

Listing 1

```
KeyExpansion(key[], w[4*(Nr*4)], key_size)
{
```

Copy the key to the first values of the key schedule

```
for (i=0; i < key_size; i++) {
    w[i] = word(key[4*i], key[4*i+1], key[4*i+2], key[4*i+3])
}
```

Expand the rest of the key schedule values

```
for (i=key_size; i < (4 * Nr * 4); i++) {
    temp = w[i-1]
    if (i mod key_size == 0)
        temp = SubWord(RotWord(temp)) xor Rcon[ i / key_size ]
    else if ((key_size > 6) and (i mod key_size == 4))
        temp = SubWord(temp)

    w[i] = w[ i - key_size ] xor temp
}
}
```