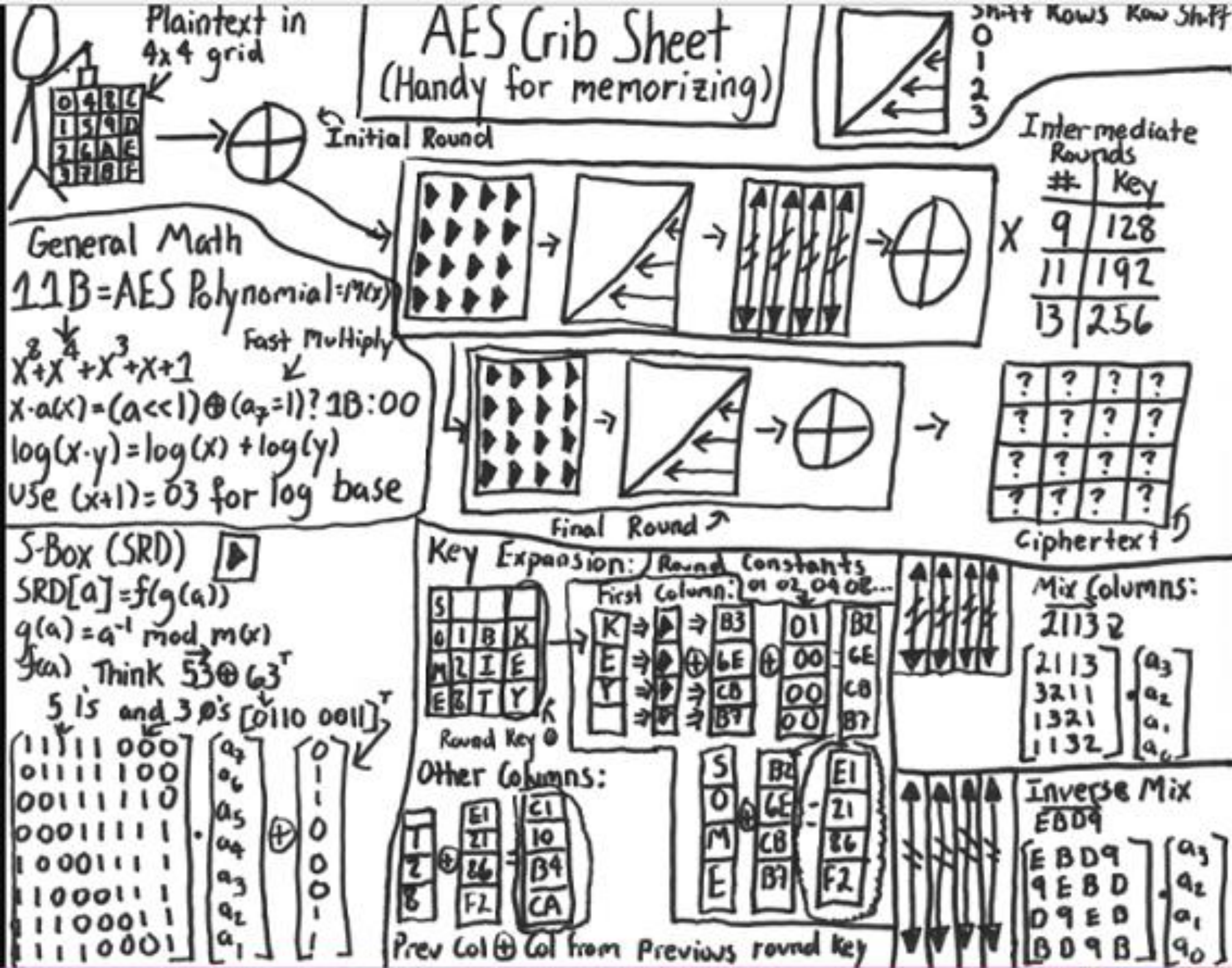


Chapter 6

Advanced Encryption Standard

Outline

- AES: introduction
- AES parameters
- AES Encryption
  - Overview
  - Data structures
  - Round functions
  - Key Expansion
- Decryption
- Implementation

Using slides from "Understanding Cryptography, by Christof Paar and Jan Pelzl, www.crypto-textbook.com"

AES: introduction

Some Basic Facts

- AES is the most widely used symmetric cipher today
- The algorithm for AES was chosen by the US *National Institute of Standards and Technology* (NIST) in a multi-year selection process
- The requirements for all AES candidate submissions were:
  - Block cipher with **128-bit block size**
  - **Three supported key lengths**: 128, 192 and 256 bit
  - Security relative to other submitted algorithms
  - **Efficiency** in software and hardware

Chronology of the AES Selection

- The need for a new block cipher announced by NIST in January, 1997
- 15 candidates algorithms accepted in August, 1998
- 5 finalists announced in August, 1999:
  - *Mars* – IBM Corporation
  - *RC6* – *RSA* Laboratories
  - *Rijndael* – J. Daemen & V. Rijmen
  - *Serpent* – Eli Biham et al.
  - *Twofish* – B. Schneier et al.
- In October 2000, *Rijndael* was chosen as the AES
- AES was formally approved as a US federal standard in November 2001

Rijndael (pronounced **rain-dahl**) is named after its two creators:
Vincent **Rij**men and Joan **Dae**men

Finite Field Arithmetic

- In the Advanced Encryption Standard (AES) all operations are performed on 8-bit bytes
  - i.e. byte operations

- The arithmetic operations of addition, multiplication, and division are performed over the finite field $GF(2^8)$
  - A field is a set in which we can do addition, subtraction, multiplication, and division without leaving the set
  - Division is defined with the following rule:
    - $a / b = a (b^{-1})$

- An example of a finite field (one with a finite number of elements) is the set Z_p consisting of all the integers $\{0, 1, \ldots, p - 1\}$, where p is a prime number and in which arithmetic is carried out modulo p

Finite Field Arithmetic: review

If one of the operations used in the algorithm is division, then we need to work in arithmetic defined over a field

- Division requires that each nonzero element have a multiplicative inverse

For convenience and for implementation efficiency we would like to work with integers that fit exactly into a given number of bits with no wasted bit patterns

- Integers in the range 0 through $2^n - 1$, which fit into an *n*-bit word

The set of such integers, Z_{2^n}, using modular arithmetic, is not a field

- For example, the integer 2 has no multiplicative inverse in Z_{2^n}, that is, there is no integer *b*, such that $2b \bmod 2^n = 1$

A finite field containing 2^n elements is referred to as $GF(2^n)$

- Every polynomial in $GF(2^n)$ can be represented by an n-bit number

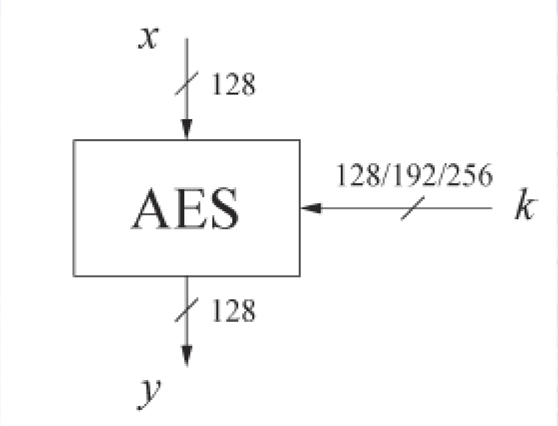
AES vs. DES

	DES	AES
Structure	Feistel	permutation-substitution-network
Key Size (s)	56 bits	128 , 192 or 256 bits
Number of Rounds	16	10, 12, 14
Block size	64 bits	128 bits
Security	Proven inadequate Breakable Small key size	Considered secure Unbreakable Large key size

AES Has Larger Block Size, Larger Key Size and Better Round Functions

AES Parameters

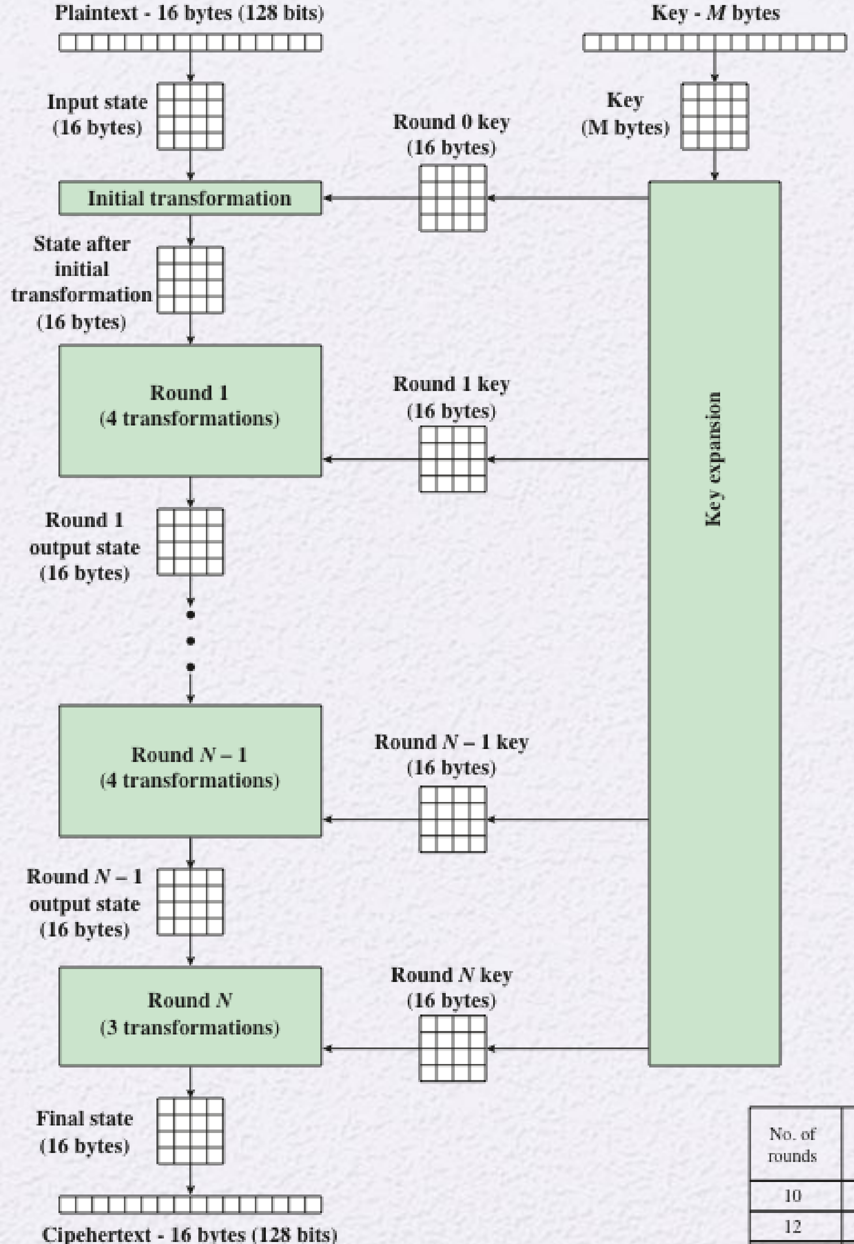
- Structure: permutation-substitution-network (PSN)
- Key sizes: 128 , 192 or 256 bits
  - Number of rounds (depends on key size): 10, 12 or 14
  - Key is expanded to: [Number_of_Rounds+1] × 4 words
- Block size (input and output): 128 bits
- Our discussion will focus on 128-bit key (i.e. 10-round algorithm)



	128-bit key 10 Rounds	192-bit key 12 Rounds	256-bit key 14 Rounds
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 Overview

- Key expansions
- ***N*** rounds (+initial transformation)
  - N is 10, 12 or 14
- Round includes four stages: 1 permutation and 3 substitutions.
  - Substitute bytes: Uses an S-box to perform a byte-by-byte substitution of the block
  - ShiftRows: A simple permutation
  - MixColumns: A substitution that makes use of arithmetic over GF(2^8)
  - AddRoundKey: A simple bitwise XOR of the current block with a portion of the expanded key
- Once it is established that all four stages are reversible.

