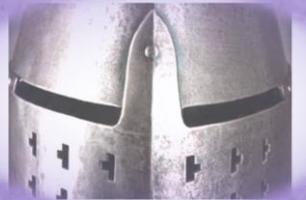


# Cryptography and Network Security

---

Sixth Edition  
by William Stallings



# *Chapter 5*

---

## Advanced Encryption Standard

*“It seems very simple.”*

*“It is very simple. But if you don’t know what  
the key is it’s virtually indecipherable.”*

**—Talking to Strange Men,  
Ruth Rendell**

# Finite Field Arithmetic

- In the Advanced Encryption Standard (AES) all operations are performed on 8-bit bytes
- The arithmetic operations of addition, multiplication, and division are performed over the finite field  $\text{GF}(2^8)$
- 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  $\mathbb{Z}_p$  consisting of all the integers  $\{0, 1, \dots, p - 1\}$ , where  $p$  is a prime number and in which arithmetic is carried out modulo  $p$

Find  $\gcd[a(x), b(x)]$  for  $a(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$  and  $b(x) = x^4 + x^2 + x + 1$ . First, we divide  $a(x)$  by  $b(x)$ :

$$\begin{array}{r} x^2 + x \\ \hline x^4 + x^2 + x + 1 \Big) x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\ \underline{x^6 + x^4 + x^3 + x^2} \\ \hline x^5 + x + 1 \\ \underline{x^5 + x^3 + x^2} \\ \hline x^3 + x^2 + 1 \end{array}$$

This yields  $r_1(x) = x^3 + x^2 + 1$  and  $q_1(x) = x^2 + x$ .

Then, we divide  $b(x)$  by  $r_1(x)$ .

$$\begin{array}{r} x + 1 \\ \hline x^3 + x^2 + 1 \Big) x^4 + x^2 + x + 1 \\ \underline{x^4 + x^3 + x} \\ \hline x^3 + x^2 + 1 \\ \underline{x^3 + x^2} \\ \hline 1 \end{array}$$

This yields  $r_2(x) = 0$  and  $q_2(x) = x + 1$ .

Therefore,  $\gcd[a(x), b(x)] = r_1(x) = x^3 + x^2 + 1$ .

The Advanced Encryption Standard (AES) uses arithmetic in the finite field  $\text{GF}(2^8)$ , with the irreducible polynomial  $m(x) = x^8 + x^4 + x^3 + x + 1$ . Consider the two polynomials  $f(x) = x^6 + x^4 + x^2 + x + 1$  and  $g(x) = x^7 + x + 1$ . Then

$$\begin{aligned}f(x) + g(x) &= x^6 + x^4 + x^2 + x + 1 + x^7 + x + 1 \\&= x^7 + x^6 + x^4 + x^2\end{aligned}$$

$$\begin{aligned}f(x) \times g(x) &= x^{13} + x^{11} + x^9 + x^8 + x^7 \\&\quad + x^7 + x^5 + x^3 + x^2 + x \\&\quad + x^6 + x^4 + x^2 + x + 1 \\&= x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1\end{aligned}$$

$$\begin{array}{r}x^5 + x^3 \\ \hline x^8 + x^4 + x^3 + x + 1 \sqrt{x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1} \\ x^{13} + x^9 + x^8 \\ \hline x^{11} + x^7 + x^6 + x^4 + x^3 \\ x^{11} + x^7 + x^6 \\ \hline x^7 + x^6 + 1\end{array}$$

Therefore,  $f(x) \times g(x) \bmod m(x) = x^7 + x^6 + 1$ .

Table 4.7 Polynomial Arithmetic Modulo  $(x^3 + x + 1)$ 

		000	001	010	011	100	101	110	111
		+	0	1	$x$	$x + 1$	$x^2$	$x^2 + 1$	$x^2 + x$
000	0	0	1	$x$	$x + 1$	$x^2$	$x^2 + 1$	$x^2 + 1$	$x^2 + x + 1$
001	1	1	0	$x + 1$	$x$	$x^2 + 1$	$x^2$	$x^2 + x + 1$	$x^2 + x$
010	$x$	$x$	$x + 1$	0	1	$x^2 + x$	$x^2 + x + 1$	$x^2$	$x^2 + 1$
011	$x + 1$	$x + 1$	$x$	1	0	$x^2 + x + 1$	$x^2 + x$	$x^2 + 1$	$x^2$
100	$x^2$	$x^2$	$x^2 + 1$	$x^2 + x$	$x^2 + x + 1$	0	1	$x$	$x + 1$
101	$x^2 + 1$	$x^2 + 1$	$x^2$	$x^2 + x + 1$	$x^2 + x$	1	0	$x + 1$	$x$
110	$x^2 + x$	$x^2 + x$	$x^2 + x + 1$	$x^2$	$x^2 + 1$	$x$	$x + 1$	0	1
111	$x^2 + x + 1$	$x^2 + x + 1$	$x^2 + x$	$x^2 + 1$	$x^2$	$x + 1$	$x$	1	0

(a) Addition

	000	001	010	011	100	101	110	111
+	0	1	2	3	4	5	6	7
000	0	1	2	3	4	5	6	7
001	1	0	3	2	5	4	7	6
010	2	3	0	1	6	7	4	5
011	3	2	1	0	7	6	5	4
100	4	5	6	7	0	1	2	3
101	5	4	7	6	1	0	3	2
110	6	7	4	5	2	3	0	1
111	7	6	5	4	3	2	1	0

(a) Addition

	000	001	010	011	100	101	110	111
$\times$	0	1	$x$	$x + 1$	$x^2$	$x^2 + 1$	$x^2 + x$	$x^2 + x + 1$
000	0	0	0	0	0	0	0	0
001	1	0	$x$	$x + 1$	$x^2$	$x^2 + 1$	$x^2 + x$	$x^2 + x + 1$
010	$x$	0	$x^2$	$x^2 + x$	$x + 1$	1	$x^2 + x + 1$	$x^2 + 1$
011	$x + 1$	0	$x^2 + x$	$x^2 + 1$	$x^2 + x + 1$	$x^2$	1	$x$
100	$x^2$	0	$x^2$	$x + 1$	$x^2 + x + 1$	$x^2 + x$	$x$	$x^2 + 1$
101	$x^2 + 1$	0	$x^2 + 1$	1	$x^2$	$x$	$x^2 + x + 1$	$x + 1$
110	$x^2 + x$	0	$x^2 + x + 1$	1	$x^2 + 1$	$x + 1$	$x$	$x^2$
111	$x^2 + x + 1$	0	$x^2 + x + 1$	$x^2 + 1$	$x$	1	$x^2 + 1$	$x^2$

