AES #2

Friday, October 9, 2020 11:30 AM

1. Mix Cols Review
2. AES Key Schedule
3. Helper Mix Cols Program
4. Helper DES S-box Program
5. AES code

Mix Cols

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

x

63	7c	77	93
36	3f	cd	26
f1	1a	0c	13
16	4b	c6	d2

Note: first matrix is fixed for the algorithm.
Second matrix is the state matrix right before Mix Cols.

Entry in row 2, column1:

01 x 63 + 02 x 36 + 03 x f1 + 01 x 16
63 + 6c + 08+ 16

Rules for multiplication in the field:

1. mult 2 is a left shift
2. If there is an overflow bit, that bit is equivalent to xoring with 0001 1011, from the AES polynomial.
3. All other multiplications can be created as a combination of these rules and addition, which is XOR in the field.

02 x 36 = 0011 0110 left shifted by 1 bit
0110 1100 = 6c

03 x f1 = 02 x f1 +
01 x f1

02 x f1 = 1111 0001 left shifted by 1
= 1 1110 0010 (overflow
= 1110 0010
+   1 1011

 1111 1001

03 x f1 = 1111 1001 (02 x f1)
+ 1111 0001 (01 x f1)

0000 1000 = 08

Final answer:

63 + 6c + 08+ 16 use the XOR chart for HEX

6 + 6 + 0 + 1 = 1 (xor)
3 + c + 8 + 6 = f + e = 1

Final Answer is **11.**

AES Key Schedule
bytes are 8 bits, words are 32 bits, so 4 bytes = word

```
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%4 == 0)  // Beginning of the new round key
         temp = SubWord(RotWord(temp)) XOR Rcon[i/4]
```

```
        w[i] = w[i-4] XOR temp;
    }
}
```

Round 0 key is the original key.
For round 1 to round 10, the keys are w[4]…w[7] R1
w[8]…w[11] R2
w[4i]…w[4i+3] Round i key

Unless it's the beginning of a new round key, all we do to generate the next 32 bits, is XOR the last 32 bits with the 32 bits from 4 times ago.

But, when we begin a new round, we want to mess stuff up…so here is what we do:

RotWord is a cyclic left rotation by one byte.

i=36 in this example..
Let's say that w[35] = 7f8d292f (in hex)
RotWord(w[35]) = 8d292f7f

Next step is to do a SubBytes on the buffer:

SubBytes(8d) = 5d (from S box)
SubBytes(29) = a5 (from S box)
SubBytes(2f) = 15 (from S box)
SubBytes(7f) = d2

So new buffer is 5da515d2, after subbytes.

XOR with Rcon[36/4] = Rcon[9].

Here are the Rcon values in hex:

I	1	2	3	4	5	6	7	8	9	10
Rcon [i]	01000000	02000000	04000000	08000000	10000000	20000000	40000000	80000000	1B000000	36000000

Our example:

5da515d2 XOR 1b000000 (since round 9)

46a515d2, this is our new buffer (for temp)

Finally to get w[i], we have to XOR it with w[i-4], so I need to give you the value of w[32].

For this example w[32] = ead27321

4 6 a 5 1 5 d 2
e a d 2 7 3 2 1
----
a c 7 7 6 6 f 3

Sbox program verification

Input: f3e = 1111 0011 1110

Sbox1(111100) = row 10 = 2, col = 1110 = 14

For Quiz

Preprint all the necessary tables.
DES tables
AES tables
Bin->Hex chart