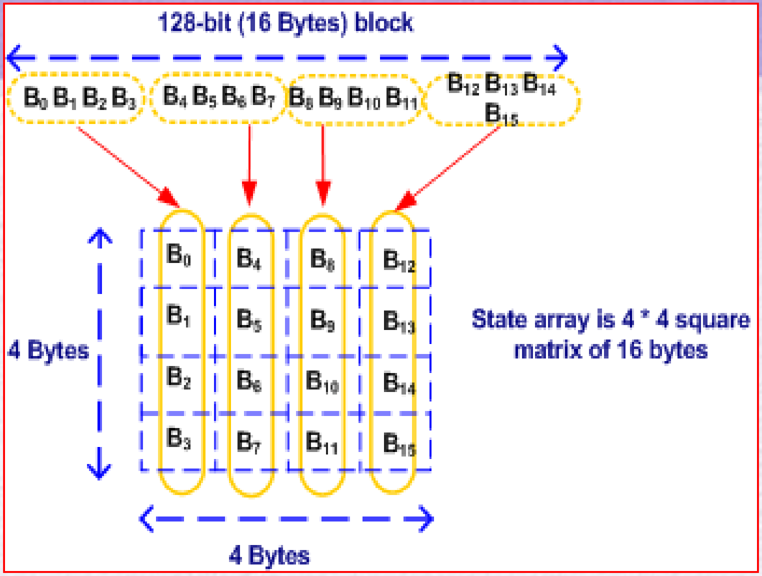


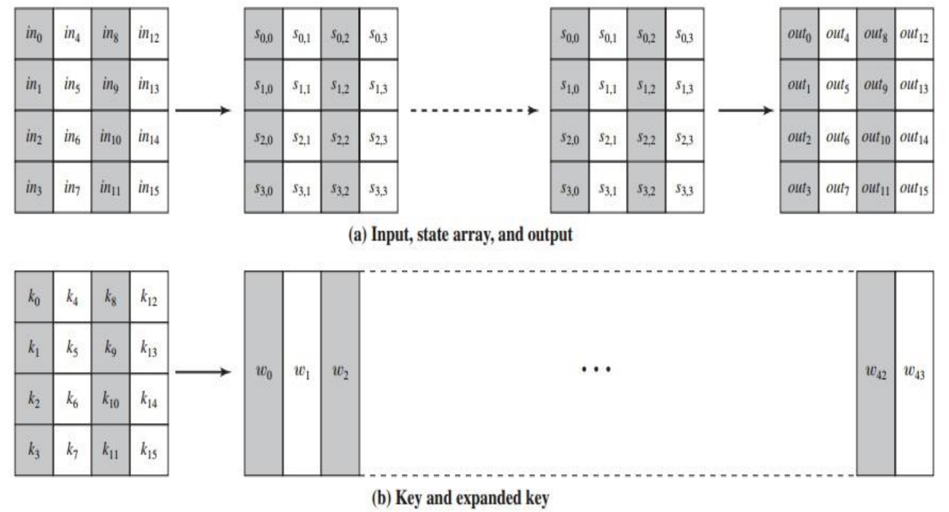
No. of rounds	Key Length (bytes)
10	16
12	24
14	32

Figure 6.1 AES Encryption Process

Data Structure: Blocks and States

- Input and outputs are 128-bit blocks of data.
- Algorithm is based on state array of 4x4 bytes.
- Input is copied to state array, then processed.
- Final state array is copied to output.
- Key is expanded to linear array of 32-bit (4-byte) words.



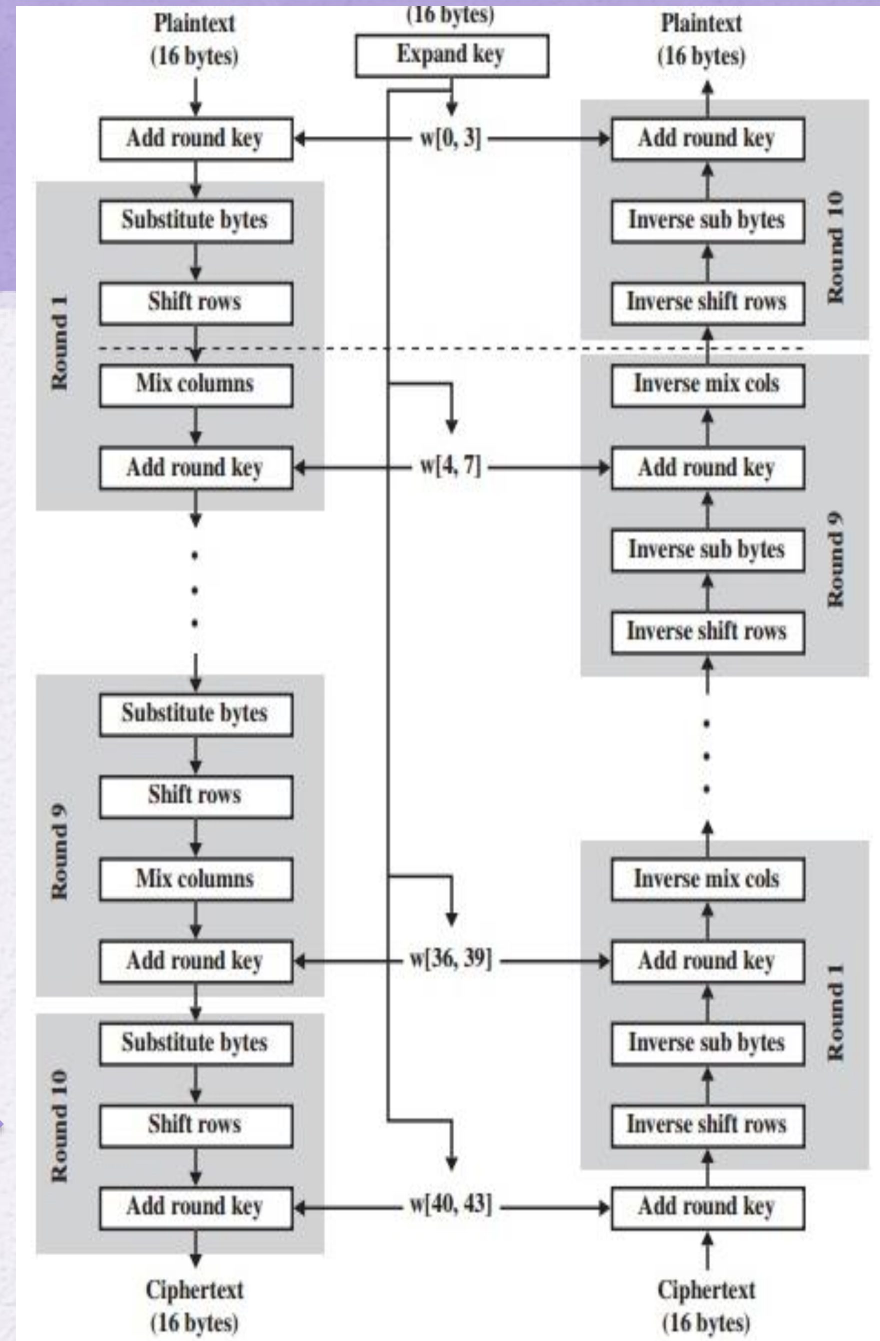


Data Structures: (a) input/output/state array (b) key and expanded key

Encryption/Decryption

- AES is **reversible**
- Decrypt reverses steps of encryption

Last round:
No Mix Columns



Encrypt **Decrypt**

10

AES Round-Transformation Functions

- There are 4 Round Transformation Functions:
  1. Substitute Bytes (**SubBytes**) Transformation
     - uses an S-box to perform a byte-by-byte substitution of the block
  2. **ShiftRows** Transformation
     - a simple permutation
  3. **MixColumns** Transformation
     - a substitution that makes use of arithmetic over $GF(2^8)$
  4. **AddRoundKey** Transformation
     - a simple bitwise XOR of the current block with a portion of the expanded key

- All functions has two flavors:
- FORWARD TRANSFORMATION (for encryption)
- INVERSE TRANSFORMATION (for decryption)

S-Box Rationale

- The S-box is designed to be resistant to known cryptanalytic attacks
- The Rijndael developers sought a design that has a low correlation between input bits and output bits and the property that the output is not a linear mathematical function of the input
- The nonlinearity is due to the use of the multiplicative inverse

Shift Row Rationale

- More substantial than it may first appear
- The State, as well as the cipher input and output, is treated as an array of four 4-byte columns
- On encryption, the first 4 bytes of the plaintext are copied to the first column of State, and so on
- The round key is applied to State column by column
  - Thus, a row shift moves an individual byte from one column to another, which is a linear distance of a multiple of 4 bytes
- Transformation ensures that the 4 bytes of one column are spread out to four different columns

Mix Columns Rationale

- Coefficients of a matrix based on a linear code with maximal distance between code words ensures a good mixing among the bytes of each column
- The mix column transformation combined with the shift row transformation ensures that after a few rounds all output bits depend on all input bits

Inputs for Single Round

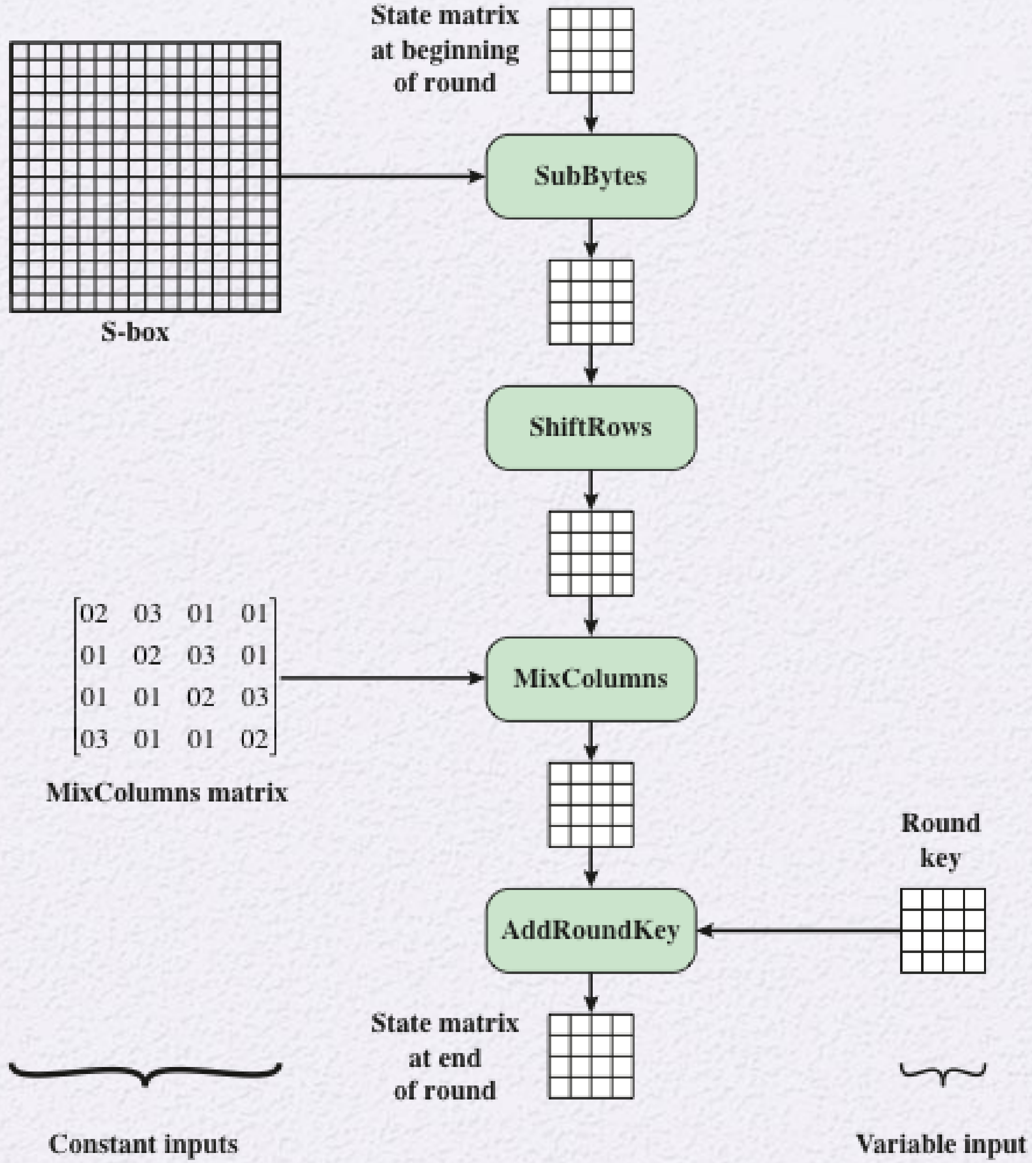


Figure 6.8 Inputs for Single AES Round

Single Round Functions

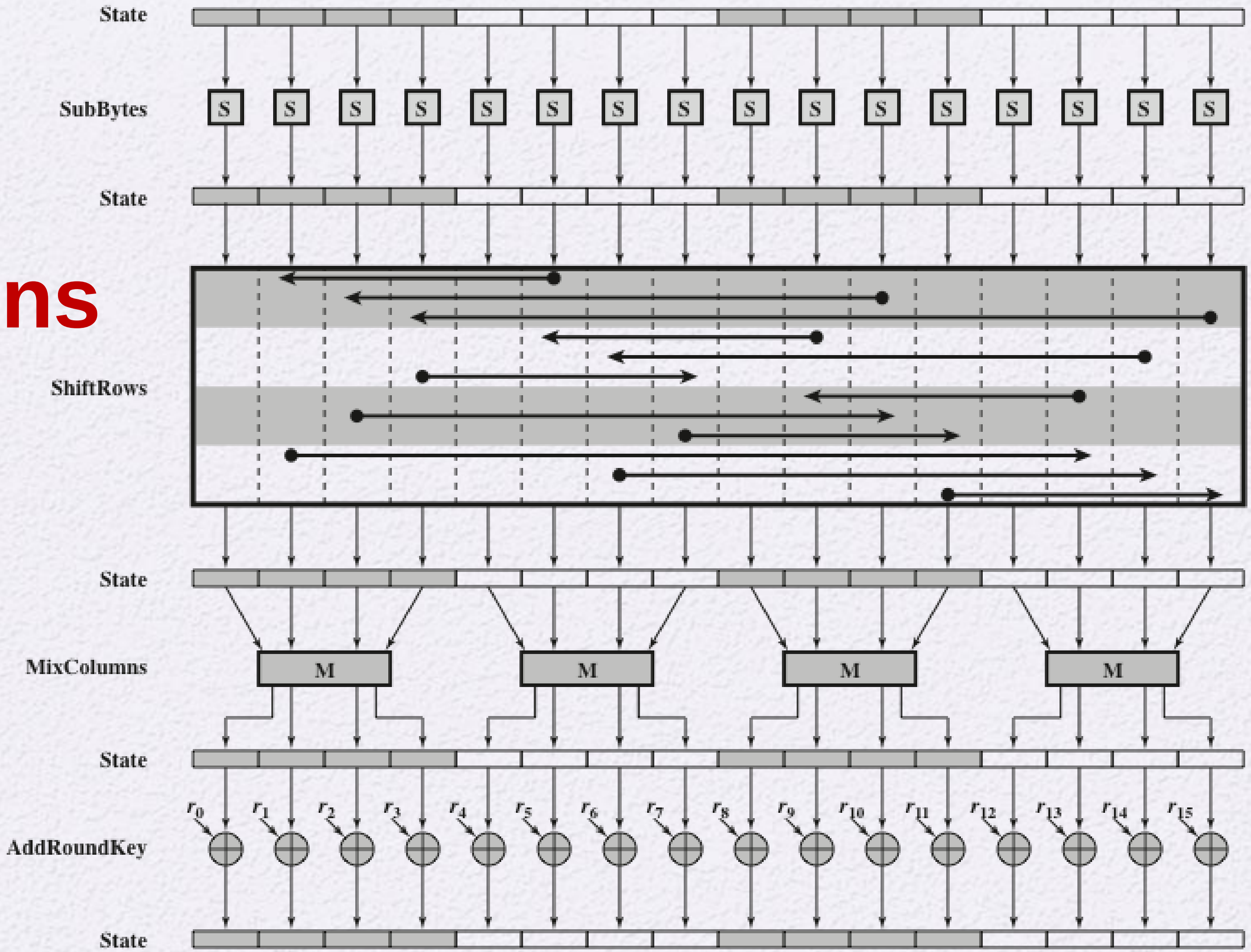
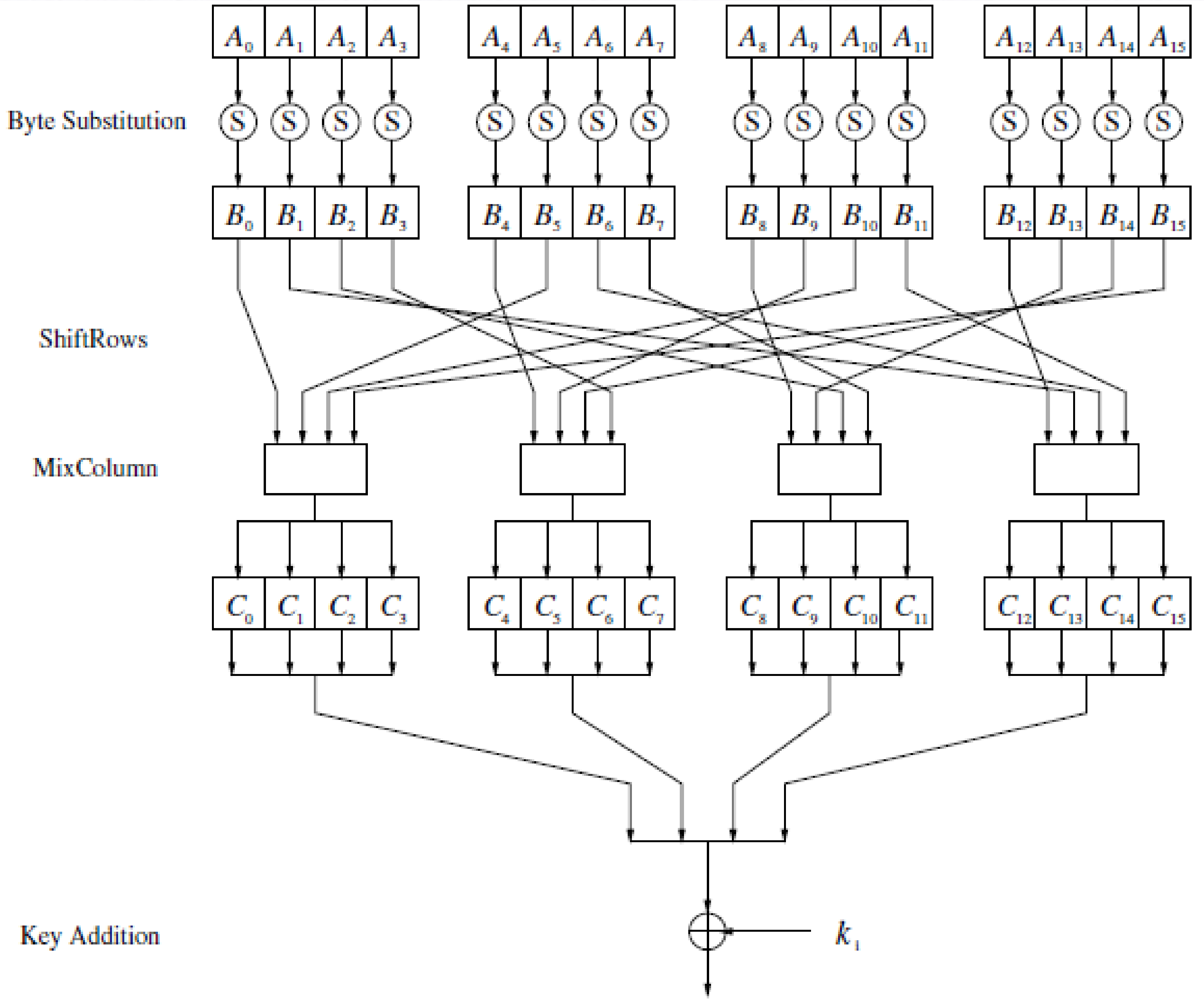
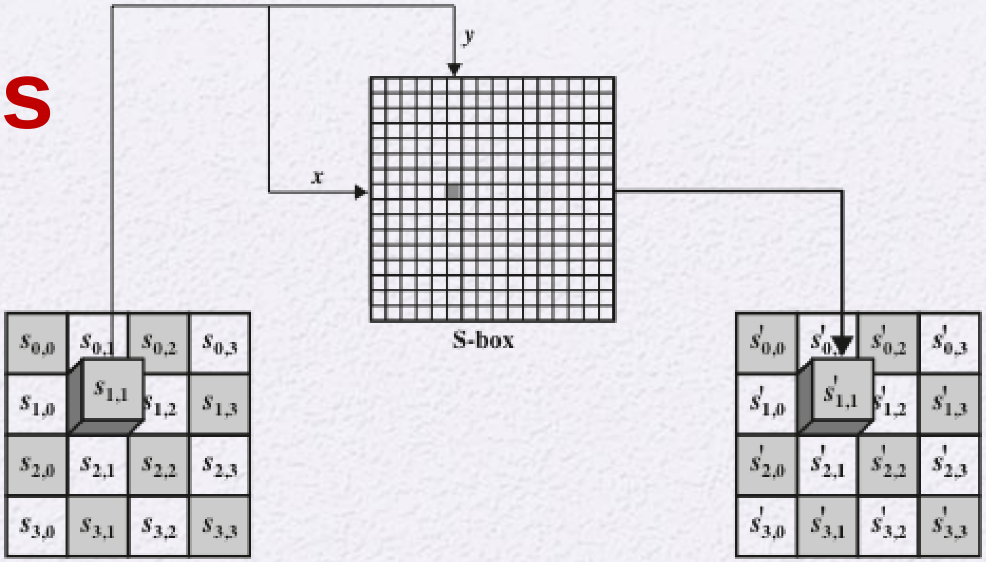