(b) Multiplication

		000	001	010	011	100	101	110	111
	$\times$	0	1	2	3	4	5	6	7
000	0	0	0	0	0	0	0	0	0
001	1	0	1	2	3	4	5	6	7
010	2	0	2	4	6	3	1	7	5
011	3	0	3	6	5	7	4	1	2
100	4	0	4	3	7	6	2	5	1
101	5	0	5	1	4	2	7	3	6
110	6	0	6	7	1	5	3	2	4
111	7	0	7	5	2	1	6	4	3

(b) Multiplication

$w$	$-w$	$w^{-1}$
0	0	—
1	1	1
2	2	5
3	3	6
4	4	7
5	5	2
6	6	3
7	7	4

(c) Additive and multiplicative  
inverses

# Galois Field

The elements of Galois Field  $gf(p^n)$  is defined as

$$\begin{aligned} gf(p^n) = & (0, 1, 2, \dots, p-1) \cup \\ & (p, p+1, p+2, \dots, p+p-1) \cup \\ & (p^2, p^2+1, p^2+2, \dots, p^2+p-1) \cup \dots \cup \\ & (p^{n-1}, p^{n-1}+1, p^{n-1}+2, \dots, p^{n-1}+p-1) \end{aligned}$$

where  $p \in \mathbb{P}$  and  $n \in \mathbb{Z}^+$ . The order of the field is given by  $p^n$  while  $p$  is called the characteristic of the field. On the other hand,  $gf$ , as one may have guessed it, stands for Galois Field. Also note that the degree of polynomial of each element is at most  $n - 1$ .

$$gf(5) = (0, 1, 2, 3, 4)$$

$$\begin{aligned}gf(2^3) &= (0, 1, 2, 2+1, 2^2, 2^2+1, 2^2+2, 2^2+2+1) \\&= (0, 1, 2, 3, 4, 5, 6, 7)\end{aligned}$$

Suppose we are working in  $gf(2^8)$ , then  $83 + 249$  is

$$\begin{aligned} 83 + 249 &= (2^6 + 2^4 + 2^1 + 2^0) + (2^7 + 2^6 + 2^5 + 2^4 + 2^3 \\ &= 2^7 + 2 \cdot 2^6 + 2^5 + 2 \cdot 2^4 + 2^3 + 2^1 + 2 \cdot 2^0 \\ &= 2^7 + 2^5 + 2^3 + 2^1 \\ &= 169 \end{aligned}$$

Alternatively, from binary numeral system perspective,

$$\begin{aligned} 83 + 249 &= 01010011 + 11111001 \\ &= 10101010 \\ &= 169 \end{aligned}$$

and the results coincide.

Suppose we are working in  $gf(2^8)$  and we take the irreducible polynomial modulo  $m(p)$  to be  $p^8 + p^6 + p^5 + p^1 + p^0$ . To calculate  $84 \cdot 13$ , we need to go through several steps. First, we compute the product of the polynomial and reduce the coefficients modulo 2.

$$\begin{aligned} 84 \cdot 13 &= ((2^6 + 2^4 + 2^2) \cdot (2^3 + 2^2 + 2^0)) \pmod{m(p)} \\ &= (2^9 + 2^8 + 2^7 + 2 \cdot 2^6 + 2^5 + 2 \cdot 2^4 + 2^2) \pmod{m(p)} \\ &= (2^9 + 2^8 + 2^7 + 2^5 + 2^2) \pmod{m(p)} \end{aligned}$$

Then we use long division to compute the reduced polynomial as follows

Remainder	Quotient
$2^9 + 2^8 + 2^7 + 2^5 + 2^2$	
$2^8 + 2^6 + 2^5 + 2^1 + 2^0$	
$2^0$	$2^1 + 2^0$

Where the last entry in the first column is the product we seek for. Since the product is 1, it follows that 84 and 13 are multiplicative inverse pairs.

To summarize, AES operates on 8-bit bytes. Addition of two bytes is defined as the bitwise XOR operation. Multiplication of two bytes is defined as multiplication in the finite field GF(2<sup>8</sup>), with the irreducible polynomial<sup>3</sup>  $m(x) = x^8 + x^4 + x^3 + x + 1$ . The developers of Rijndael give as their motivation for selecting this one of the 30 possible irreducible polynomials of degree 8 that it is the first one on the list.

In the 1970's, IBM developed Data Encryption Standard (DES). However, given that DES uses humble 56-bit key and technology advances rapidly, a supercomputer was able to break the key in less than 24 hours thus a more sophisticated algorithm was necessary. In 2001, Vincent Rijmen and John Daemon came up with a more complicated algorithm called Rijndael and it has been the Advanced Encryption Standard (AES) ever since.

Before data scrambling and encryption can begin, the data must first be arranged in a state or a matrix of bytes. The algorithm for Advanced Encryption Standard (AES) consists of smaller, sub-algorithms namely SubBytes, ShiftRows, MixColumns, and AddRoundKey, where each method will be explained in details below. Note that the following explanation only applies to AES with 128-bit key. The algorithm for other variations such as AES with 192-bit and 256-bit keys slightly differs.

