# AES #1

Wednesday, October 7, 2020 11:31 AM

128 bit key
128 bit block
10 rounds
Will have Round keys just like DES

AES has a state matrix

| | | | |
|---|---|---|---|
| b1 | b5 | b9 | b13 |
| b2 | b6 | b10 | b14 |
| b3 | b7 | b11 | b15 |
| b4 | b8 | b12 | b16 |

in some books they will write it this way:

| | | | |
|---|---|---|---|
| b0,0 | b0,1 | b0,2 | b0,3 |
| b1,0 | b1,1 | b1,2 | b1,3 |
| b2,0 | b1,2 | b2,2 | b2,3 |
| b3,0 | b1,3 | b3,2 | b3,3 |

b means byte. A byte is 8 bits, usually in most books the byte is represented as 2 Hex characters.

Before we start the rounds, we add the Round 0 key (which is the original key.

Add Round Key just means XOR all the bytes. (Round 0 key)
Note: Round 0 key is the original key.

Rounds 1-9 are full rounds
---

a) Sub bytes
b) Shift rows
c) Mix columns

d) Add round key

Round 10
---
a) Sub bytes
b) Shift rows
c) Add round key

Sub Bytes
---
There is a table…for each byte, it tells us which byte to substitute!

Let's say here is our state matrix:

| | | | |
|---|---|---|---|
| 00 | 01 | 02 | 22 |
| 23 | 24 | 25 | 80 |
| 81 | 82 | a1 | a2 |
| b3 | b4 | b5 | ff |

After sub bytes it will look like this:

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

The s-boxes were created in a mathematical way. It uses a field from number theory (group theory). I will mention this later.

Shift Rows
---
First row is unchanged.
Second row is cyclically shifted to the left by 1 byte
Third row is cyclically shifted to the left by 2 bytes
Fourth row is cyclically shifted to the left by 3 bytes.

| | | | |
|---|---|---|---|
| b1 | b5 | b9 | b13 |

| | | | |
|---|---|---|---|
| b2 | b6 | b10 | b14 |
| b3 | b7 | b11 | b15 |
| b4 | b8 | b12 | b16 |

-->

| | | | |
|---|---|---|---|
| b1 | b5 | b9 | b13 |
| b6 | b10 | b14 | b2 |
| b11 | b15 | b3 | b7 |
| b16 | b4 | b8 | b12 |

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

-->

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

Mix columns
---
This step is tough…will come back to in a couple minutes…

Add Round key
---
Just XOR each byte of the state matrix with each byte of the key for that round.

Mix columns
---
The entire basis of the security of AES is based on the mathematical field, GF($2^8$) with the irreducible polynomial

$$x^8 + x^4 + x^3 + x + 1$$

A byte is not interpreted as a binary number in AES, it is interpreted as a special polynomial of at most degree 7.

When you see 63 = 0110 0011, this doesn't mean 63, what it really means is

$$x^6 + x^5 + x + 1$$

We think of 63 (in binary) = 99 (in decimal) = $2^6 + 2^5 + 2 + 1$
So just think of replacing 2 with x to make it a polynomial…

What GF($2^8$) means is that there are 8 coefficients, and each of those 8 coefficients is chosen from a set of 2 values {0,1}.

So we can define addition, subtraction and multiplication on these polynomials and our system must have closure…all answers must be a valid polynomial as well.

Way we do this: calculate coefficients mod 2, which is essentially similar to XOR:

$(x^6 + x^5 + x + 1) + (x^3 + x^2 + x) =$

$(x^6 + x^5 + x^3 + x^2 + 2x + 1)$ now reduce coefficients mod 2

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

Note: subtraction is IDENTICAL to ADDITION and both are essentially like XOR.

Tricky thing is multiplication:

$(x+1)(x^6 + x^5 + x + 1) =$

$(x^7 + x^6 + x^2 + x) + (x^6 + x^5 + x + 1) =$
$= x^7 + 2x^6 + x^5 + x^2 + 2x + 1$
$= x^7 + x^5 + x^2 + 1$

So, multiplying by x is USUALLY leftshifting the byte by 1. Multiplying by (x+1) is taking the byte leftshifted by 1 and then XORing to the byte itself.

0110 0011
1100 0110
---
1010 0101 , identical work, displayed differently.

What problem occurs with multiplication?

Consider:

$x(x^7 + x^5 + x^2 + 1) =$

$x^8 + x^6 + x^3 + x$

What is the problem?

Problem is $x^8$ doesn't fit in the byte!!! It's an overflow.

What AES does is calculate this term MOD the AES polynomial…

$x^8 + x^6 + x^3 + x \bmod x^8 + x^4 + x^3 + x + 1$

All the terms less than $x^8$ stay as the same term under this mod

$x^8$ equivalent to $x^4 + x^3 + x + 1 \bmod x^8 + x^4 + x^3 + x + 1$

So, when you see $x^8$ in AES, just replace with $x^4 + x^3 + x + 1$.

$x(x^7 + x^5 + x^2 + 1) =$

$x^8 + x^6 + x^3 + x =$

$(x^4 + x^3 + x + 1) + x^6 + x^3 + x =$
$x^6 + x^4 + 1$

1010 0101 mult by 2

1 0100 1010 this equals

0100 1010
0001 1011
---
0101 0001, this work is the exact same as the work above.

$(x+1)(x^7 + x^5 + x^2 + 1) =$

$x(x^7 + x^5 + x^2 + 1) + (x^7 + x^5 + x^2 + 1) =$
$x^6 + x^4 + 1 + (x^7 + x^5 + x^2 + 1) =$
$x^7 + x^6 + x^5 + x^4 + x^2$

This is 03 x A5 = F4

Mix columns is a matrix multiplication in the field by a fixed matrix:

| | | | |
|---|---|---|---|
| 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 |

So for example, the entry in row 1, column 2 would be

02 x 7c + 03 x 3f + 01 x 1a + 01 x 4b

02 x 7c = 0111 1100 times x = 1111 1000 (F8)

03 x 3f = 02 x 3f + 3f

02 x 3f = 0011 1111 times x = 0111 1110

3f = 0011 1111

---

0100 0001 (41)

= (f8 + 41) + (1a + 4b)
= b9 + 51
= e8

1111 1000
0100 0001
---
1011 1001 (b9)

0001 1010
0100 1011
---
0101 0001 (51)

1011 1001
0101 0001
---
1110 1000 (e8)