Figure 6.4 AES Encryption Round

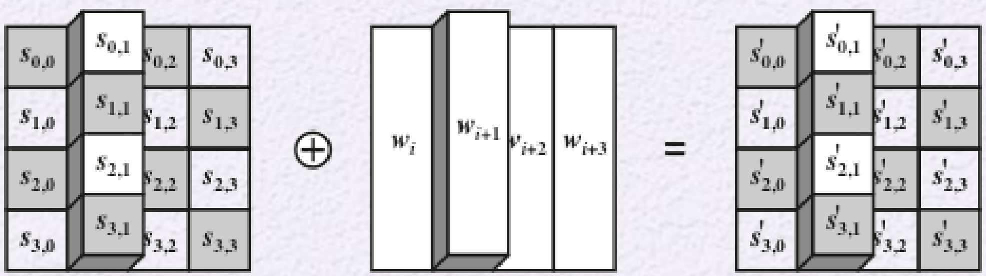
Single Round Functions



Operations are Byte-level



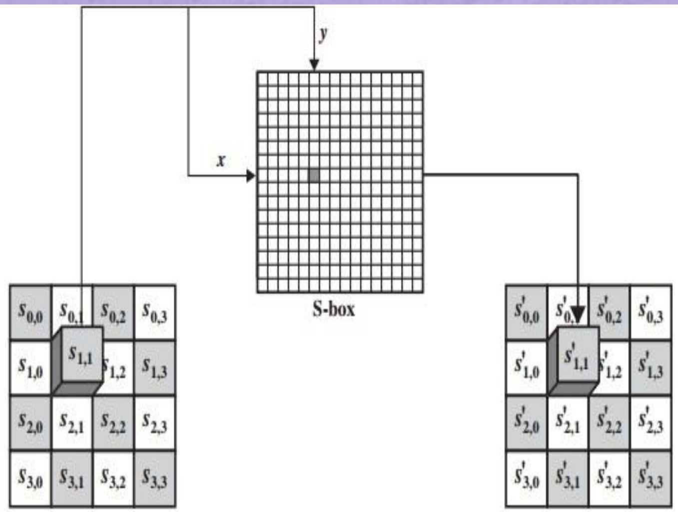
(a) Substitute byte transformation



(b) Add round key Transformation

Figure 6.5 AES Byte-Level Operations

1. SubBytes Transformation



Substitute Byte Transformation

	x \ y	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
x	0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
	1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
	2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
	3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
	4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
	5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
	6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
	7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
	8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
	9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
	A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
	B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
	C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
	D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
	E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
	F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

(a) S-box

S-box

EA	04	65	85
83	45	5D	96
5C	33	98	B0
F0	2D	AD	C5

→

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

S-box is designed to have following properties:

- Low correlation between input bits and output bits
- Output is not a linear mathematical function of input
- No self-inverse.
    - Example : S (a) ≠ IS (a)
- Invertible.
    - Example: IS [S (a)] = a

S-box and IS-box

S-box

ES S-Boxes

x \ y	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

(a) S-box

IS-box

x \ y	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	52	09	6A	D5	30	36	A5	38	BF	40	A3	9E	81	F3	D7	FB
1	7C	E3	39	82	9B	2F	FF	87	34	8E	43	44	C4	DE	E9	CB
2	54	7B	94	32	A6	C2	23	3D	EE	4C	95	0B	42	FA	C3	4E
3	08	2E	A1	66	28	D9	24	B2	76	5B	A2	49	6D	8B	D1	25
4	72	F8	F6	64	86	68	98	16	D4	A4	5C	CC	5D	65	B6	92
5	6C	70	48	50	FD	ED	B9	DA	5E	15	46	57	A7	8D	9D	84
6	90	D8	AB	00	8C	BC	D3	0A	F7	E4	58	05	B8	B3	45	06
7	D0	2C	1E	8F	CA	3F	0F	02	C1	AF	BD	03	01	13	8A	6B
8	3A	91	11	41	4F	67	DC	EA	97	F2	CF	CE	F0	B4	E6	73
9	96	AC	74	22	E7	AD	35	85	E2	F9	37	E8	1C	75	DF	6E
A	47	F1	1A	71	1D	29	C5	89	6F	B7	62	0E	AA	18	BE	1B
B	FC	56	3E	4B	C6	D2	79	20	9A	DB	C0	FE	78	CD	5A	F4
C	1F	DD	A8	33	88	07	C7	31	B1	12	10	59	27	80	EC	5F
D	60	51	7F	A9	19	B5	4A	0D	2D	E5	7A	9F	93	C9	9C	EF
E	A0	E0	3B	4D	AE	2A	F5	B0	C8	EB	BB	3C	83	53	99	61
F	17	2B	04	7E	BA	77	D6	26	E1	69	14	63	55	21	0C	7D

(b) Inverse S-box

S(EA) = 87

IS (87) = EA

S-box Generation

- How to generate S-box
- How S(C2)=25?
- Computation is done in two stages:
  - $GF(2^8)$ inverse
  - Affine mapping

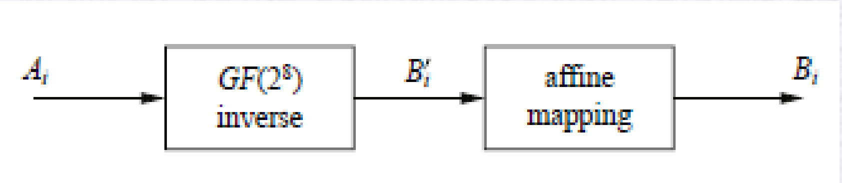
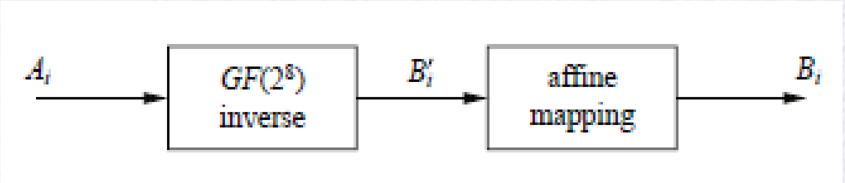


Table 4.2 Multiplicative inverse table in $GF(2^8)$ for bytes *xy* used within the AES S-Box

X \ Y	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	00	01	8D	F6	CB	52	7B	D1	E8	4F	29	C0	B0	E1	E5	C7
1	74	B4	AA	4B	99	2B	60	5F	58	3F	FD	CC	FF	40	EE	B2
2	3A	6E	5A	F1	55	4D	A8	C9	C1	0A	98	15	30	44	A2	C2
3	2C	45	92	6C	F3	39	66	42	F2	35	20	6F	77	BB	59	19
4	1D	FE	37	67	2D	31	F5	69	A7	64	AB	13	54	25	E9	09
5	ED	5C	05	CA	4C	24	87	BF	18	3E	22	F0	51	EC	61	17
6	16	5E	AF	D3	49	A6	36	43	F4	47	91	DF	33	93	21	3B
7	79	B7	97	85	10	B5	BA	3C	B6	70	D0	06	A1	FA	81	82
8	83	7E	7F	80	96	73	BE	56	9B	9E	95	D9	F7	02	B9	A4
9	DE	6A	32	6D	D8	8A	84	72	2A	14	9F	88	F9	DC	89	9A
A	FB	7C	2E	C3	8F	B8	65	48	26	C8	12	4A	CE	E7	D2	62
B	0C	E0	1F	EF	11	75	78	71	A5	8E	76	3D	BD	BC	86	57
C	0B	28	2F	A3	DA	D4	E4	0F	A9	27	53	04	1B	FC	AC	E6
D	7A	07	AE	63	C5	DB	E2	EA	94	8B	C4	D5	9D	F8	90	6B
E	B1	0D	D6	EB	C6	0E	CF	AD	08	4E	D7	E3	5D	50	1E	B3
F	5B	23	38	34	68	46	03	8C	DD	9C	7D	A0	CD	1A	41	1C

S-box Generation

- How to generate S-box
- How $S(C2_{HEX})=25_{HEX}$?
- Computation is done in two stages:
  - $GF(2^8)$ inverse
  - Affine mapping



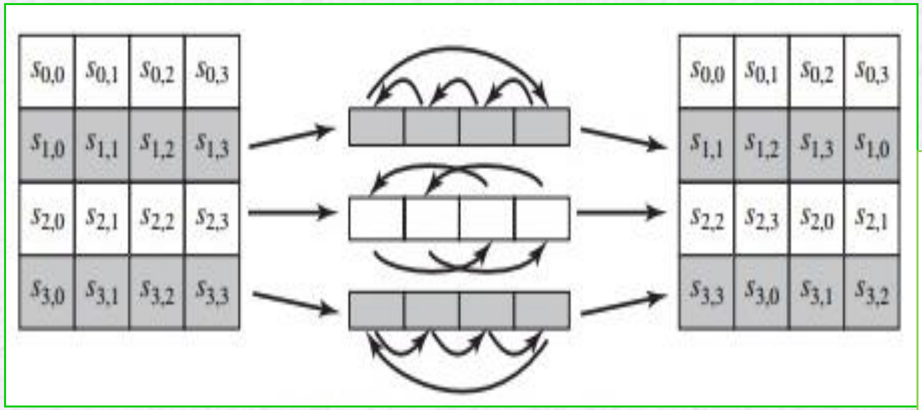
$$\begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{pmatrix} \equiv \begin{pmatrix} 1&0&0&0&1&1&1&1 \\ 1&1&0&0&0&1&1&1 \\ 1&1&1&0&0&0&1&1 \\ 1&1&1&1&0&0&0&1 \\ 1&1&1&1&1&0&0&0 \\ 0&1&1&1&1&1&0&0 \\ 0&0&1&1&1&1&1&0 \\ 0&0&0&1&1&1&1&1 \end{pmatrix} \begin{pmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} \bmod 2$$

- Example: let us compute $S(C2)$
  - $B'=F2_{HEX}$
  - $B=25_{HEX}$

2. ShiftRows Transformation

- ShiftRows performs left rotations on the bytes of each row as follows:
  - First row: nothing
  - Second row: rotate-left(1) ; **note: rotate-left (1) ≡ rotate-right(3)**
  - Third row: rotate-left(2) ; **note: rotate-left (2) ≡ rotate-right(2)**
  - Fourth row: rotate-left(3) ; **note: rotate-left (3) ≡ rotate-right(1)**

- So, ShiftRows moves an individual byte from one column to another.



