Advanced Encryption Standard

Reference: Stallings, **Data and Computer Communications, 7th Edition**,Pearson/P-H, 2004

AES Background

- 1997 --National Institute of Standards and Technology (NIST) issues a call for proposals.
- 2001--AES issues as a federal information processing standards (FIPS 197)
- AES published in December 2001, a replacement for DES.

AES Requirements

- Security Strength Equal to or Better than 3DES
- Significantly More Efficient than 3DES
- Symmetric Block Cipher
- Block Length = 128 bits
- Support for Key Lengths of 128, 192, and 256 bits

Evaluation Criteria for AES Proposals

- Security
- Computational Efficiency
- Memory Requirements
- Hardware and Software Suitability
- Flexibility

Rounds and Transformation Stages

- The encryption process executes a **round function**, Nr times, with the number of rounds (Nr) being dependent on key size.
- The round function consists of four **transformation** stages.
  - SubBytes()
  - ShiftRows()
  - MixColumns()
  - AddRoundKey()

Rounds and Transformation Stages (p.2)

- The cipher begins with an AddRoundKey().
- All rounds then execute each of the transformations except the last round.
- The MixColumns( ) transformation is not executed in the final round.
- For a 128 bit key, there are 10 rounds.
- 12 and 14 rounds are used with keys of 192 and 256.

SubBytes ( ) Transformation

- The substitute transformation is an S-Box process, that is independent of the key.
- Each of the bytes of the State is replaced by a different byte, according to a table.
- The table is fixed and derived from two transformations defined in the standard.
- The table is an 8 x 8 array, indexed with the State byte.

ShiftRows( ) Transformation

- The ShiftRows() transformation is a permutation that is performed row by row on the State array, independently of the key.
- The first row is not shifted.
- The 2^{nd} row is circularly shifted left 1 byte.
- The 3^{rd} row is circularly shifted left 2 bytes.
- The 4^{th} row is circularly shifted left 3 bytes.

MixColumns() Transformation

- The MixColumns( ) transformation manipulates each column of the state array.
- The process can be described as a matrix multiplication of a polynomial and the state array.
- This process does not depend on the key.

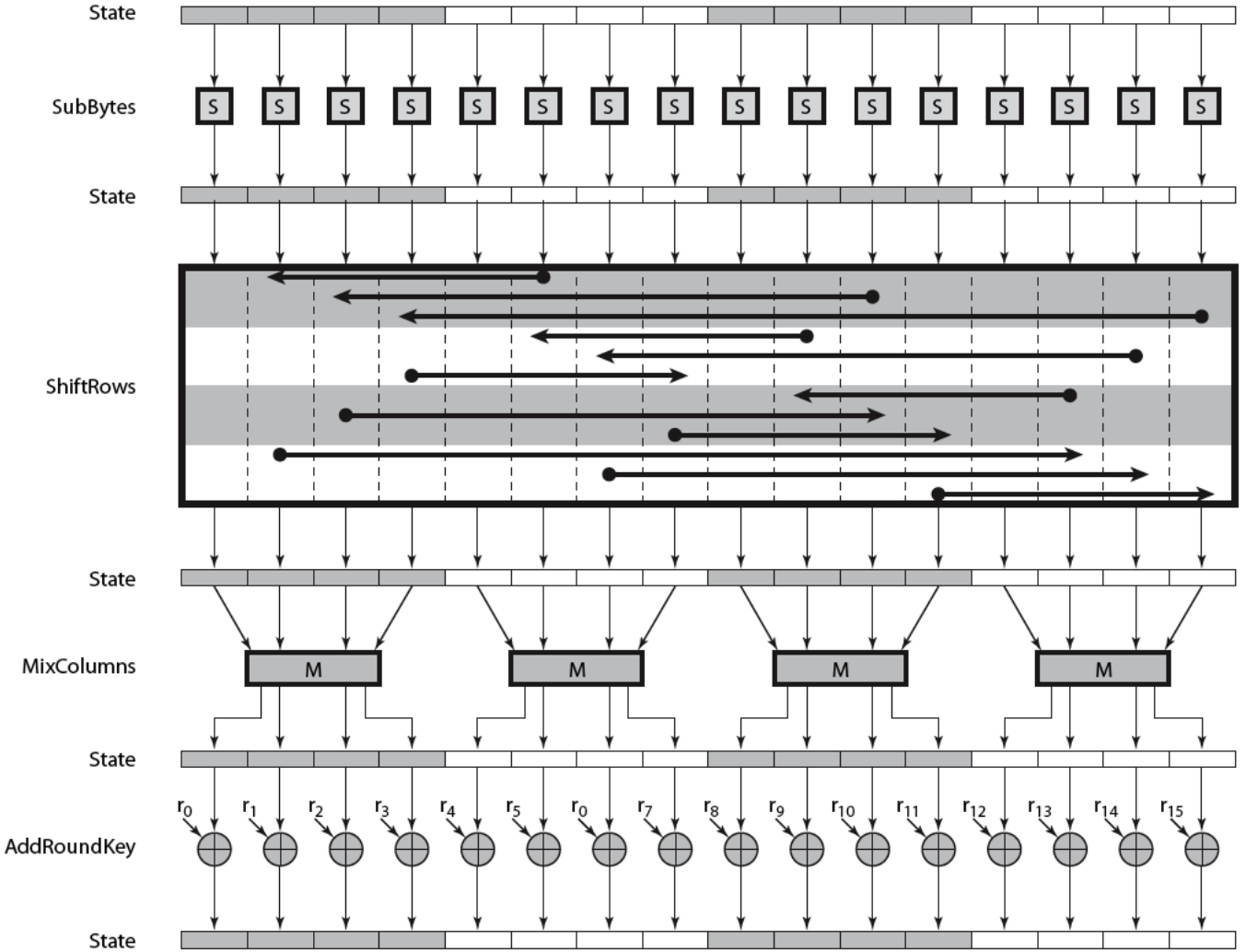
AddRoundKey( ) Transformation

- The AddRoundKey( ) transformation uses the key schedule word.
- The process is a bitwise XOR of the columns of the state array, with the key schedule word.

AES Decryption

- AES decryption is accomplished using inverses of the transformations, in the appropriate order.
- The AddRoundKey( ) is its own inverse when (since $A \oplus B \oplus B = A$).

AES Round


State
SubBytes
S
State
ShiftRows
State
MixColumns
M
State
AddRoundKey
r0
r1
r2
r3
r4
r5
r0
r7
r8
r9
r10
r11
r12
r13
r14
r15
State

AES Decryption