# Finite Field Arithmetic

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

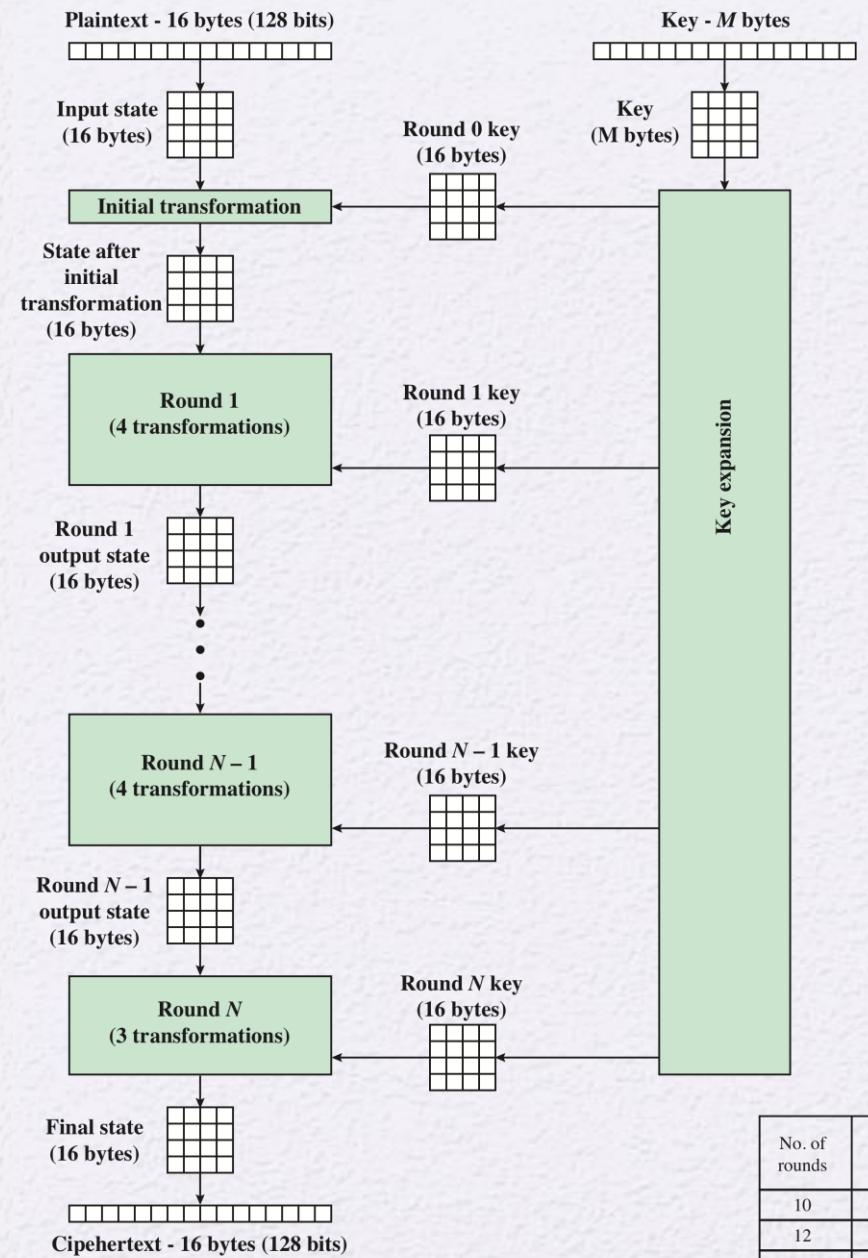
The set of such integers,  $Z_{2^n}$ , using modular arithmetic, is not a field

- 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  $GF(2^n)$

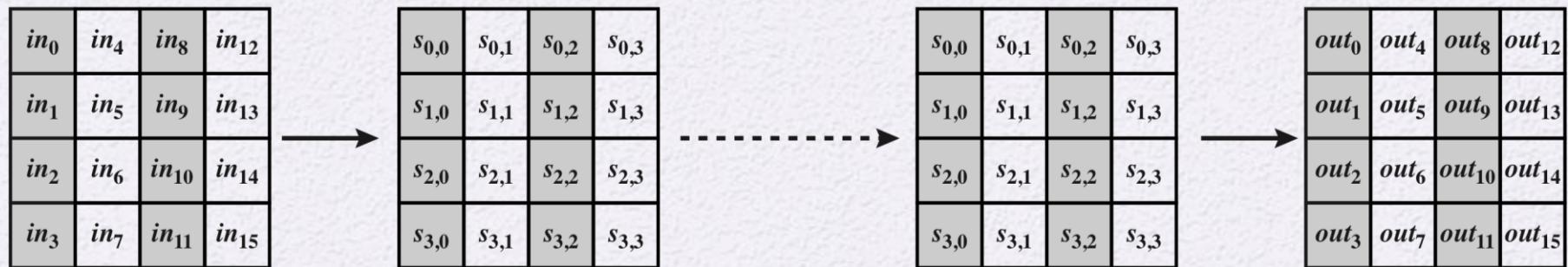
- Every polynomial in  $GF(2^n)$  can be represented by an  $n$ -bit number

# AES Encryption Process



**Figure 5.1 AES Encryption Process**

# AES Data Structures



(a) Input, state array, and output



(b) Key and expanded key

Figure 5.2 AES Data Structures

# Table 5.1

## AES Parameters

<b>Key Size (words/bytes/bits)</b>	4/16/128	6/24/192	8/32/256
<b>Plaintext Block Size (words/bytes/bits)</b>	4/16/128	4/16/128	4/16/128
<b>Number of Rounds</b>	10	12	14
<b>Round Key Size (words/bytes/bits)</b>	4/16/128	4/16/128	4/16/128
<b>Expanded Key Size (words/bytes)</b>	44/176	52/208	60/240