Example

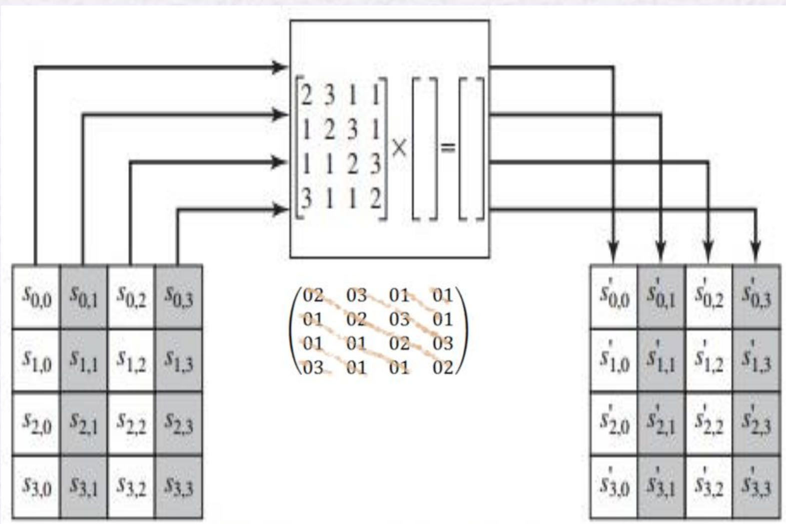
87	F2	4D	97
EC	6E	4C	90
4A	C3	46	E7
8C	D8	95	A6

→

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

3. MixColumns

- MixColumns, operates on each column individually.
- Each byte of a column is mapped into a new value that is a function of all four bytes in that column.



$$s'_{0,j} = (2 \cdot s_{0,j}) \oplus (3 \cdot s_{1,j}) \oplus s_{2,j} \oplus s_{3,j}$$
$$s'_{1,j} = s_{0,j} \oplus (2 \cdot s_{1,j}) \oplus (3 \cdot s_{2,j}) \oplus s_{3,j}$$
$$s'_{2,j} = s_{0,j} \oplus s_{1,j} \oplus (2 \cdot s_{2,j}) \oplus (3 \cdot s_{3,j})$$
$$s'_{3,j} = (3 \cdot s_{0,j}) \oplus s_{1,j} \oplus s_{2,j} \oplus (2 \cdot s_{3,j})$$

Example

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

$$\begin{pmatrix} 47 \\ 37 \\ 94 \\ ED \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \cdot \begin{pmatrix} 87 \\ 6E \\ 46 \\ A6 \end{pmatrix}$$

$$\begin{array}{llllll}
(\{02\} \cdot \{87\}) & \oplus (\{03\} \cdot \{6E\}) & \oplus \{46\} & \oplus \{A6\} & = \{47\} \\
\{87\} & \oplus (\{02\} \cdot \{6E\}) & \oplus (\{03\} \cdot \{46\}) & \oplus \{A6\} & = \{37\} \\
\{87\} & \oplus \{6E\} & \oplus (\{02\} \cdot \{46\}) & \oplus (\{03\} \cdot \{A6\}) & = \{94\} \\
(\{03\} \cdot \{87\}) & \oplus \{6E\} & \oplus \{46\} & \oplus (\{02\} \cdot \{A6\}) & = \{ED\}
\end{array}$$

For the first equation, we have $\{02\} \cdot \{87\} = (0000\ 1110) \oplus (0001\ 1011) = (0001\ 0101)$ and $\{03\} \cdot \{6E\} = \{6E\} \oplus (\{02\} \cdot \{6E\}) = (0110\ 1110) \oplus (1101\ 1100) = (1011\ 0010)$. Then,

$$\begin{array}{lcl}
\{02\} \cdot \{87\} & = & 0001\ 0101 \\
\{03\} \cdot \{6E\} & = & 1011\ 0010 \\
\{46\} & = & 0100\ 0110 \\
\{A6\} & = & \underline{1010\ 0110} \\
 & & 0100\ 0111 = \{47\}
\end{array}$$

MixColumns Computations

- Computations follows $GF(2^8)$
- For results that have more than 8 bits (i.e., x^8 or lager), use irreducible polynomial:
  - $x^8+x^4+x^3+x+1$
  - Which maps to: $11B_{HEX}$

$\{02\} \bullet \{87\} = \{15\}$

$\{02\}$ corresponds to : $f1(x) = x$

$\{87\}$ corresponds to : $f2(x) = x^7 + x^2 + x + 1$

$\{02\} \bullet \{87\} = f1(x) \bullet f2(x) = x^8 + x^3 + x^2 + x$

$f1(x) \bullet f2(x) \mod(m(x)) = x^4 + x^2 + 1 = \{15\}$

$\{02\} \bullet \{87\}$	=	0001 0101
$\{03\} \bullet \{6E\}$	=	1011 0010
$\{46\}$	=	0100 0110
$\{A6\}$	=	1010 0110
		0100 0111 = { 47}

```
  1000  0111  {87}
  0000  0010  {02}
 -------------
1 0000  1110   result
1 0001  1011   mod (11B)
 -------------
0 0001  0101   {15}
```

```
  0110  1110  {6E}
  0000  0011  {03}
 -------------
  1011  0010  {B2}
```

Review of FG(2^8) Mathematics

- AES uses special polynomials in GF(2^8)

Operation	Description	Example
Addition	bitwise XOR	
Multip. by 02: {02} • {B}	• 1-bit left shift • Followed by a conditional bitwise XOR with (0001 1011) if the leftmost bit of the original value (prior to the shift) is 1.	{02} • {87} = (0000 1110) ⊕(0001 1011) = (0001 0101) = {15}
{03} • {B}	{03} • {B} = {B} ⊕ ({02} • {B})	{03} • {6E} ={6E} ⊕ ({02} • {6E}) =(0110 1110) ⊕ (1101 1100) = (1011 0010) = {B2}

Explaining Calculation in Finite Field GF(2^8)

- AES uses arithmetic in finite field GF(2^8)
  - Polynomial based math.
  - Polynomial are expressed as binary
    - $m(x) = x^8 + x^4 + x^3 + x + 1$ (expression)
    - $m(x) = 1\ 0001\ 1011 = 11B_{HEX}$ (binary/Hex)
  - Add/Sub : XOR operation
  - Multiply : AND operation
- In GF(2^8) field:
  - Additions and multiplications are performed on polynomials
  - Polynomials are multiplied /added,
  - Then divided by m(x) to compute remainder (i.e., modulus operation)
    - $m(x) = x^8 + x^4 + x^3 + x + 1$

MixColumns: Encryption and Decryption

- Encryption:

$$\mathrm{MixColumn}(B) = C$$

$$\begin{pmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} B_0 \\ B_5 \\ B_{10} \\ B_{15} \end{pmatrix}$$

- Decryption:

$$\mathrm{InverseMixColumn}(C) = B$$

$$\begin{pmatrix} B_0 \\ B_1 \\ B_2 \\ B_3 \end{pmatrix} = \begin{pmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{pmatrix} \begin{pmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \end{pmatrix}$$

MixColumns: Encryption and Decryption

- Encryption

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

$$\begin{pmatrix} 47 \\ 37 \\ 94 \\ ED \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \cdot \begin{pmatrix} 87 \\ 6E \\ 46 \\ A6 \end{pmatrix}$$

$$\begin{aligned}
(\{02\}\bullet\{87\}) \oplus (\{03\}\bullet\{6E\}) \oplus \{46\} \oplus \{A6\} &= \{47\} \\
\{87\} \oplus (\{02\}\bullet\{6E\}) \oplus (\{03\}\bullet\{46\}) \oplus \{A6\} &= \{37\} \\
\{87\} \oplus \{6E\} \oplus (\{02\}\bullet\{46\}) \oplus (\{03\}\bullet\{A6\}) &= \{94\} \\
(\{03\}\bullet\{87\}) \oplus \{6E\} \oplus \{46\} \oplus (\{02\}\bullet\{A6\}) &= \{ED\}
\end{aligned}$$

For the first equation, we have $\{02\}\bullet\{87\} = (0000\ 1110) \oplus (0001\ 1011) = (0001\ 0101)$ and $\{03\}\bullet\{6E\} = \{6E\} \oplus (\{02\}\bullet\{6E\}) = (0110\ 1110) \oplus (1101\ 1100) = (1011\ 0010)$. Then,

$$\begin{aligned}
\{02\}\bullet\{87\} &= 0001\ 0101 \\
\{03\}\bullet\{6E\} &= 1011\ 0010 \\
\{46\} &= 0100\ 0110 \\
\{A6\} &= \underline{1010\ 0110} \\
& \ 0100\ 0111 = \{47\}
\end{aligned}$$

- Decryption

InverseMixColumn (C) =*B*

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

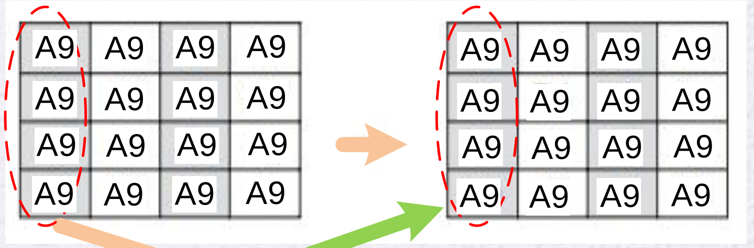
87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

$$\begin{pmatrix} 87 \\ 6E \\ 46 \\ A6 \end{pmatrix} = \begin{pmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{pmatrix} \cdot \begin{pmatrix} 47 \\ 37 \\ 94 \\ ED \end{pmatrix}$$

{0E}.{47}=87 ➔ 1 0 0 0 0 1 1 1
{0B}.{37}=FA ➔ 1 1 1 1 1 0 1 0
{0D}.{94}=3E ➔ 0 0 1 1 1 1 1 0
{09}.{ED}]=C4➔ 1 1 0 0 0 1 0 0
----
1 0 0 0 0 1 1 1 ➔ 87

MixColumns: One Issue You Should Know

- If all state bytes are the same, then applying MixComlumns step will produce the same state!
- Why? Because XOR operation cancels identical terms:
  - {03}.{A9} cancels {02}{A9} and {01}{A9}
  - there is one term left {01}.{A9}={A9}



$$\begin{pmatrix} A9 \\ A9 \\ A9 \\ A9 \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \cdot \begin{pmatrix} A9 \\ A9 \\ A9 \\ A9 \end{pmatrix}$$

4. AddRoundKey Transformation

- AddRoundKey is byte-leve XOR-ing between state array and round key

128-bit state | **128-bit key**

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

$\oplus$

AC	19	28	57
77	FA	D1	5C
66	DC	29	00
F3	21	41	6A

=

EB	59	8B	1B
40	2E	A1	C3
F2	38	13	42
1E	84	E7	D6

AddRoundKey Transformation

- The 128 bits of State are bitwise XORed with the 128 bits of the round key
- Operation is viewed as a columnwise operation between the 4 bytes of a State column and one word of the round key
  - Can also be viewed as a byte-level operation

Rationale:

Is as simple as possible and affects every bit of State

The complexity of the round key expansion plus the complexity of the other stages of AES ensure security

AES Key Expansion

- Takes as input a four-word (16 byte) key and produces a linear array of 44 words (176) bytes
  - This is sufficient to provide a four-word round key for the initial AddRoundKey stage and each of the 10 rounds of the cipher
- Key is copied into the first four words of the expanded key
  - The remainder of the expanded key is filled in four words at a time
- Each added word *w*[i] depends on the immediately preceding word, *w[i – 1]*, and the word four positions back, w[i – 4]
  - In three out of four cases a simple XOR is used
  - For a word whose position in the *w* array is a multiple of 4, a more complex function is used

Key Expansion Rationale

- The Rijndael developers designed the expansion key algorithm to be resistant to known cryptanalytic attacks
- Inclusion of a round-dependent round constant eliminates the symmetry between the ways in which round keys are generated in different rounds

The specific criteria that were used are:

- Knowledge of a part of the cipher key or round key does not enable calculation of many other round-key bits
- An invertible transformation
- Speed on a wide range of processors
- Usage of round constants to eliminate symmetries
- Diffusion of cipher key differences into the round keys
- Enough nonlinearity to prohibit the full determination of round key differences from cipher key differences only
- Simplicity of description

Key Expansion

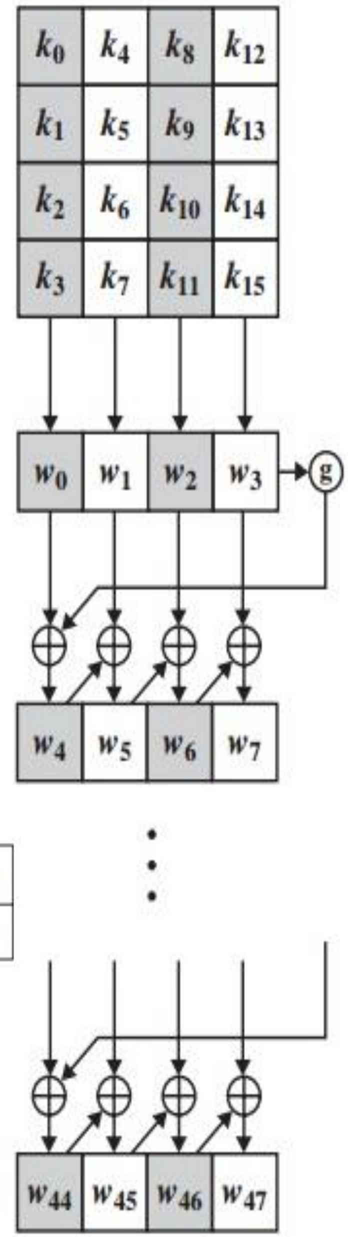
- The AES key expansion algorithm takes as **input** a four-word (16-byte) key and **outputs** a linear array of 44 words (176 bytes).
- This is sufficient to provide a four-word round key for the initial AddRoundKey stage and each of the 10 rounds of the cipher.

