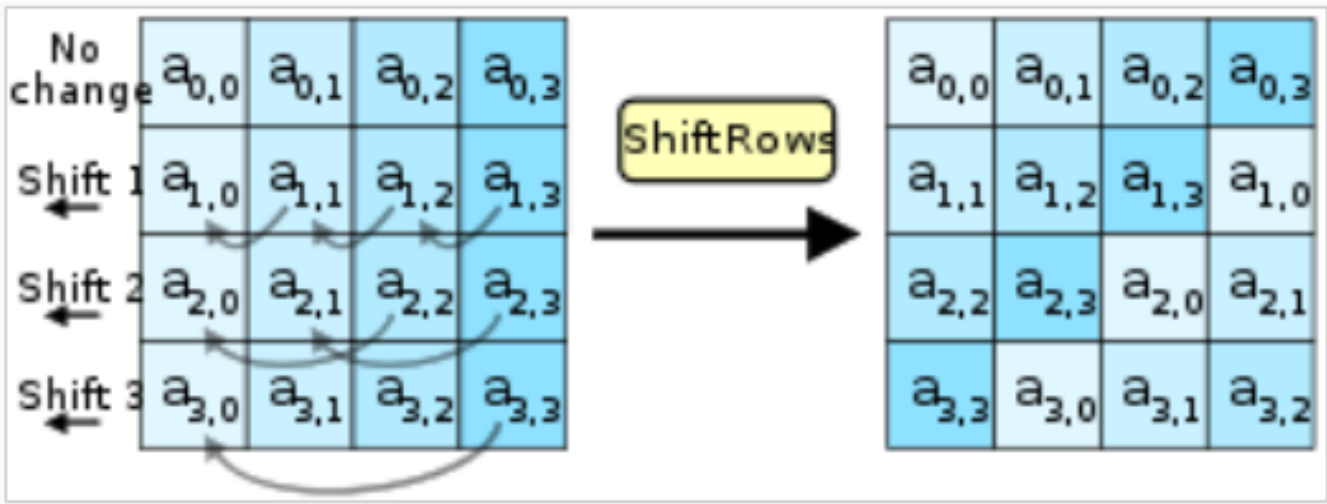
Advanced Encryption Standard (AES):



Advanced Encryption Standard (AES):SubBytes:



Advanced Encryption Standard (AES):ShiftRows:

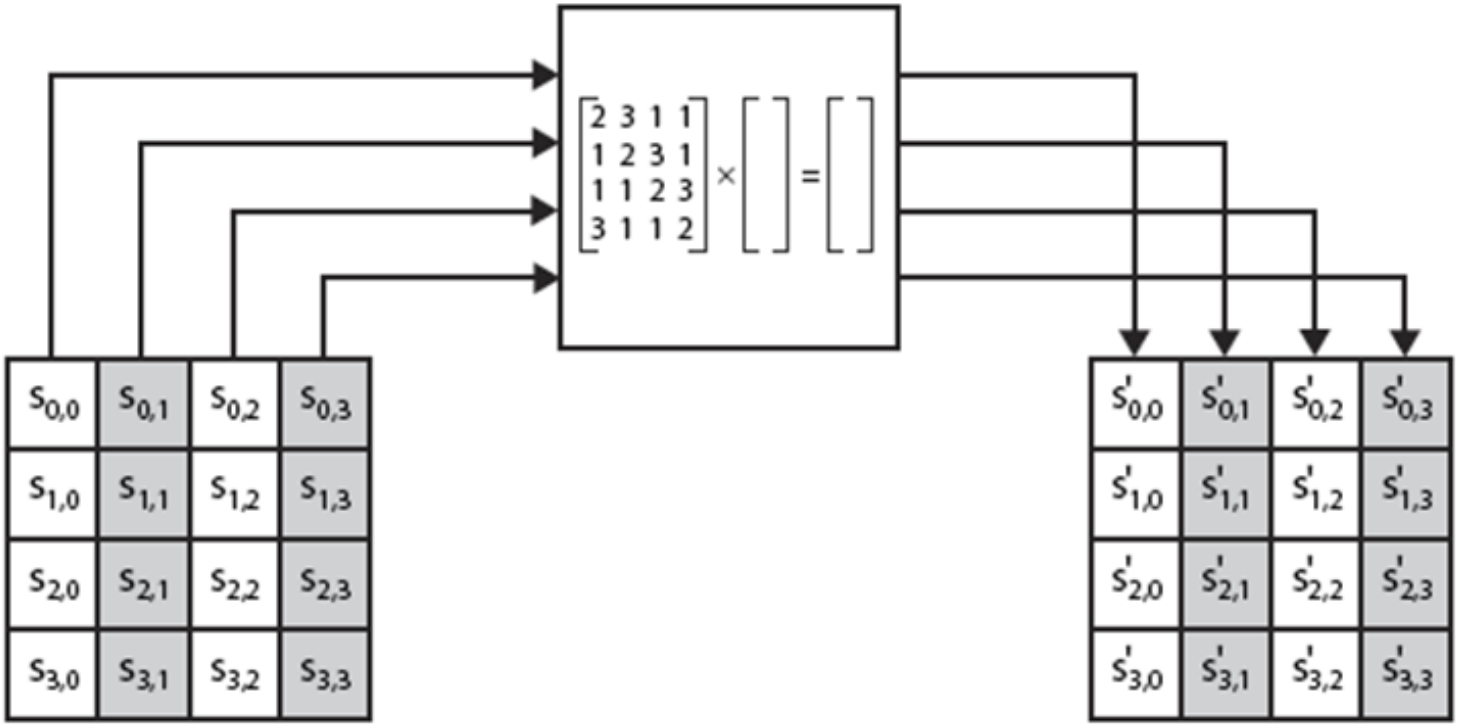


87	F2	4D	97
EC	6E	4C	90
4A	C3	46	E7
8C	D8	95	A6

→

87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

Advanced Encryption Standard (AES):MixColumns:



Advanced Encryption Standard (AES):MixColumns:

87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

→

47	40	A3	4C
37	D4	70	9F
94	E4	3A	42
ED	A5	A6	BC

$$(\{02\} \bullet \{87\}) \oplus (\{03\} \bullet \{6E\}) \oplus \{46\} \oplus \{A6\} = \{47\}$$

$$\{87\} \oplus (\{02\} \bullet \{6E\}) \oplus (\{03\} \bullet \{46\}) \oplus \{A6\} = \{37\}$$

$$\{87\} \oplus \{6E\} \oplus (\{02\} \bullet \{46\}) \oplus (\{03\} \bullet \{A6\}) = \{94\}$$

$$(\{03\} \bullet \{87\}) \oplus \{6E\} \oplus \{46\} \oplus (\{02\} \bullet \{A6\}) = \{ED\}$$

Advanced Encryption Standard (AES):MixColumns:

Calculation of MixColumns:

1. Take the value: 02 and 87.(Hex format)
2. Perform their multiplication.(Result is: 10E: binary equivalent: 1 0000 1110
3. Consider only 8 bits from left side.
4. Perform X-OR of this with: 11B (binary equivalent:1 0001 1011)
5. Record the result: 15 (binary equivalent: 0001 0101)
6. Galois Field GF(2^8) = 11B = polynomial $x^8 + x^4 + x^3 + x + 1$ (binary equivalent:1 0001 1011). This will be discussed in details in modular arithmetic.
7. 03 x 6E = 14A = 1 0100 1010 xor 1 0001 1011 = 0 0101 0001

Advanced Encryption Standard (AES):AddRoundKey: