Advanced Encryption Standard

CSS 322 – Security and Cryptography

Contents

- History of AES
- Simplified AES as an example
- Features of AES

History of AES

- 1977 – DES (56-bit key). NIST published.
- 1999 – 3DES (168-bit key). NIST recommended 3DES be used (DES only for legacy systems)
  - 3DES is considered very secure (no known attacks apart from brute force)
  - But 3DES is very slow, especially in software
  - DES and 3DES use 64-bit blocks – larger block sizes required for efficiency
- 1991 – IDEA, similar to DES, secure but patent issues
- 1997 – NIST called for proposals for new Advanced Encryption Standards
  - Proposals made public and evaluations performed
- 2001 – Selected algorithm for AES, Rijndael, published as standard

Selecting a Winner

- Original NIST criteria:
  - Security: effort to cryptoanalyze algorithm, randomness, …
  - Cost: royalty-free license, computationally efficient, …
  - Algorithm and implementation characteristics: flexibility (different keys/blocks, implement on different systems), simplicity, …
- 21 candidate algorithms reduced to 5
- Updated NIST evaluation criteria for 5 algorithms:
  - General Security
  - Software and hardware implementations (needs to be efficient)
  - Low RAM/ROM requirements (e.g. for smart cards)
  - Ability to change keys quickly
  - Potential to use parallel processors

Selecting Rijndael for AES

- Security: good, no known attacks
- Software implementation: fast, can make use of parallel processors
- Hardware implmentation: fastest of all candidates
- Low memory requirements: good, except encryption and decryption require separate space
- Timing and Power analysis attacks: easiest to defend against
- Key flexibility: supports on-the-fly change of keys and different size of keys/blocks

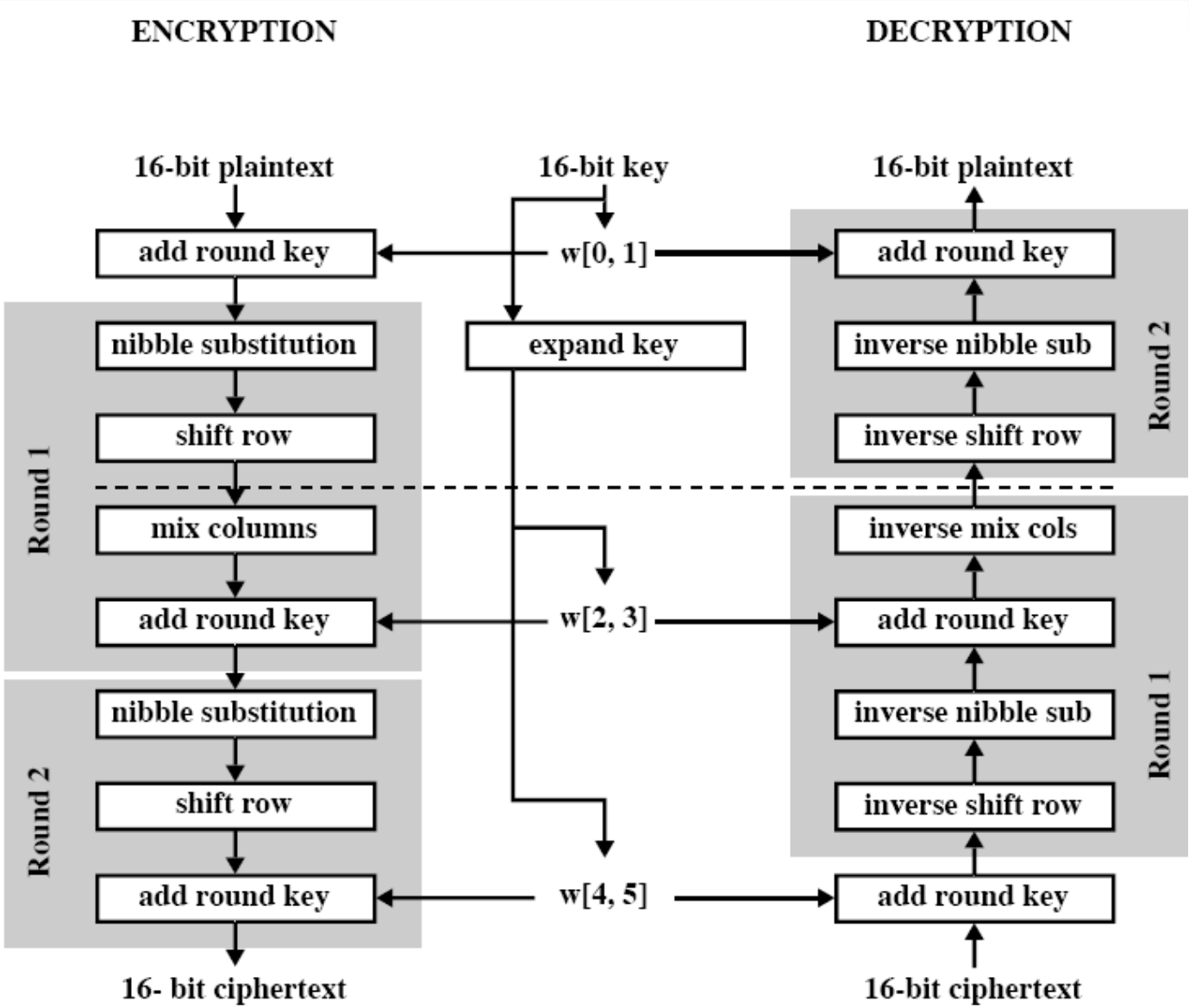
Overview of Rijndael/AES

- Rijndael allows variety of block and key sizes
  - 128, 160, 192, 224 and 256 bits
  - Key can be different size to block
- AES standardises block size of 128 bits, key sizes of 128, 192 and 256 bits
- We will use Simplified AES (S-AES) to help understand
  - Again, S-AES is not used in the real world, only an educational tool
- For details of AES (S-Boxes and other operations), see the textbook

Simplified AES

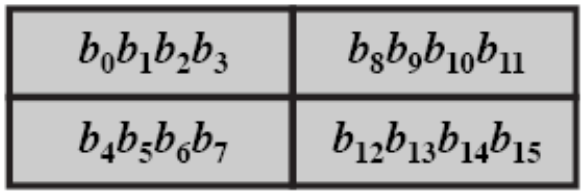
- Input: 16-bit block of plaintext; 16-bit key
- Output: 16-bit block of ciphertext
- Four operations:
  1. Add Key: XOR of a 16-bit key and 16-bit state matrix
  2. Nibble substitution: table lookup that swaps nibbles (4-bits)
  3. Shift Row: shift of nibbles in a row
  4. Mix Column: re-order columns
- 3 rounds:
  - Round 0: Add key
  - Round 1: All four operations
  - Round 2: Three operations

S-AES Encryption and Decryption

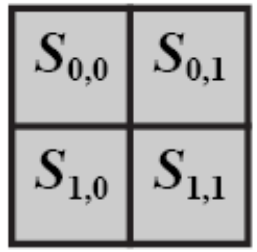


S-AES State Operations

- S-AES performs operations on 16-bit state matrix
  - View as 4 nibbles (a nibble is 4 bits)
  - Initial value is the 16-bit plaintext



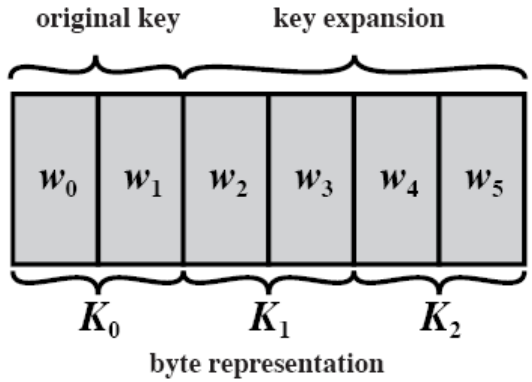
bit representation



nibble representation

  - The original 16-bit key is expanded to 3 x 16-bit round keys

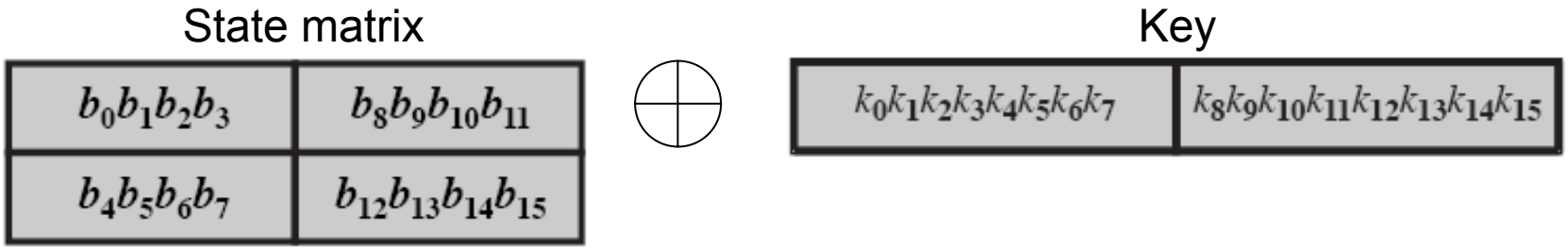
bit representation



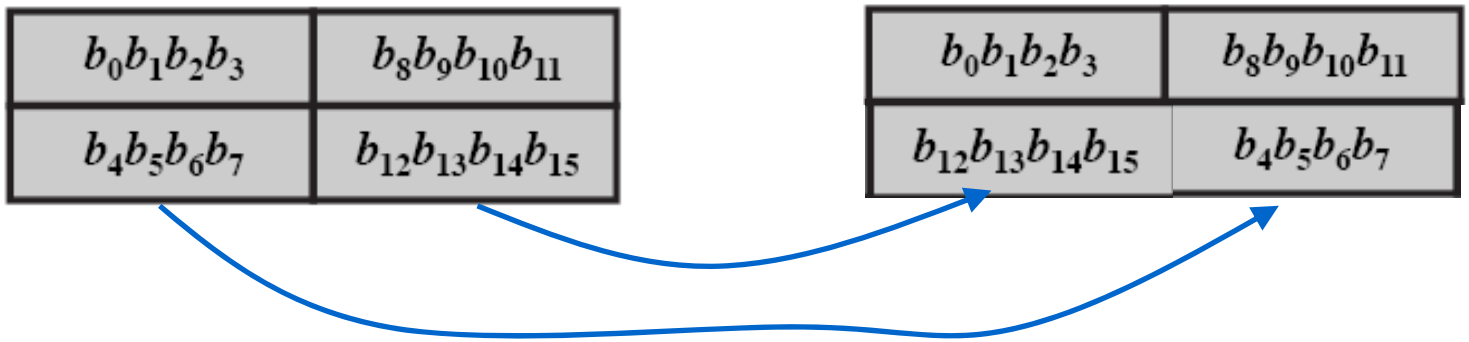
byte representation

S-AES Add Key and Shift Row

- Add Key: 16-bit State matrix XOR 16-bit key



- Shift Row: swap nibbles on second row of state matrix



S-AES Nibble Substitution

- Nibble substitution replaces one nibble in state matrix with a new nibble:
  - Substitution is defined by an S-Box
  - Left most 2 bits in state matrix nibble point to row of S-Box
  - Right most 2 bit in state matrix nibble point to column of S-Box
  - State matrix nibble is replaced with S-Box nibble in row/column

	00	01	10	11
00	1001	0100	1010	1011
01	1101	0001	1000	0101
10	0110	0010	0000	0011
11	1100	1110	1111	0111

S-Box (encryption)

	00	01	10	11
00	1010	0101	1001	1011
01	0001	0111	1000	1111
10	0110	0000	0010	0011
11	1100	0100	1101	1110

Inverse S-Box (decryption)

S-AES Mix Column Operation

- Mix the columns in state matrix as follows:

$$\begin{bmatrix} 1 & 4 \\ 4 & 1 \end{bmatrix}\begin{bmatrix} S_{0,0} & S_{0,1} \\ S_{1,0} & S_{1,1} \end{bmatrix}=\begin{bmatrix} S'_{0,0} & S'_{0,1} \\ S'_{1,0} & S'_{1,1} \end{bmatrix}$$

such that:

$$S'_{0,0} = S_{0,0} \oplus (4 \cdot S_{1,0})$$
$$S'_{1,0} = (4 \cdot S_{0,0}) \oplus S_{1,0}$$
$$S'_{0,1} = S_{0,1} \oplus (4 \cdot S_{1,1})$$
$$S'_{1,1} = (4 \cdot S_{0,1}) \oplus S_{1,1}$$

- NOTE: addition and multiplication are performed using GF(2^4) arithmetic
  - We do not cover fields and Galois fields (GF). Addition and multiplication tables for GF(2^4) are given in following slides. Details can be found in textbook
- Inverse mix column (for decryption)

$$\begin{bmatrix} 9 & 2 \\ 2 & 9 \end{bmatrix}\begin{bmatrix} S_{0,0} & S_{0,1} \\ S_{1,0} & S_{1,1} \end{bmatrix}=\begin{bmatrix} S'_{0,0} & S'_{0,1} \\ S'_{1,0} & S'_{1,1} \end{bmatrix}$$

GF(2^4) Addition

+	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
1	1	0	3	2	5	4	7	6	9	8	B	A	D	C	F	E
2	2	3	0	1	6	7	4	5	A	B	8	9	E	F	C	D
3	3	2	1	0	7	6	5	4	B	A	9	8	F	E	D	C
4	4	5	6	7	0	1	2	3	C	D	E	F	8	9	A	B
5	5	4	7	6	1	0	3	2	D	C	F	E	9	8	B	A
6	6	7	4	5	2	3	0	1	E	F	C	D	A	B	8	9
7	7	6	5	4	3	2	1	0	F	E	D	C	B	A	9	8
8	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7
9	9	8	B	A	D	C	F	E	1	0	3	2	5	4	7	6
A	A	B	8	9	E	F	C	D	2	3	0	1	6	7	4	5
B	B	A	9	8	F	E	D	C	3	2	1	0	7	6	5	4
C	C	D	E	F	8	9	A	B	4	5	6	7	0	1	2	3
D	D	C	F	E	9	8	B	A	5	4	7	6	1	0	3	2
E	E	F	C	D	A	B	8	9	6	7	4	5	2	3	0	1
F	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0

Examples: 5+A=F; C+D=1, 1+1=0

GF(2^4) Multiplication

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
2	0	2	4	6	8	A	C	E	3	1	7	5	B	9	F	D
3	0	3	6	5	C	F	A	9	B	8	D	E	7	4	1	2
4	0	4	8	C	3	7	B	F	6	2	E	A	5	1	D	9
5	0	5	A	F	7	2	D	8	E	B	4	1	9	C	3	6
6	0	6	C	A	B	D	7	1	5	3	9	F	E	8	2	4
7	0	7	E	9	F	8	1	6	D	A	3	4	2	5	C	B
8	0	8	3	B	6	E	5	D	C	4	F	7	A	2	9	1
9	0	9	1	8	2	B	3	A	4	D	5	C	6	F	7	E
A	0	A	7	D	E	4	9	3	F	5	8	2	1	B	6	C
B	0	B	5	E	A	1	F	4	7	C	2	9	D	6	8	3
C	0	C	B	7	5	9	E	2	A	6	1	D	F	3	4	8
D	0	D	9	4	1	C	8	5	2	F	B	6	3	E	A	7
E	0	E	F	1	D	3	2	C	9	7	6	8	4	A	B	5
F	0	F	D	2	9	6	4	B	1	E	C	3	8	7	5	A

Examples: 5xA=4, CxD=3, 1x1=1

S-AES Key Expansion

- Original 16-bit key is expanded to 3 x 16-bit keys
  - Represent 16-bit key as two 8-bit word:
    - Key 1: w0, w1
    - Key 2: w2, w3
    - Key 3: w4, w5

$$w_2 = w_0 \oplus 10000000 \oplus SubNib\left(RotNib\left(w_1\right)\right)$$

$$w_3 = w_2 \oplus w_1$$

$$w_4 = w_2 \oplus 00110000 \oplus SubNib\left(RotNib\left(w_3\right)\right)$$

$$w_5 = w_4 \oplus w_3$$

    - where RotNib swaps the left nibble with the right nibble and SubNib is a substitution as defined on previous slide

Comparing S-AES and AES

- S-AES
  - 16-bit key
  - 16-bit plaintext/ciphertext
  - 2 rounds
    - First with all four operations
    - Last with 3 operations
  - Round key size: 16 bits
  - Mix Columns: arithmetic over GF(2^4)
- AES-128
  - 128-bit key
  - 128 bit plaintext/ciphertext
  - 10 rounds
    - 9 with all four operations
    - Last with 3 operations
  - Round key size: 128 bits
  - Mix Columns: arithmetic over GF(2^8)

Principles of operation are the same
Details of AES can be found in textbook and standard

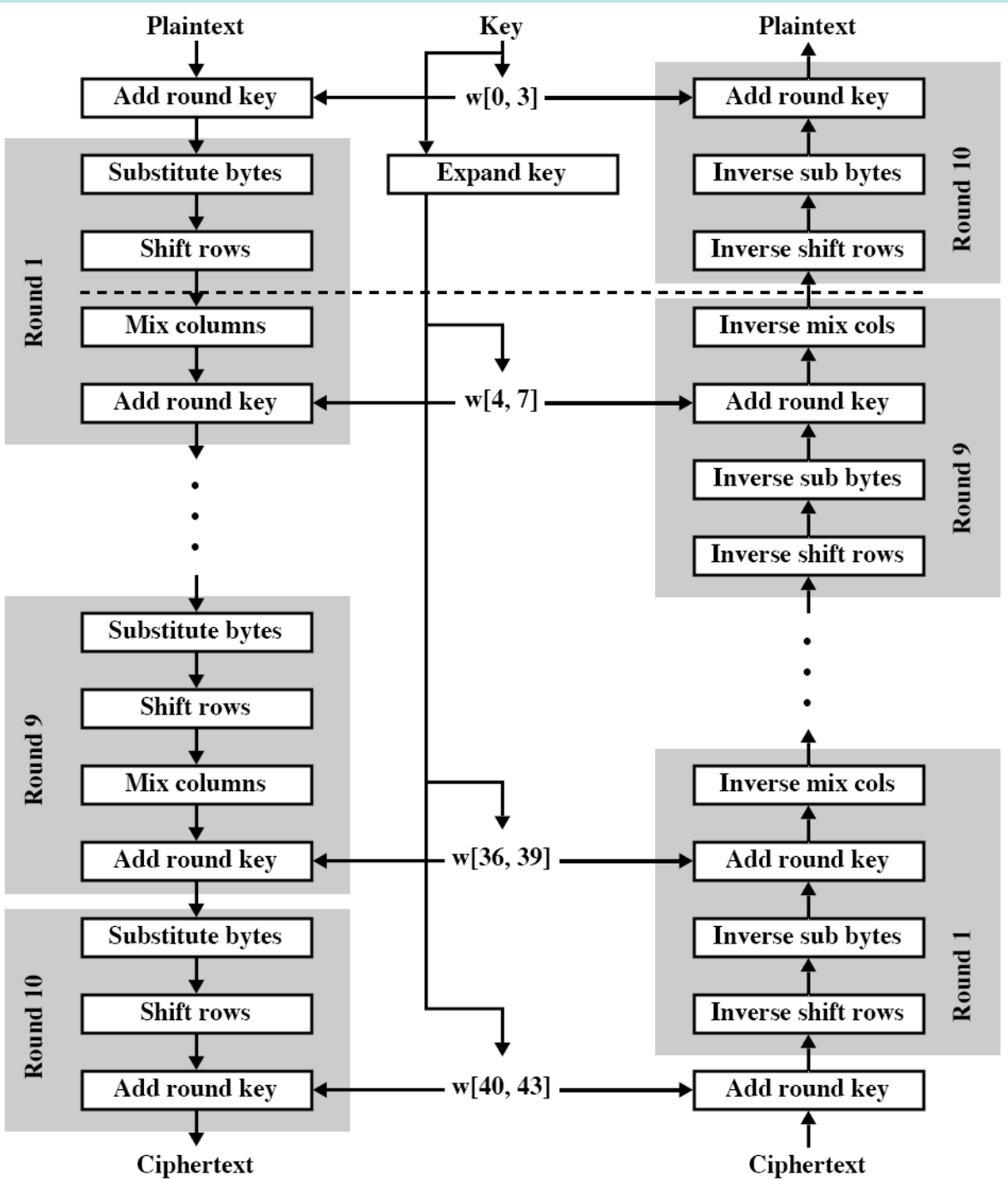
AES Design Features

- Only the Add Key stage makes use of the key
  - The other 3 stages (Shift Row, Mix Column, Nibble Substitution) provide confusion and diffusion of bits. On their own, they provide no security (do not use key)
- The four operations are easily reversible (for decryption)
- Encryption and decryption algorithms not identical
- Final round is only 3 operations, so algorithm is reversible
- S-Box design aims:
  - Low correlation between input bits and output bits
  - Cannot describe output as simple function of input
  - No fixed or opposite points, for example S-box(a) ≠ a
- Mix columns and shift rows ensure all output bits depend on all input bits after several rounds
- In Mix Columns, encryption more efficient than decryption
  - Only encryption used CFB/OFB modes for block ciphers and for message authentication
- Very efficient implementations for 8- and 32-bit processors

AES Parameters

Key size (words/bytes/bits)	4/16/128	6/24/192	8/32/256
Plaintext block size (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Number of rounds	10	12	14
Round key size (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Expanded key size (words/bytes)	44/176	52/208	60/240

AES Encryption and Decryption



AES Encryption Round