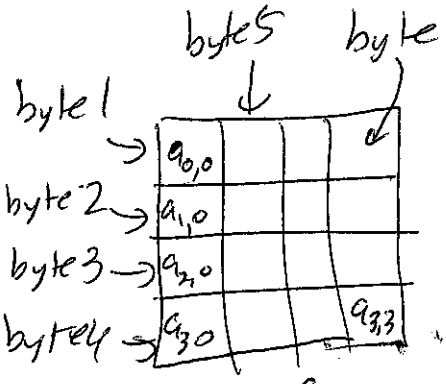
Rijndahl (pronounced RAIN-DOLL)

SECURE
FAST
SIMPLE
EXTENDIBLE → operations are very fast in either software or hardware

(128 bit key,
192 bit key
256 bit key)



16 squares × 8 bits = 128 bits
BLOCK SIZE

Generally bytes expressed in HEX

7C = 01111100

S-box(7C) = 10, S-inv(10) = 7C

S-box(A4) = 49, S-inv(49) = A4

Input

(SHIFT ROWS)

a_{00}	a_{01}	a_{02}	a_{03}
a_{10}	a_{11}	a_{12}	a_{13}
a_{20}	a_{21}	a_{22}	a_{23}
a_{30}	a_{31}	a_{32}	a_{33}

→

a_{00}	a_{01}	a_{02}	a_{03}
a_{11}	a_{12}	a_{13}	a_{10}
a_{22}	a_{23}	a_{20}	a_{21}
a_{33}	a_{30}	a_{31}	a_{32}

Mix Columns

col 4

row 2

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} 7A & 8F & 26 & 39 \\ CB & 04 & D1 & EE \\ 67 & 4B & 39 & 48 \\ BF & F1 & 00 & 32 \end{bmatrix} = \begin{bmatrix} - & - & - & - \\ - & - & - & \square \\ - & - & - & - \\ - & - & - & - \end{bmatrix}$$

each byte is actually a special type of polynomial.

$39 = 00111001 = x^5 + x^4 + x^3 + 1$

↳ poly is deg 7 or less, coefficients 0, 1

polynomials for AES for a field in $GF(2^8)$.

all calculations are done mod $\boxed{x^8 + x^4 + x^3 + x + 1}$.

Irreducible Polynomial

if $f(x)$ is degree 7 or less then

$f(x) \bmod x^8 + x^4 + x^3 + x + 1 = f(x)$.

Since only coefficients are 0 and 1, all coefficients are considered mod 2.

$$(x^6 + x^5 + x^3 + x + 1) + (x^7 + x^5 + x^3 + x)$$

$$= \boxed{x^7 + x^6 + 1}$$

$$(x^4 + 1)(x^4 + x^2 + x)$$

$$= x^8 + x^6 + x^5 + x^4 + x^2 + x$$

$x^6+x^4+x^3+x+1 \;\big|\; x^6+x^6+x^5+x^4+x^2+x$

$-\;x^6 \qquad\qquad +x^4+x^3 \quad +x \quad +1$

$x^6+x^5+x^3+x^2+1$

If I have 1 in the 9th bit position, the 1 is equivalent to getting rid of the 1 and flipping bits $x^4, x^3, x, 1$.

$$10111010 = 01110110 \oplus 11011$$

$$01101101$$

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} 7A & 8F & 26 & 39 \\ CB & 04 & D1 & EE \\ 67 & 4B & 39 & 48 \\ BF & F1 & 00 & 32 \end{bmatrix}$$

$1 \times 39 = 39 = 00111001$

$2 \times EE = C7 = 11000111$

$3 \times 48 = D8 = 11011000$

$1 \times 32 = 32 = 00110010$

$00010100 = 14$

mult by 2 is just adding a 0.

$(10) \times (11101110) = 11011100$

$= 11011100 \oplus 11011$

11000111

$\rightarrow (11) \times (01001000) =$

$x+1$

$$\begin{array}{r} 01001000 \\ \oplus\ 10010000 \\ \hline 11011000 \end{array}$$

10/3/16 (3) 4

Most of the time

$$w[i] = w[i-4] \oplus w[i-1]$$

If triggers when we start to fill in a new round key. → Uses S-box

$$temp = subword(rotword(temp)) \oplus Rcon[i/4]$$

- rotword: left cyclic rotation by one byte
- Rcon: pad with 3 bytes of 0s on right.

$w[32] = 36A7490F$

$temp = w[35] = AB286C5D$

$w[36] = ?$

$rotword(temp) = 286C5DAB$

$subword(\ ) = 345D4C62$

$Rcon(i/4) \quad \oplus\ 1B000000$

$2F5D4C62$

$\oplus\ 36A749DF$

$w[36] = 19F7D56D$

100
1011
1111

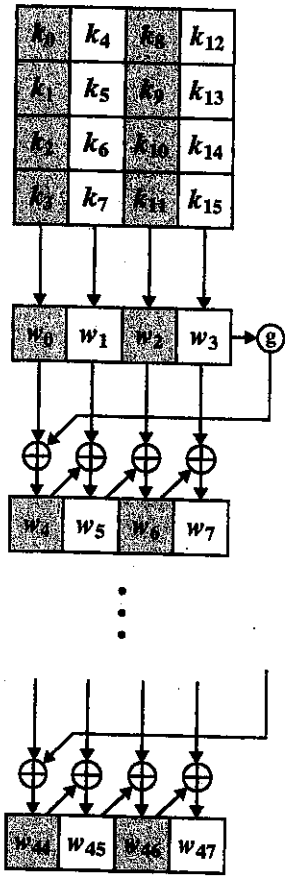
1111
0110
1010
0101

1100
1001
0101

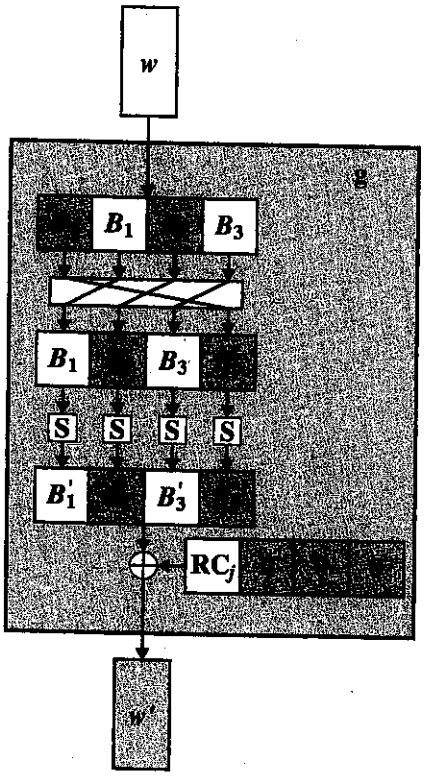
1111
10

```
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
   }
}
```



(a) Overall algorithm



(b) Function g

Figure 5.9 AES Key Expansion

cation defined over the field GF(2^8). The values of RC[j] in hexadecimal are

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