AES Key Schedule

1. $R_0$ key is the key for the alg.

   ⇒ 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

```plaintext
for (i = 4, i < 44, i++) {
    temp = $w[i-17]
    if (i % 4 == 0)
        temp = SubWord(RotWord(temp)) ⊕ (Rcon $[i/4]000000$)
    $w[i] = w[i-47] ⊕$ temp
}
```

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

Example: \( w[12] = 01\ 23\ 45\ 67 \)
\( w[15] = 89\ ab\ cd\ ef \)

Goal: Calculate \( w[16] \)

<table>
<thead>
<tr>
<th>Original</th>
<th>RotWord</th>
<th>SubWord</th>
<th>Reun.</th>
<th>Temp</th>
<th>Ans</th>
</tr>
</thead>
<tbody>
<tr>
<td>89\ ab\ cd\ ef</td>
<td>ab\ cd\ ef\ 89</td>
<td>62\ bd\ df\ a7</td>
<td>08000000</td>
<td>6a\ bd\ df\ a7</td>
<td>6B9E9A7C0</td>
</tr>
</tbody>
</table>

**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 = \( c_d x^d + c_{d-1} x^{d-1} + c_{d-2} x^{d-2} + \ldots + c_1 x + c_0 \)

**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 \( x + 2 \) (terms \( 3x^4, -6x^2 \) disappear since \( 3 \equiv -6 \equiv 0 \) (mod 3))

In AES all poly coeff are \( \text{MOD} 2 \).
- Every coeff is 0 or 1

\( \text{byte} = \text{AS} = 10100101 \)
- \( = x^7 + x^5 + x^2 + 1 \) is what that \( \underline{\text{MEANS}} \)

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

Adding polynomials under \( \text{mod} 2 \) is \( \underline{\text{IDENTICAL}} \) to XORing them!
AES polynomials are \( \mod 2 \) where

\[ \mod \ x^8 + x^4 + x^3 + x + 1 \]

Divide a by \( b \) \( \Rightarrow \) \( q \cdot b + r \), \( q \) = quotient, \( r \) = remainder

Divide \( q(x) \) by \( b(x) \) \( \Rightarrow \) \( q(x) = b(x)q(x) + r(x) \), \( \deg r(x) \leq \deg b(x) \)

\[
\begin{array}{c|c}
\hline
x^2 + 1 & x^2 + 1 \\
\hline
- x^2 + x^3 + x^2 + 1 & \text{Quotient} = x^2 + 1 \\
\hline
\hline
q & r \\
\hline
\end{array}
\]

\( x^4 + x^3 + 1 = (x^2 + x + 1)(x^2 + 1) + x \)

In AES all operations are \( \mod \)

\[
\begin{array}{c|c}
\hline
x^8 + x^4 + x^3 + x + 1 & 1 \\
\hline
- x^{q + x}x^{3 + x} + 1 & \text{Remainder} \equiv x^4 + x^3 + 1 \pmod{m(x)} \\
\hline
\end{array}
\]

\( x^6 \equiv x^{4 + x^3 + x} + 1 \pmod{m(x)} \) is irreducible and can't break it as the product of 2 polynomials degree 1 or higher.
To Do Larger Calc

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

\[ x^6 + x^3 \]

\[ x^{10} + x^7 + x^6 + x^3 \]

\[ x^8 + x^3 + x^2 + 1 \]

\[ x^{10} = x^2 \cdot x^8 = x^2 (x^4 + x^3 + x + 1) = x^6 + x^5 + x^3 + x^2 \]

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