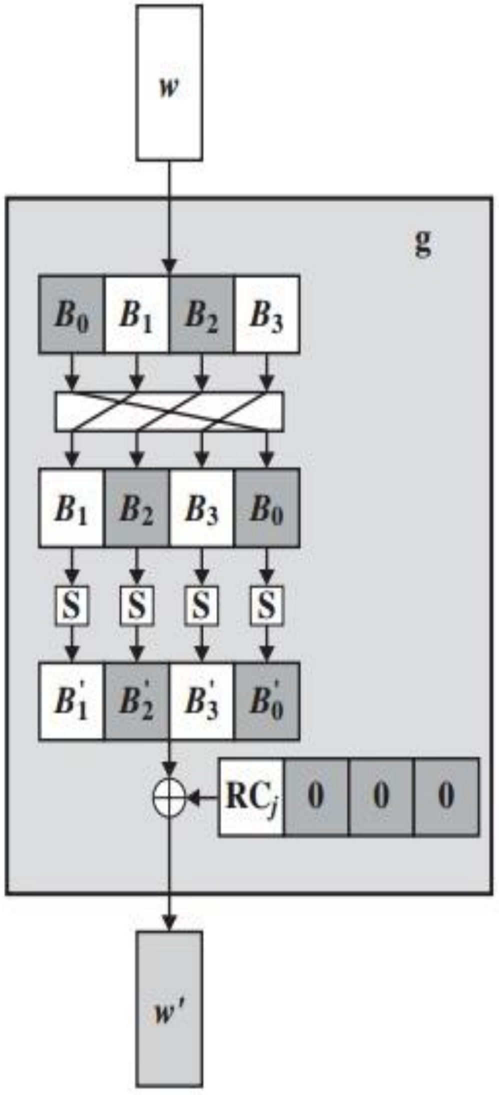
```
KeyExpansion (byte key[16], word w[44])
{
    word temp
    for (i = 0; i < 4; i++)    w[i] = (key[4*i], key[4*i+1],
                                       key[4*i+2],
                                       key[4*i+3]);
    for (i = 4; i < 44; i++)
    {
     temp = w[i - 1];
     if (i mod 4 = 0)    temp = SubWord (RotWord (temp))
                                  ⊕ Rcon[i/4];
     w[i] = w[i-4] ⊕ temp
    }
}
```

Key Expansion Algorithm

j	1	2	3	4	5	6	7	8	9	10
RC[j]	01	02	04	08	10	20	40	80	1B	36

RC$_j$ table

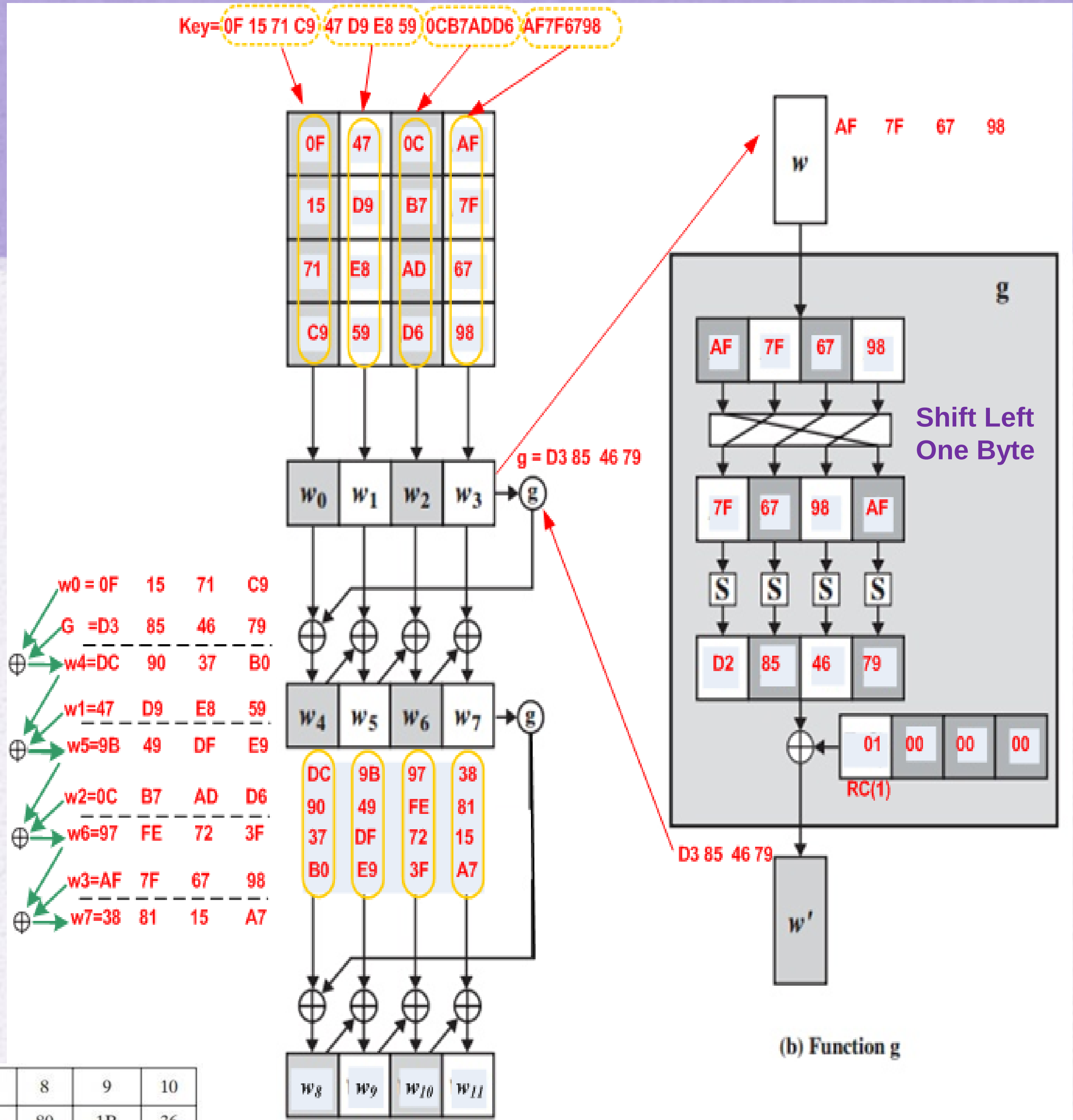




(b) Function g

g-function

Key Expansion: Example



j	1	2	3	4	5	6	7	8	9	10
RC[j]	01	02	04	08	10	20	40	80	1B	36

RC_j table

Key Expansion: Example

Key Words	Auxiliary Function
w0 = 0f 15 71 c9 w1 = 47 d9 e8 59 w2 = 0c b7 ad w3 = af 7f 67 98	RotWord(w3) = 7f 67 98 af = x1 SubWord(x1) = d2 85 46 79 = y1 Rcon(1) = 01 00 00 00 y1 ⊕ Rcon(1) = d3 85 46 79 = z1
w4 = w0 ⊕ z1 = dc 90 37 b0 w5 = w4 ⊕ w1 = 9b 49 df e9 w6 = w5 ⊕ w2 = 97 fe 72 3f w7 = w6 ⊕ w3 = 38 81 15 a7	RotWord(w7) = 81 15 a7 38 = x2 SubWord(x4) = 0c 59 5c 07 = y2 Rcon(2) = 02 00 00 00 y2 ⊕ Rcon(2) = 0e 59 5c 07 = z2
w8 = w4 ⊕ z2 = d2 c9 6b b7 w9 = w8 ⊕ w5 = 49 80 b4 5e w10 = w9 ⊕ w6 = de 7e c6 61 w11 = w10 ⊕ w7 = e6 ff d3 c6	RotWord(w11) = ff d3 c6 e6 = x3 SubWord(x2) = 16 66 b4 83 = y3 Rcon(3) = 04 00 00 00 y3 ⊕ Rcon(3) = 12 66 b4 8e = z3
w12 = w8 ⊕ z3 = c0 af df 39 w13 = w12 ⊕ w9 = 89 2f 6b 67 w14 = w13 ⊕ w10 = 57 51 ad 06 w15 = w14 ⊕ w11 = b1 ae 7e c0	RotWord(w15) = ae 7e c0 b1 = x4 SubWord(x3) = e4 f3 ba c8 = y4 Rcon(4) = 08 00 00 00 y4 ⊕ Rcon(4) = ec f3 ba c8 = 4

Key Words	Auxiliary Function
w16 = w12 ⊕ z4 = 2c 5c 65 f1 w17 = w16 ⊕ w13 = a5 73 0e 96 w18 = w17 ⊕ w14 = f2 22 a3 90 w19 = w18 ⊕ w15 = 43 8c dd 50	RotWord(w19) = 8c dd 50 43 = x5 SubWord(x4) = 64 c1 53 1a = y5 Rcon(5) = 10 00 00 00 y5 ⊕ Rcon(5) = 74 c1 53 1a = z5
w20 = w16 ⊕ z5 = 58 9d 36 eb w21 = w20 ⊕ w17 = fd ee 38 7d w22 = w21 ⊕ w18 = 0f cc 9b ed w23 = w22 ⊕ w19 = 4c 40 46 bd	RotWord (w23) = 40 46 bd 4c = x6 SubWord (x5) = 09 5a 7a 29 = y6 Rcon(6) = 20 00 00 00 y6 ⊕ Rcon(6) = 29 5a 7a 29 = z6
w24 = w20 ⊕ z6 = 71 c7 4c c2 w25 = w24 ⊕ w21 = 8c 29 74 bf w26 = w25 ⊕ w22 = 83 e5 ef 52 w27 = w26 ⊕ w23 = cf a5 a9 ef	RotWord (w27) = a5 a9 ef cf = x7 SubWord (x6) = 06 d3 bf 8a = y7 Rcon (7) = 40 00 00 00 y7 ⊕ Rcon(7) = 46 d3 df 8a = z7
w28 = w24 ⊕ z7 = 37 14 93 48 w29 = w28 ⊕ w25 = bb 3d e7 f7 w30 = w29 ⊕ w26 = 38 d8 08 a5 w31 = w30 ⊕ w27 = f7 7d a1 4a	RotWord (w31) = 7d a1 4a f7 = x8 SubWord (x7) = ff 32 d6 68 = y8 Rcon (8) = 80 00 00 00 y8 ⊕ Rcon(8) = 7f 32 d6 68 = z8
w32 = w28 ⊕ z8 = 48 26 45 20 w33 = w32 ⊕ w29 = f3 1b a2 d7 w34 = w33 ⊕ w30 = cb c3 aa 72 w35 = w34 ⊕ w32 = 3c be 0b 3	RotWord (w35) = be 0b 38 3c = x9 SubWord (x8) = ae 2b 07 eb = y9 Rcon (9) = 1B 00 00 00 y9 ⊕ Rcon (9) = b5 2b 07 eb = z9
w36 = w32 ⊕ z9 = fd 0d 42 cb w37 = w36 ⊕ w33 = 0e 16 e0 1c w38 = w37 ⊕ w34 = c5 d5 4a 6e w39 = w38 ⊕ w35 = f9 6b 41 56	RotWord (w39) = 6b 41 56 f9 = x10 SubWord (x9) = 7f 83 b1 99 = y10 Rcon (10) = 36 00 00 00 y10 ⊕ Rcon (10) = 49 83 b1 99 = z10
w40 = w36 ⊕ z10 = b4 8e f3 52 w41 = w40 ⊕ w37 = ba 98 13 4e w42 = w41 ⊕ w38 = 7f 4d 59 20 w43 = w42 ⊕ w39 = 86 26 18 76	

