CIS 3362 10/12/22

AES Key Schedule

QUIZ 3 - Will Get 4 Reference Sheets

1. R_0 key IS the key for the alg.

$\Rightarrow$ use to XOR w/ Plaintext in very beginning

R_0 key is $w[0]w[1]w[2]w[3]$

In general R_i key is $w[4i]w[4i+1]w[4i+2]w[4i+3]$

Pseudo Code for rounds 1 to 10

```
for (i=4; i<44; i++) {
    temp = ~~w[i-1]~~ w[i-1]
    if (i%4 == 0)
        temp = SubWord(RotWord(temp)) ⊕ (Rcon[i/4] 000000)
    w[i] = w[i-4] ⊕ temp
}
```

if i isn't divisible by 4, we just do

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

Example w[12] = 01 23 45 67

w[15] = 89 ab cd ef

mostly same

goal calculate w[16]

Original	RotWord	SubWord	Rcon	temp	ans
89 ab cd ef	ab cd ef 89	62 bd df a7	08000000	6a bd df a7	6B9E9A C0

RotWord = cyclic left shift by one byte

SubWord = S-box lookup

w[12] = 01 23 45 67

6a BD DF A7

6B 9E 9A C0

Rules for a field in typed notes

Now AES Field.

Polynomial $= c_d x^d + c_{d-1} x^{d-1} + c_{d-2} x^{d-2} + \cdots c_1 x x^1 + c_0$

example $3x^4 - 6x^2 + 4x + 2$

limit all coefficients to be a remainder when divided by n, so if $n=4$, only valid coeff are 0, 1, 2 and 3

Under mod 3 for coeff. is just $\underline{X+2}$ (terms $3x^4, -6x^2$ disappear since $3 \equiv -6 \equiv 0 \pmod 3$)

In AES all poly coeff are MOD 2.
(every coeff is 0 or 1)

byte = A5 = 10100101
$= x^7 + x^5 + x^2 + 1$ is what that <u>MEANS</u>.

(every byte is a poly w/max deg 7 all coeff 0 or 1)

Adding polynomials under mod 2 is <u>IDENTICAL</u> to XORing them!

AES polynomials are mod 2 coeff

<u>AND</u> mod $x^8+x^4+x^3+x+1$

Divide a by b $= a = bq+r$, q = quotient, r = remainder

Divide $a(x)$ by $b(x)$ $\rightarrow a(x) = b(x)q(x)+r(x)$, $\deg r(x) < \deg b(x)$

$$\begin{array}{r|l} & x^2 \qquad +1 \\ \hline x^2+x+1 & x^4+x^3 \qquad +1 \\ & -x^4+x^3+x^2 \\ \hline & \qquad x^2+1 \\ & \quad -x^2+x+1 \\ \hline & \qquad \boxed{x} \end{array}$$

Quotient $= x^2+1$

Remainder $= x$

$$\underbrace{x^4+x^3+1}_{a} = \underbrace{(x^2+x+1)}_{b}\underbrace{(x^2+1)}_{q} + \underbrace{x}_{r}$$

In AES all operations are mod $x^8+x^4+x^3+x+1$

$\Longrightarrow$ if $\deg < 8$ mod makes no changes

$$\begin{array}{r|l} & \quad 1 \\ \hline m(x) = x^8+x^4+x^3+x+1 & x^8 \\ & -x^8+x^4+x^3+x+1 \\ \hline & \quad x^4+x^3+x+1 \end{array}$$ Remainder

$x^8 \equiv x^4+x^3+x+1 \pmod{m(x)}$

IRREDUCIBLE] Can't write it as the product of 2 polys degree 1 or higher.

To Do Larger Calc

$$(x^5+x^4+1)(x^6+x^3) = x^6+x^5+x^2+x+1$$

$$\begin{aligned} = \; & x^{11} + x^8 \\ & x^{10} + x^7 \\ & + x^6 + x^3 \end{aligned}$$

$$\begin{array}{r} 11011000 \\ 01101100 \\ 00011011 \\ 11001000 \\ \hline 01100111 \end{array}$$

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

$$x^{10} = x^2 x^8 = x^2(x^4+x^3+x+1) = x^6+x^5+x^3+x^2$$

$$x^{11} = x \cdot x^{10} = x^7+x^6+x^4+x^3$$