# AES Encryption and Decryption

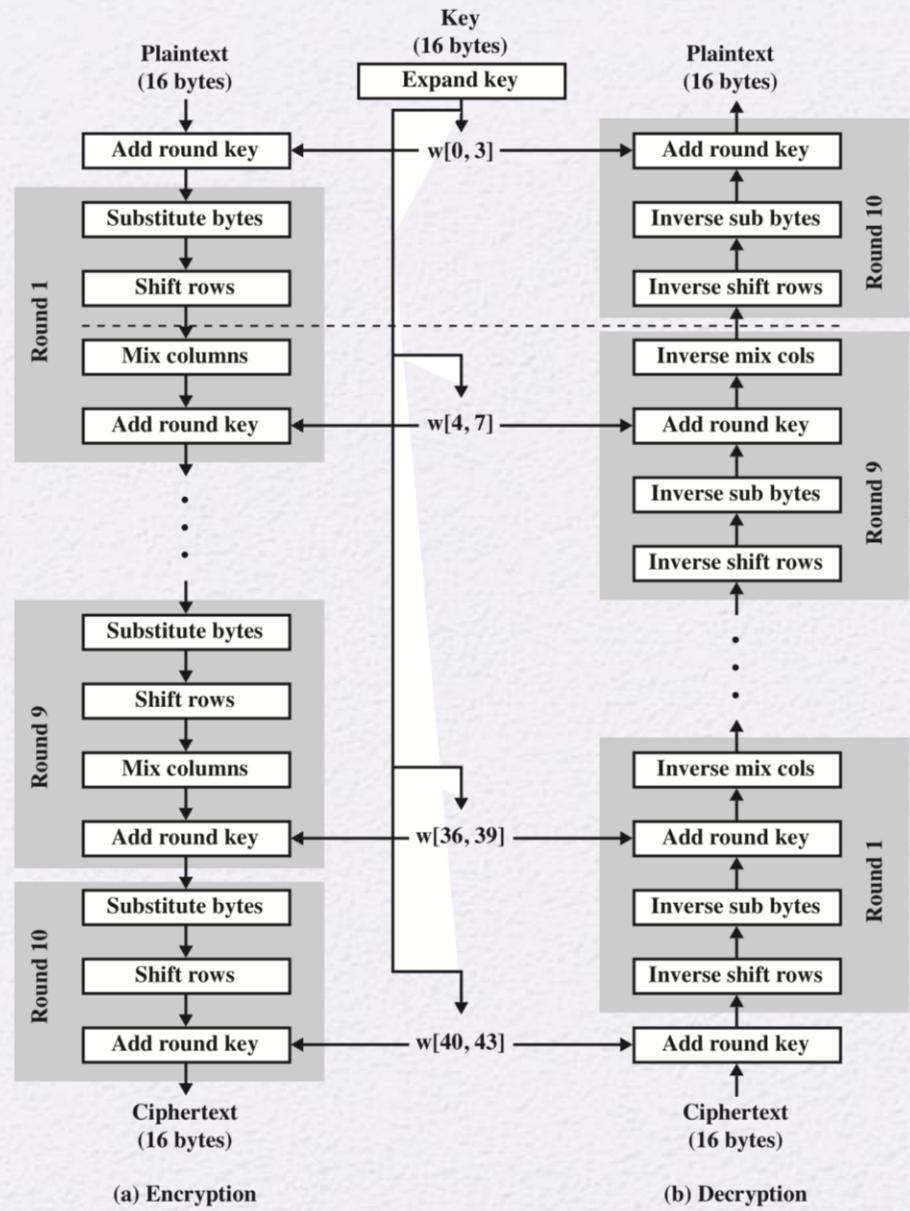


Figure 5.3 AES Encryption and Decryption

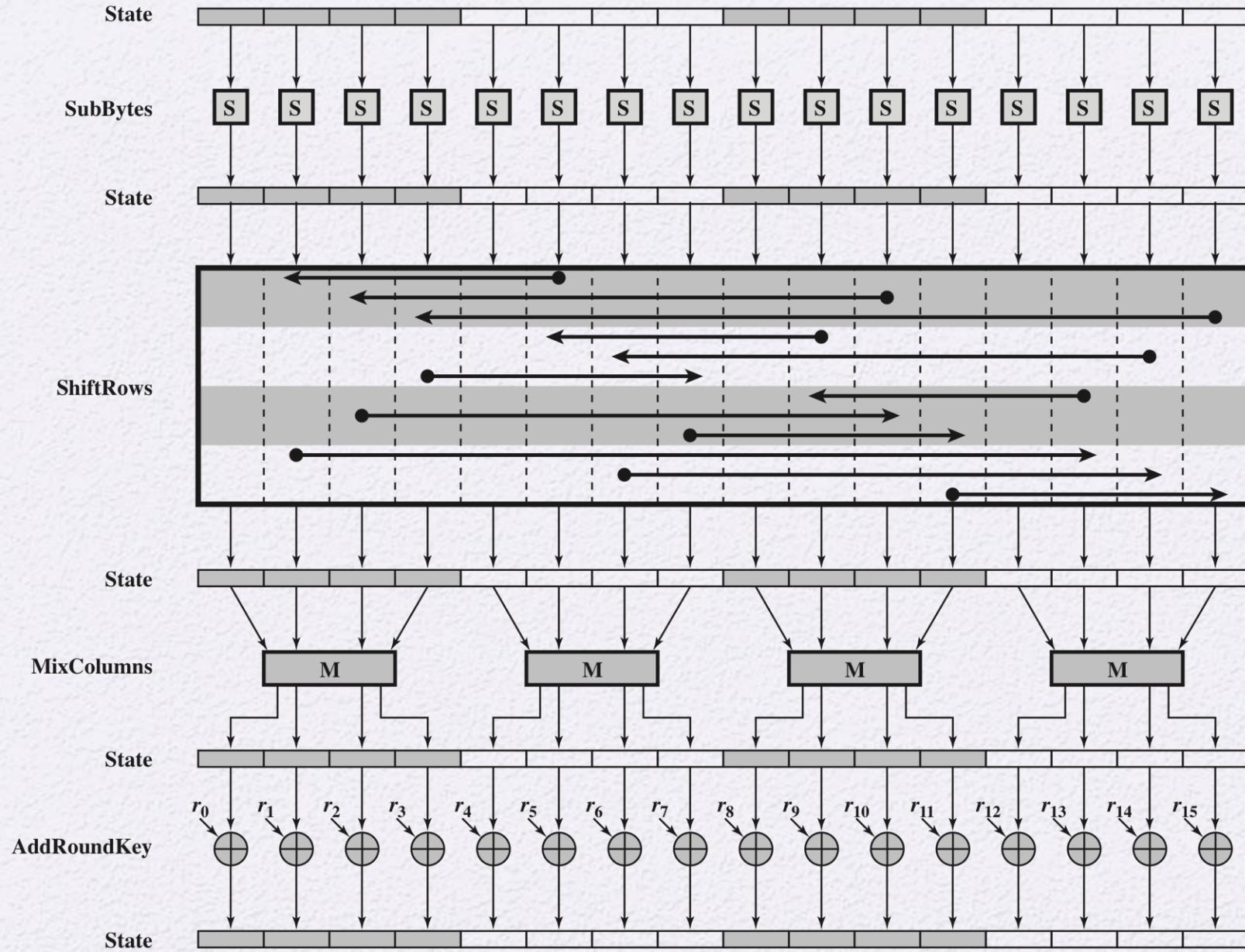
# Detailed Structure

- Processes the entire data block as a single matrix during each round using substitutions and permutation
- The key that is provided as input is expanded into an array of forty-four 32-bit words,  $w[i]$

Four different stages are used:

- 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

- The cipher begins and ends with an AddRoundKey stage
- Can view the cipher as alternating operations of XOR encryption (AddRoundKey) of a block, followed by scrambling of the block (the other three stages), followed by XOR encryption, and so on
- Each stage is easily reversible
- The decryption algorithm makes use of the expanded key in reverse order, however the decryption algorithm is not identical to the encryption algorithm
- State is the same for both encryption and decryption
- Final round of both encryption and decryption consists of only three stages



**Figure 5.4 AES Encryption Round**

# AES Byte Level Operations

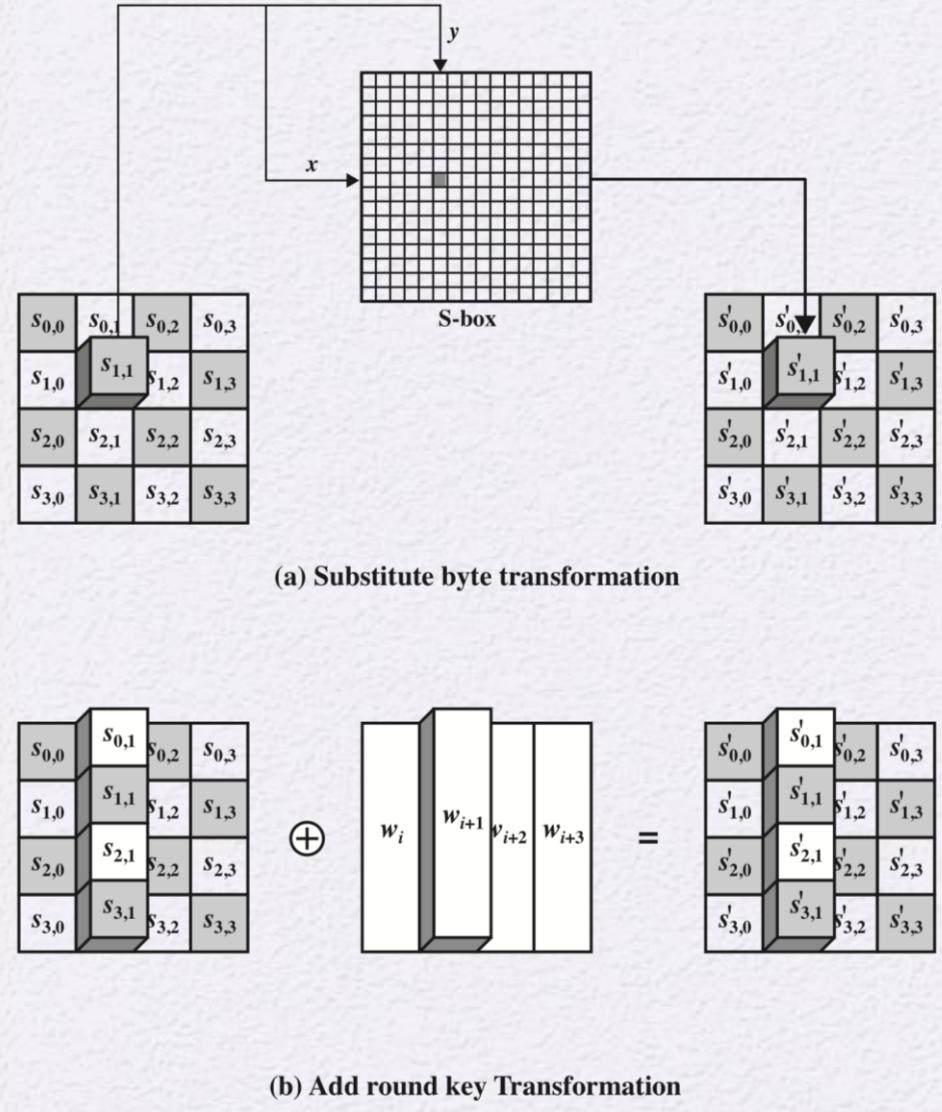


Figure 5.5 AES Byte-Level Operations

# Table 5.2

(a) S-box

		y															
	x	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

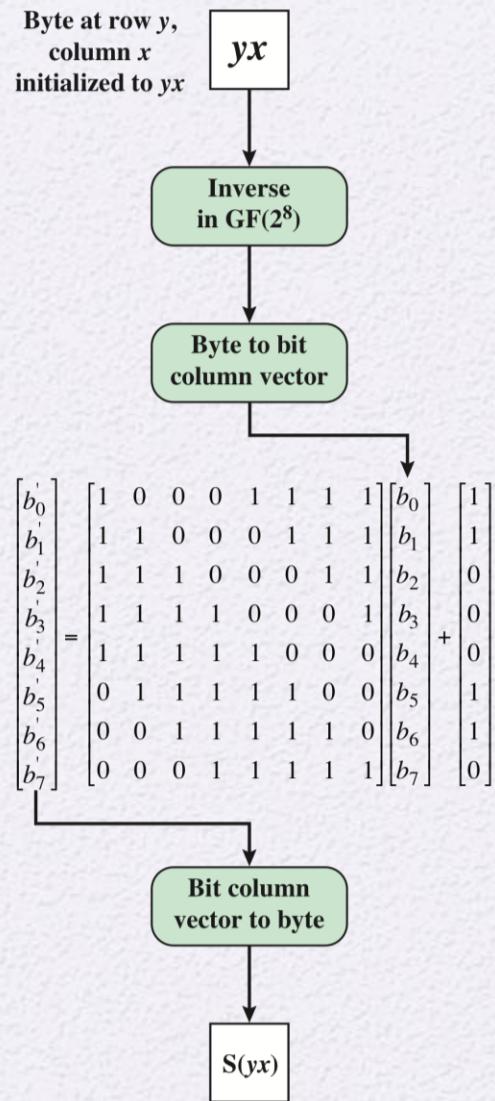
(Table can be found on page 139 in textbook)

# Table 5.2

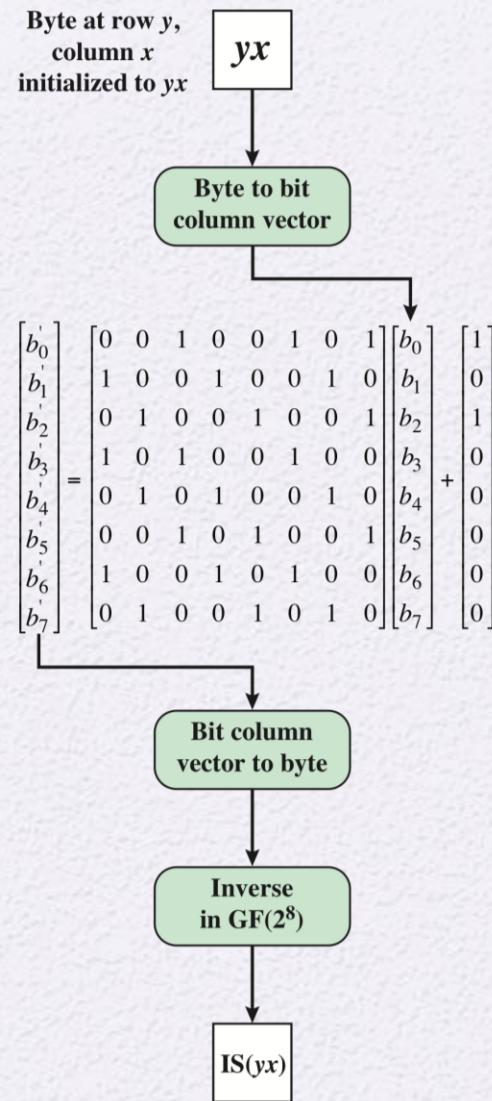
(b) Inverse S-box

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

(Table can be found on page 139 in textbook)



(a) Calculation of byte at  
row y, column x of S-box



(a) Calculation of byte at  
row y, column x of IS-box

Figure 5.6 Construction of S-Box and IS-Box

# 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 Transformation

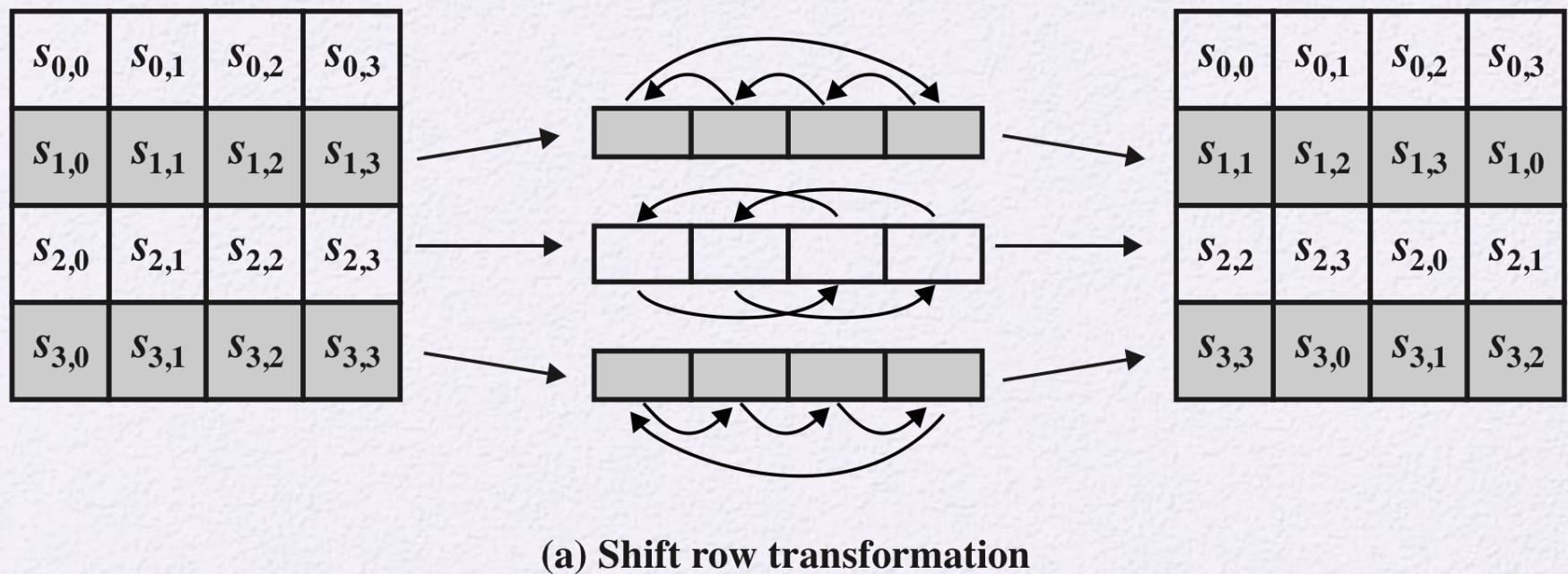


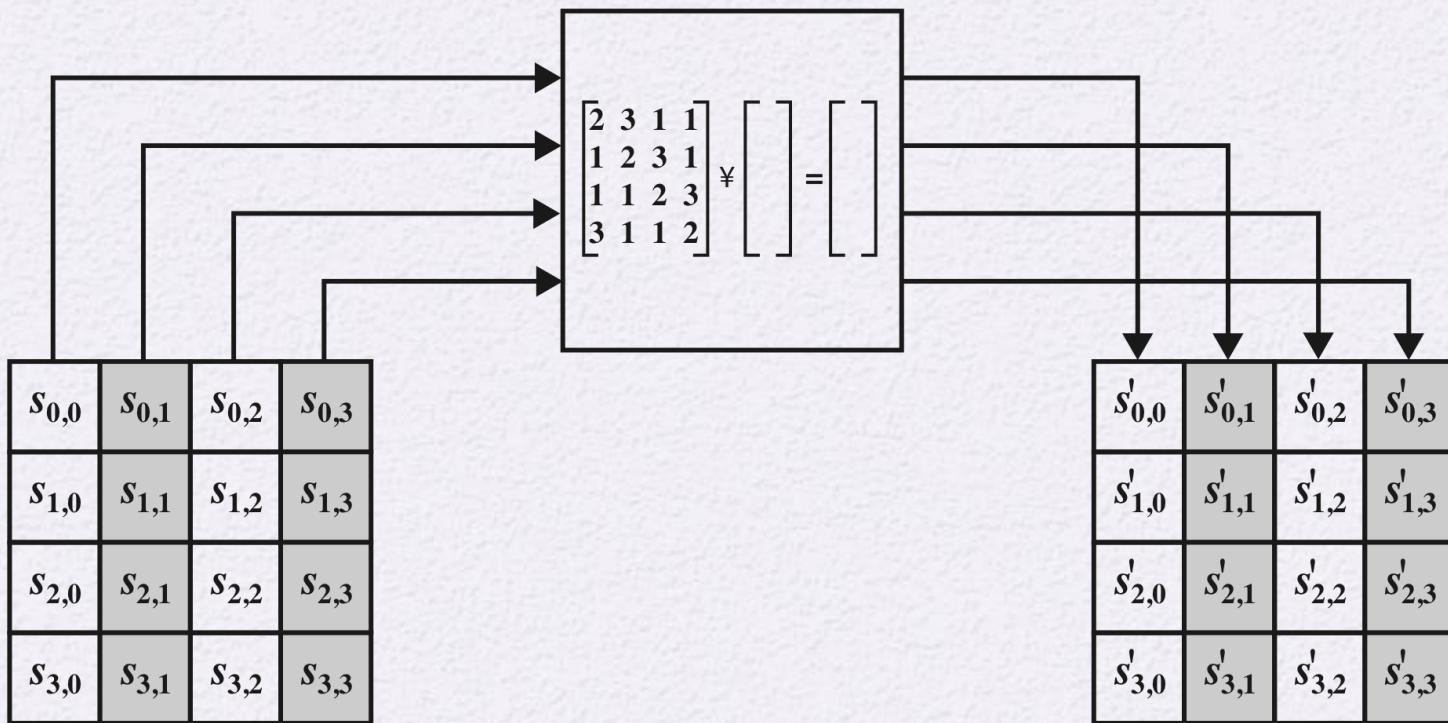
Figure 5.7 AES Row and Column Operations

(Figure can be found on page 144 in textbook)