Detailed Calculations

Full AES Example (1)

Plaintext (input)				Key (input)				Ciphertext (output)			
01	89	FE	76	0F	47	0C	AF	FF	08	69	64
23	AB	DC	54	15	D9	B7	7F	0B	53	34	14
45	CD	BA	32	71	E8	AD	67	84	BF	AB	8F
67	EF	98	10	C9	59	D6	98	4A	7C	43	B9

String Representations	
Plaintext:	0123456789ABCDEFFEDCBA9876543210
Key:	0F1571C947D9E8590CB7ADD6AF7F6798
Ciphertext:	FF0B844A0853BF7C6934AB4364148FB9

	Start of Round				SubBytes				ShiftRows				MixColumns				AddRoundKey				Key Schedule				Round Constant
Round 0	**01**	**89**	**FE**	**76**													0E	CE	F2	D9	0F	47	0C	AF	
	23	**AB**	**DC**	**54**													36	72	6B	2B	15	D9	B7	7F	
	45	**CD**	**BA**	**32**													34	25	17	55	71	E8	AD	67	
	67	**EF**	**98**	**10**													AE	B6	4E	88	C9	59	D6	98	
Round 1	0E	CE	F2	D9	AB	8B	89	35	AB	8B	89	35	B9	94	57	75	65	0F	C0	4D	DC	9B	97	38	01
	36	72	6B	2B	05	40	7F	F1	40	7F	F1	05	E4	8E	16	51	74	C7	E8	D0	90	49	FE	81	
	34	25	17	55	18	3F	F0	FC	F0	FC	18	3F	47	20	9A	3F	70	FF	E8	2A	37	DF	72	15	
	AE	B6	4E	88	E4	4E	2F	C4	C4	E4	4E	2F	C5	D6	F5	3B	75	3F	CA	9C	B0	E9	3F	A7	
Round 2	65	0F	C0	4D	4D	76	BA	E3	4D	76	BA	E3	8E	22	DB	12	5C	6B	05	F4	D2	49	DE	E6	02
	74	C7	E8	D0	92	C6	9B	70	C6	9B	70	92	B2	F2	DC	92	7B	72	A2	6D	C9	80	7E	FF	
	70	FF	E8	2A	51	16	9B	E5	9B	E5	51	16	DF	80	F7	C1	B4	34	31	12	6B	B4	C6	D3	
	75	3F	CA	9C	9D	75	74	DE	DE	9D	75	74	2D	C5	1E	52	9A	9B	7F	94	B7	5E	61	C6	

Full AES Example (2)

	Start of Round				**SubBytes**				**ShiftRows**				**MixColumns**				**AddRoundKey**				**Key Schedule**				**Round Constant**
Round 3	5C	6B	05	F4	4A	7F	6B	BF	4A	7F	6B	BF	B1	C1	0B	CC	71	48	5C	7D	C0	89	57	B1	04
	7B	72	A2	6D	21	40	3A	3C	40	3A	3C	21	BA	F3	8B	07	15	DC	DA	A9	AF	2F	51	AE	
	B4	34	31	12	8D	18	C7	C9	C7	C9	8D	18	F9	1F	6A	C3	26	74	C7	BD	DF	6B	AD	7E	
	9A	9B	7F	94	B8	14	D2	22	22	B8	14	D2	1D	19	24	5C	24	7E	22	9C	39	67	06	C0	
Round 4	71	48	5C	7D	A3	52	4A	FF	A3	52	4A	FF	D4	11	FE	0F	F8	B4	0C	4C	2C	A5	F2	43	08
	15	DC	DA	A9	59	86	57	D3	86	57	D3	59	3B	44	06	73	67	37	24	FF	5C	73	22	8C	
	26	74	C7	BD	F7	92	C6	7A	C6	7A	F7	92	CB	AB	62	37	AE	A5	C1	EA	65	0E	A3	DD	
	24	7E	22	9C	36	F3	93	DE	DE	36	F3	93	19	B7	07	EC	E8	21	97	BC	F1	96	90	50	
Round 5	F8	B4	0C	4C	41	8D	FE	29	41	8D	FE	29	2A	47	C4	48	72	BA	CB	04	58	FD	0F	4C	10
	67	37	24	FF	85	9A	36	16	9A	36	16	85	83	E8	18	BA	1E	06	D4	FA	9D	EE	CC	40	
	AE	A5	C1	EA	E4	06	78	87	78	87	E4	06	84	18	27	23	B2	20	BC	65	36	38	9B	46	
	E8	21	97	BC	9B	FD	88	65	65	9B	FD	88	EB	10	0A	F3	00	6D	E7	4E	EB	7D	ED	BD	
Round 6	72	BA	CB	04	40	F4	1F	F2	40	F4	1F	F2	7B	05	42	4A	0A	89	C1	85	71	8C	83	CF	20
	1E	06	D4	FA	72	6F	48	2D	6F	48	2D	72	1E	D0	20	40	D9	F9	C5	E5	C7	29	E5	A5	
	B2	20	BC	65	37	B7	65	4D	65	4D	37	B7	94	83	18	52	D8	F7	F7	FB	4C	74	EF	A9	
	00	6D	E7	4E	63	3C	94	2F	2F	63	3C	94	94	C4	43	FB	56	7B	11	14	C2	BF	52	EF	

Full AES Example (3)

	Start of Round				SubBytes				ShiftRows				MixColumns				AddRoundKey				Key Schedule				Round Constant
Round 7	0A	89	C1	85	67	A7	78	97	67	A7	78	97	EC	1A	C0	80	DB	A1	F8	77	37	BB	38	F7	40
	D9	F9	C5	E5	35	99	A6	D9	99	A6	D9	35	0C	50	53	C7	18	6D	8B	BA	14	3D	D8	7D	
	D8	F7	F7	FB	61	68	68	0F	68	0F	61	68	3B	D7	00	EF	A8	30	08	4E	93	E7	08	A1	
	56	7B	11	14	B1	21	82	FA	FA	B1	21	82	B7	22	72	E0	FF	D5	D7	AA	48	F7	A5	4A	
Round 8	DB	A1	F8	77	B9	32	41	F5	B9	32	41	F5	B1	1A	44	17	F9	E9	8F	2B	48	F3	CB	3C	80
	18	6D	8B	BA	AD	3C	3D	F4	3C	3D	F4	AD	3D	2F	EC	B6	1B	34	2F	08	26	1B	C3	BE	
	A8	30	08	4E	C2	04	30	2F	30	2F	C2	04	0A	6B	2F	42	4F	C9	85	49	45	A2	AA	0B	
	FF	D5	D7	AA	16	03	0E	AC	AC	16	03	0E	9F	68	F3	B1	BF	BF	81	89	20	D7	72	38	
Round 9	F9	E9	8F	2B	99	1E	73	F1	99	1E	73	F1	31	30	3A	C2	CC	3E	FF	3B	FD	0E	C5	F9	1B
	1B	34	2F	08	AF	18	15	30	18	15	30	AF	AC	71	8C	C4	A1	67	59	AF	0D	16	D5	6B	
	4F	C9	85	49	84	DD	97	3B	97	3B	84	DD	46	65	48	EB	04	85	02	AA	42	E0	4A	41	
	BF	BF	81	89	08	08	0C	A7	A7	08	08	0C	6A	1C	31	62	A1	00	5F	34	CB	1C	6E	56	
Round 10	CC	3E	FF	3B	4B	B2	16	E2	4B	B2	16	E2					**FF**	**08**	**69**	**64**	B4	BA	7F	86	36
	A1	67	59	AF	32	85	CB	79	85	CB	79	32					**0B**	**53**	**34**	**14**	8E	98	4D	26	
	04	85	02	AA	F2	97	77	AC	77	AC	F2	97					**84**	**BF**	**AB**	**8F**	F3	13	59	18	
	A1	00	5F	34	32	63	CF	18	18	32	63	CF					**4A**	**7C**	**43**	**B9**	52	4E	20	76	
					SubBytes				**ShiftRows**				**MixColumns**				**AddRoundKey**				**Key Schedule**				**Round Constant**

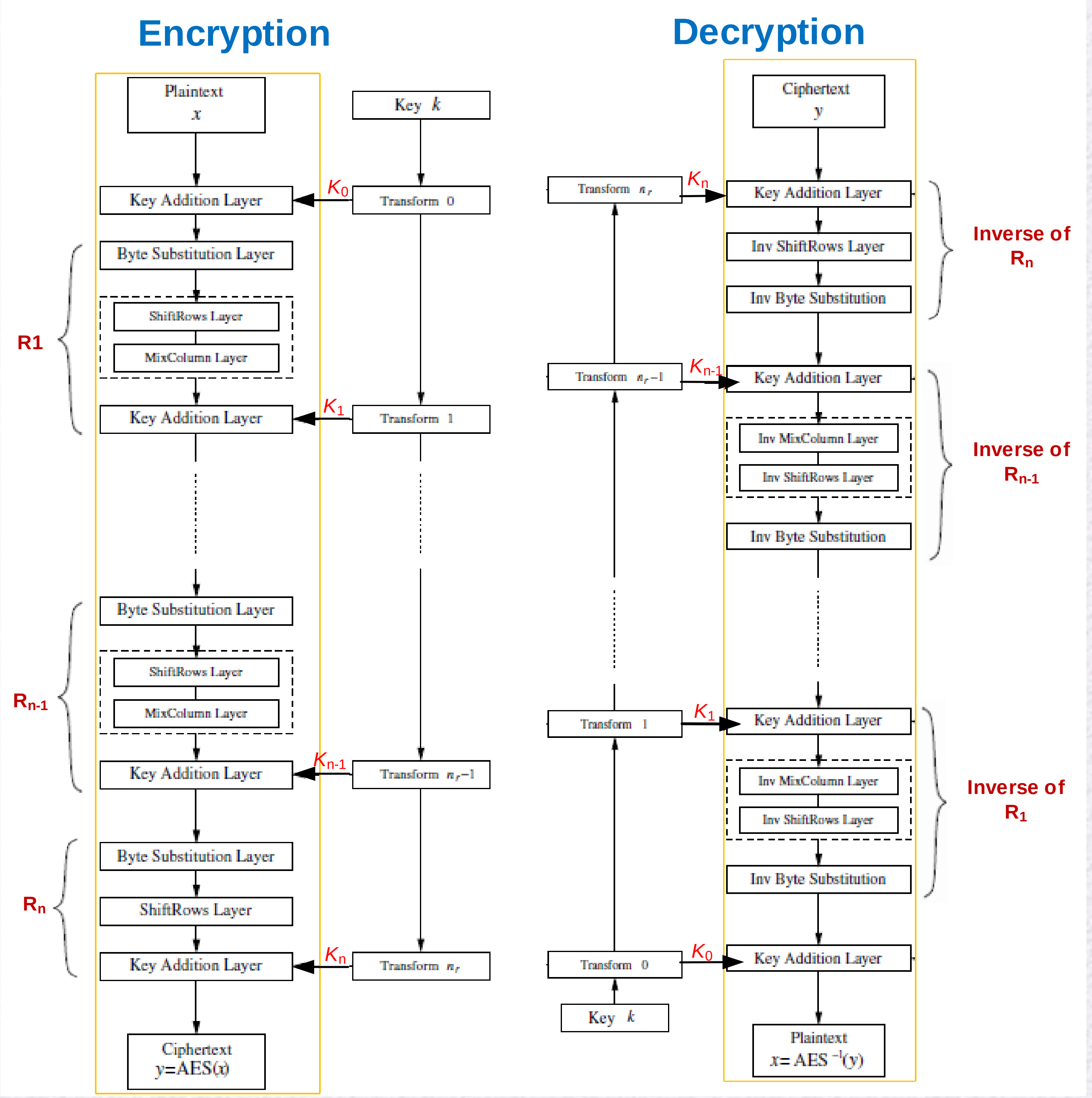
Summary of AES Example

(Table is located on page 177 in textbook)

