Caballero Huesca Carlos Eduardo 11 de octubre de 2016

Implementación AES. Generar Sub llaves (Expandir llaves).

```
for (int i = 0; i < 4; i++){
    for (int j = 0; j < 4; j++){
    mClaveExp[k] = arrClave[j][i];
    k++;
        }
    }
```

Pasamos la clave a las primeras posiciones de clave expandida

```
for(i=4;i < 44;i++){
    for( j = 0; j < 4; j++){
    copia[j] = mClaveExp[(i-1) * 4 + j];
    }
```

Metemos la última columna en copia

```
if (i % 4 == 0){
    copia2 = copia[0];
    copia[0] = copia[1];
    copia[1] = copia[2];
    copia[2] = copia[3];
    copia[3] = copia2;
```

Hacemos el corrimiento cada 4 filas.

```
    copia[0] = valorCajaS(copia[0]);
    copia[1] = valorCajaS(copia[1]);
    copia[2] = valorCajaS(copia[2]);
    copia[3] = valorCajaS(copia[3]);
```

Aplicamos la caja S a cada uno de los 4 bytes

```
    copia[0] =  copia[0] ^ rCon[i/4];
```

Hacemos XOR con el primer byte

```
mClaveExp[i*4+0] = mClaveExp[(i-4)*4+0] ^ copia[0];
mClaveExp[i*4+1] = mClaveExp[(i-4)*4+1] ^ copia[1];
mClaveExp[i*4+2] = mClaveExp[(i-4)*4+2] ^ copia[2];
mClaveExp[i*4+3] = mClaveExp[(i-4)*4+3] ^ copia[3];
```

XOR entre el resultado anterior y Ci