# 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

# MixColumn Transformation



(b) Mix column transformation

Figure 5.7 AES Row and Column Operations

# 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

# AddRoundKey Transformation

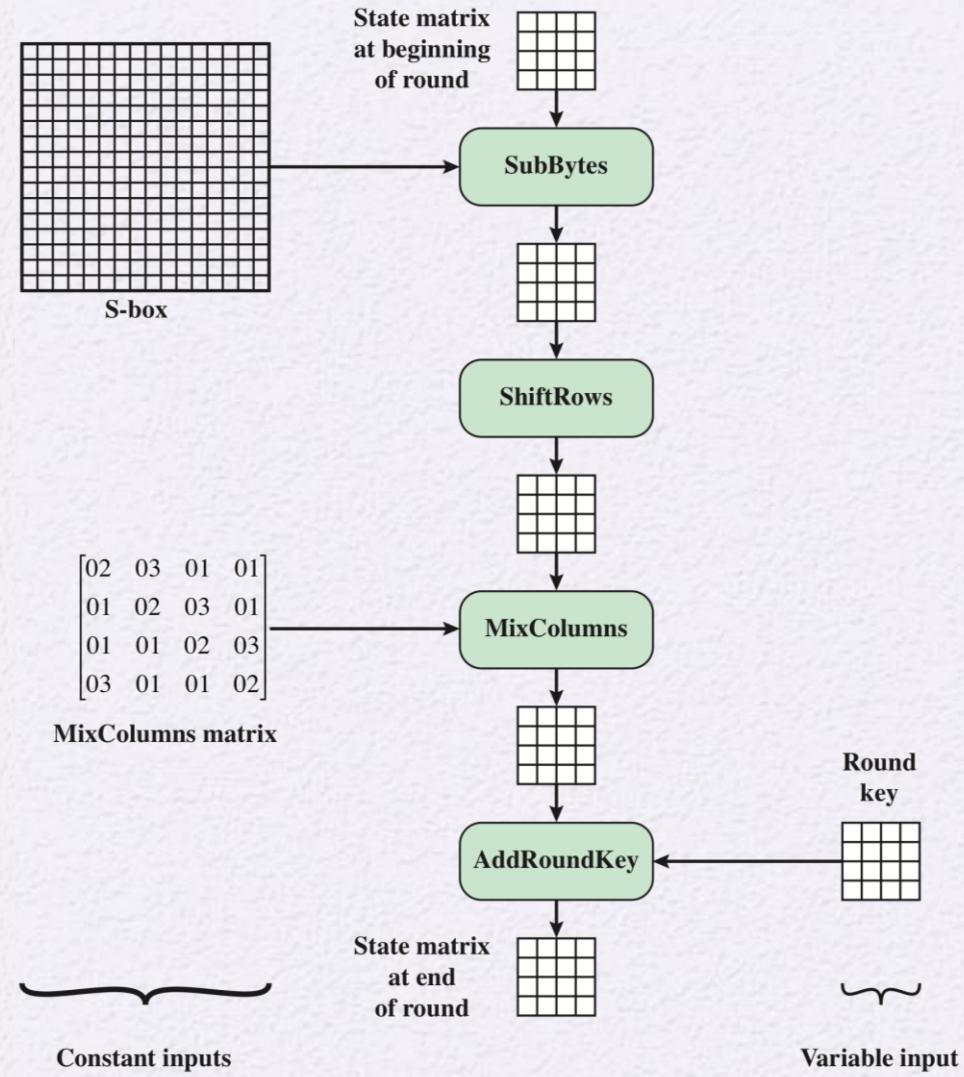
- The 128 bits of State are bitwise XORed with the 128 bits of the round key
- Operation is viewed as a columnwise operation between the 4 bytes of a State column and one word of the round key
  - Can also be viewed as a byte-level operation

## 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

# Inputs for Single AES Round

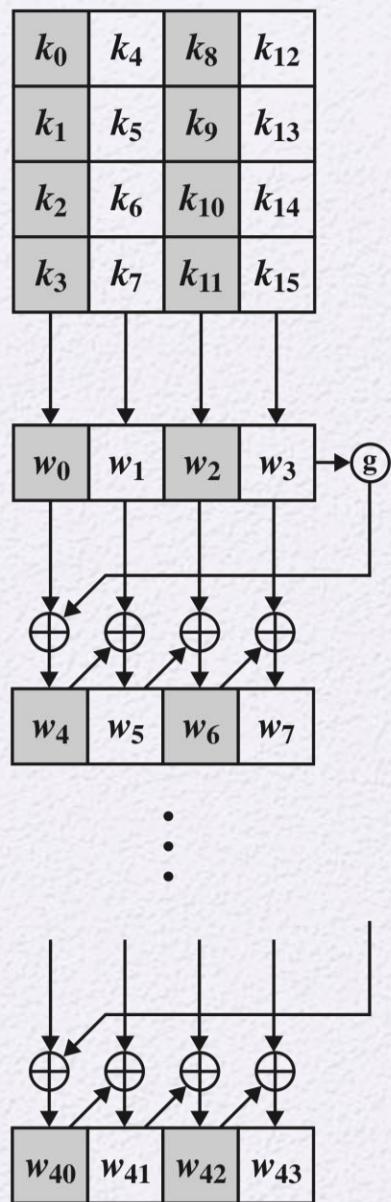


**Figure 5.8 Inputs for Single AES Round**

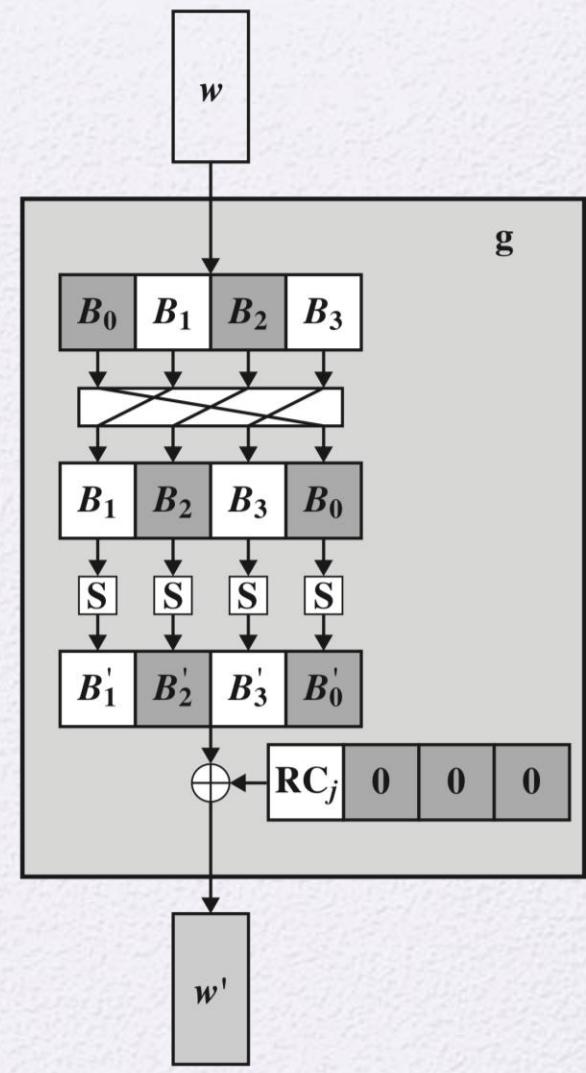
# AES Key Expansion

- 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

# AES Key Expansion



(a) Overall algorithm



(b) Function  $g$

Figure 5.9 AES Key Expansion

# 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

# Table 5.3

## AES Example

### Key Expansion

(Table is located on page 151  
in textbook)