Start of round	After SubBytes	After ShiftRows	After MixColumns	Round Key
01 89 fe 76 23 ab dc 54 45 cd ba 32 67 ef 98 10				0f 47 0c af 15 d9 b7 7f 71 e8 ad 67 c9 59 d6 98
0e ce f2 d9 36 72 6b 2b 34 25 17 55 ae b6 4e 88	ab 8b 89 35 05 40 7f f1 18 3f f0 fc e4 4e 2f c4	ab 8b 89 35 40 7f f1 05 f0 fc 18 3f c4 e4 4e 2f	b9 94 57 75 e4 8e 16 51 47 20 9a 3f c5 d6 f5 3b	dc 9b 97 38 90 49 fe 81 37 df 72 15 b0 e9 3f a7
65 0f c0 4d 74 c7 e8 d0 70 ff e8 2a 75 3f ca 9c	4d 76 ba e3 92 c6 9b 70 51 16 9b e5 9d 75 74 de	4d 76 ba e3 c6 9b 70 92 9b e5 51 16 de 9d 75 74	8e 22 db 12 b2 f2 dc 92 df 80 f7 c1 2d c5 1e 52	d2 49 de e6 c9 80 7e ff 6b b4 c6 d3 b7 5e 61 c6
5c 6b 05 f4 7b 72 a2 6d b4 34 31 12 9a 9b 7f 94	4a 7f 6b bf 21 40 3a 3c 8d 18 c7 c9 b8 14 d2 22	4a 7f 6b bf 40 3a 3c 21 c7 c9 8d 18 22 b8 14 d2	b1 c1 0b cc ba f3 8b 07 f9 1f 6a c3 1d 19 24 5c	c0 89 57 b1 af 2f 51 ae df 6b ad 7e 39 67 06 c0
71 48 5c 7d 15 dc da a9 26 74 c7 bd 24 7e 22 9c	a3 52 4a ff 59 86 57 d3 f7 92 c6 7a 36 f3 93 de	a3 52 4a ff 86 57 d3 59 c6 7a f7 92 de 36 f3 93	d4 11 fe 0f 3b 44 06 73 cb ab 62 37 19 b7 07 ec	2c a5 f2 43 5c 73 22 8c 65 0e a3 dd f1 96 90 50
f8 b4 0c 4c 67 37 24 ff ae a5 c1 ea e8 21 97 bc	41 8d fe 29 85 9a 36 16 e4 06 78 87 9b fd 88 65	41 8d fe 29 9a 36 16 85 78 87 e4 06 65 9b fd 88	2a 47 c4 48 83 e8 18 ba 84 18 27 23 eb 10 0a f3	58 fd 0f 4c 9d ee cc 40 36 38 9b 46 eb 7d ed bd
72 ba cb 04 1e 06 d4 fa b2 20 bc 65 00 6d e7 4e	40 f4 1f f2 72 6f 48 2d 37 b7 65 4d 63 3c 94 2f	40 f4 1f f2 6f 48 2d 72 65 4d 37 b7 2f 63 3c 94	7b 05 42 4a 1e d0 20 40 94 83 18 52 94 c4 43 fb	71 8c 83 cf c7 29 e5 a5 4c 74 ef a9 c2 bf 52 ef
0a 89 c1 85 d9 f9 c5 e5 d8 f7 f7 fb 56 7b 11 14	67 a7 78 97 35 99 a6 d9 61 68 68 0f b1 21 82 fa	67 a7 78 97 99 a6 d9 35 68 0f 61 68 fa b1 21 82	ec 1a c0 80 0c 50 53 c7 3b d7 00 ef b7 22 72 e0	37 bb 38 f7 14 3d d8 7d 93 e7 08 a1 48 f7 a5 4a
db a1 f8 77 18 6d 8b ba a8 30 08 4e ff d5 d7 aa	b9 32 41 f5 ad 3c 3d f4 c2 04 30 2f 16 03 0e ac	b9 32 41 f5 3c 3d f4 ad 30 2f c2 04 ac 16 03 0e	b1 1a 44 17 3d 2f ec b6 0a 6b 2f 42 9f 68 f3 b1	48 f3 cb 3c 26 1b c3 be 45 a2 aa 0b 20 d7 72 38
f9 e9 8f 2b 1b 34 2f 08 4f c9 85 49 bf bf 81 89	99 1e 73 f1 af 18 15 30 84 dd 97 3b 08 08 0c a7	99 1e 73 f1 18 15 30 af 97 3b 84 dd a7 08 08 0c	31 30 3a c2 ac 71 8c c4 46 65 48 eb 6a 1c 31 62	fd 0e c5 f9 0d 16 d5 6b 42 e0 4a 41 cb 1c 6e 56
cc 3e ff 3b a1 67 59 af 04 85 02 aa a1 00 5f 34	4b b2 16 e2 32 85 cb 79 f2 97 77 ac 32 63 cf 18	4b b2 16 e2 85 cb 79 32 77 ac f2 97 18 32 63 cf	4b 86 8a 36 b1 cb 27 5a fb f2 f2 af cc 5a 5b cf	b4 ba 7f 86 8e 98 4d 26 f3 13 59 18 52 4e 20 76
ff 08 69 64 0b 53 34 14 84 bf ab 8f 4a 7c 43 b9				

Encryption vs Decryption

- AES decryption cipher is not identical to the encryption cipher
  - The sequence of transformations differs although the form of the key schedules is the same
  - Has the disadvantage that two separate software or firmware modules are needed for applications that require both encryption and decryption



Decryption: Equivalent Inverse Cipher

- AES decryption cipher is not identical to the encryption cipher
  - The sequence of transformations differs although the form of the key schedules is the same
  - Has the disadvantage that two separate software or firmware modules are needed for applications that require both encryption and decryption

Two separate changes are needed to bring the decryption structure in line with the encryption structure

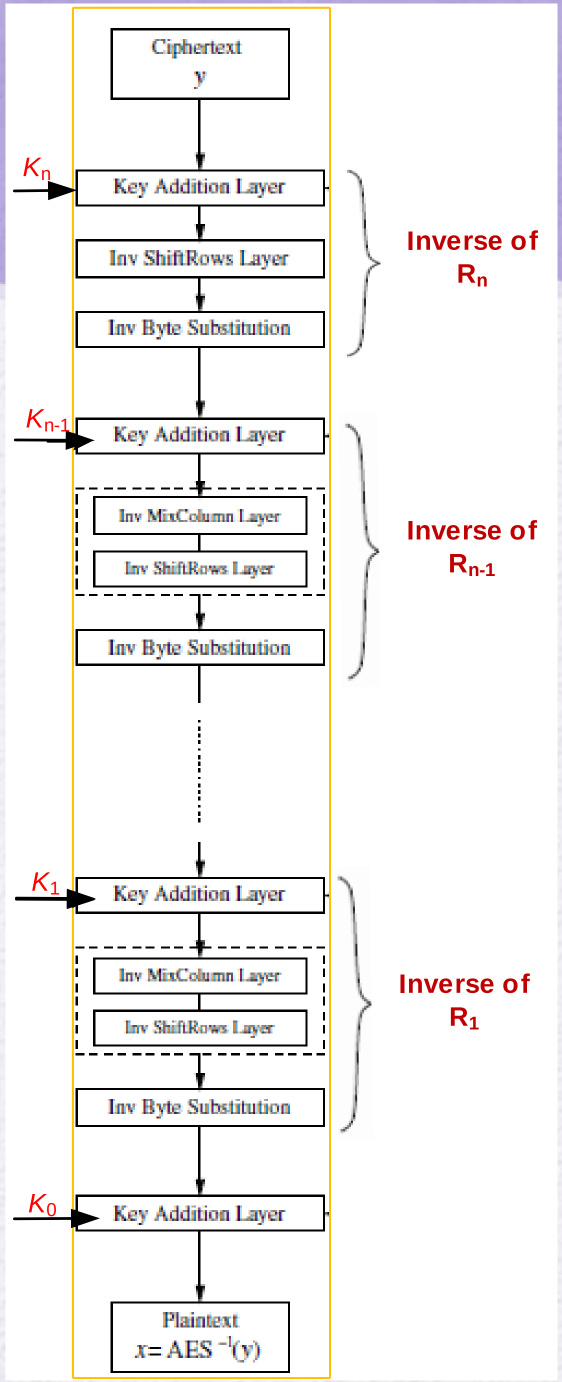
The first two stages of the decryption round need to be interchanged

The second two stages of the decryption round need to be interchanged

Interchanging InvShiftRows and InvSubBytes

- InvShiftRows *affects the sequence* of bytes in State but *does not alter byte contents* and *does not depend on byte contents* to perform its transformation
- InvSubBytes *affects the contents* of bytes in State but *does not alter byte sequence* and *does not depend on byte sequence* to perform its transformation

Thus, these two operations commute and can be interchanged



Interchanging AddRoundKey and InvMixColumns

The transformations AddRoundKey and InvMixColumns do not alter the sequence of bytes in State

If we view the key as a sequence of words, then both AddRoundKey and InvMixColumns operate on State one column at a time

These two operations are linear with respect to the column input

AES Implementation Aspects

- AES can be implemented very efficiently on an 8-bit processor
- AddRoundKey is a bytewise XOR operation
- ShiftRows is a simple byte-shifting operation
- SubBytes operates at the byte level and only requires a table of 256 bytes
- MixColumns requires matrix multiplication in the field GF(2^8), which means that all operations are carried out on bytes

Implementation Aspects

- Can efficiently implement on a 32-bit processor
  - Redefine steps to use 32-bit words
  - Can precompute 4 tables of 256-words
  - Then each column in each round can be computed using 4 table lookups + 4 XORs
  - At a cost of 4Kb to store tables
- Designers believe this very efficient implementation was a key factor in its selection as the AES cipher

Summary

- Finite field arithmetic
- AES structure
  - General structure
  - Detailed structure
- AES key expansion
  - Key expansion algorithm
  - Rationale

- AES transformation functions
  - Substitute bytes
  - ShiftRows
  - MixColumns
  - AddRoundKey
- AES implementation
  - Equivalent inverse cipher
  - Implementation aspects