Key Words	Auxiliary Function
w0 = 0f 15 71 c9 w1 = 47 d9 e8 59 w2 = 0c b7 ad d6 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 8e = 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
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 df 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 38	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	

Table 5.4

# AES Example

(Table is located on page 153  
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				

# Table 5.5

## Avalanche Effect in AES: Change in Plaintext

(Table is located on page 154  
in textbook)

Round		Number of Bits that Differ
	0123456789abcdeffedcba9876543210 0023456789abcdeffedcba9876543210	1
0	0e3634aece7225b6f26b174ed92b5588 0f3634aece7225b6f26b174ed92b5588	1
1	657470750fc7ff3fc0e8e8ca4dd02a9c c4a9ad090fc7ff3fc0e8e8ca4dd02a9c	20
2	5c7bb49a6b72349b05a2317ff46d1294 fe2ae569f7ee8bb8c1f5a2bb37ef53d5	58
3	7115262448dc747e5cdac7227da9bd9c ec093dfb7c45343d689017507d485e62	59
4	f867aee8b437a5210c24c1974cffebc 43efdb697244df808e8d9364ee0ae6f5	61
5	721eb200ba06206dcbd4bce704fa654e 7b28a5d5ed643287e006c099bb375302	68
6	0ad9d85689f9f77bc1c5f71185e5fb14 3bc2d8b6798d8ac4fe36a1d891ac181a	64
7	db18a8ffa16d30d5f88b08d777ba4eaa 9fb8b5452023c70280e5c4bb9e555a4b	67
8	f91b4fbfe934c9bf8f2f85812b084989 20264e1126b219aef7feb3f9b2d6de40	65
9	cca104a13e678500ff59025f3bafaa34 b56a0341b2290ba7dfdfbddcd8578205	61
10	ff0b844a0853bf7c6934ab4364148fb9 612b89398d0600cde116227ce72433f0	58

# Table 5.6

## Avalanche Effect in AES: Change in Key

(Table is located on page 155 in textbook)

Round		Number of Bits that Differ
	0123456789abcdefedcba9876543210 0123456789abcdefedcba9876543210	0
0	0e3634aece7225b6f26b174ed92b5588 0f3634aece7225b6f26b174ed92b5588	1
1	657470750fc7ff3fc0e8e8ca4dd02a9c c5a9ad090ec7ff3fc1e8e8ca4cd02a9c	22
2	5c7bb49a6b72349b05a2317ff46d1294 90905fa9563356d15f3760f3b8259985	58
3	7115262448dc747e5cdac7227da9bd9c 18aeb7aa794b3b66629448d575c7cebf	67
4	f867aee8b437a5210c24c1974cfffeabc f81015f993c978a876ae017cb49e7eec	63
5	721eb200ba06206dcbd4bce704fa654e 5955c91b4e769f3cb4a94768e98d5267	81
6	0ad9d85689f9f77bc1c5f71185e5fb14 dc60a24d137662181e45b8d3726b2920	70
7	db18a8ffa16d30d5f88b08d777ba4eaa fe8343b8f88bef66cab7e977d005a03c	74
8	f91b4fbfe934c9bf8f2f85812b084989 da7dad581d1725c5b72fa0f9d9d1366a	67
9	cca104a13e678500ff59025f3bafaa34 0ccb4c66bbfd912f4b511d72996345e0	59
10	ff0b844a0853bf7c6934ab4364148fb9 fc8923ee501a7d207ab670686839996b	53

# 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

# Equivalent Inverse Cipher

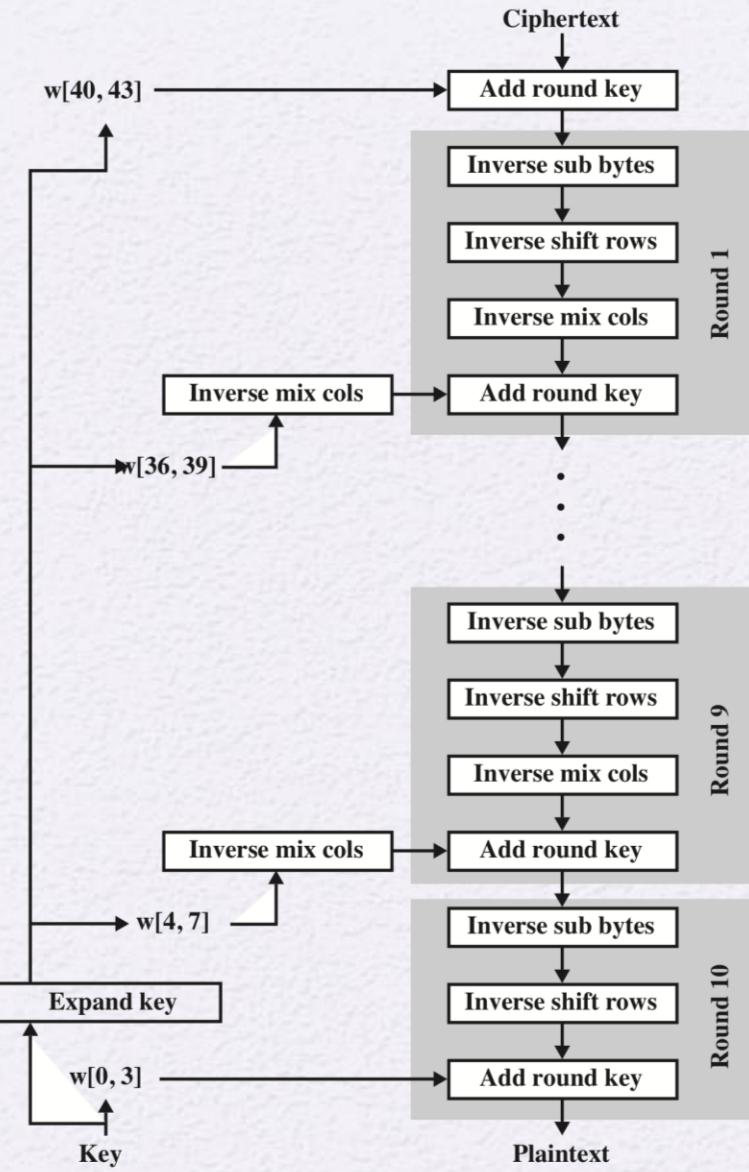


Figure 5.10 Equivalent Inverse Cipher

# 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  $\text{GF}(2^8)$ , 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

