

Simplified AES

Example

Steven Gordon

1 Simplified AES Example

Lets assume the inputs for the encryption are:

16-bit Plaintext, P : 1101 0111 0010 1000

16-bit Key, K : 0100 1010 1111 0101

1.1 Key Generation

The first step is to generate the sub-keys. This is called *Key Generation* or *Key Expansion*:

The input key, K , is split into 2 words, w_0 and w_1 :

$w_0 = 0100\ 1010$

$w_1 = 1111\ 0101$

The first sub-key, Key_0 , is in fact just the input key: $Key_0 = w_0w_1 = K$

The other sub-keys are generated as follows:

$w_2 = w_0 \text{ XOR } 10000000 \text{ XOR } \text{SubNib}(\text{RotNib}(w_1))$

(Note: RotNib() is “rotate the nibbles”, which is equivalent to swapping the nibbles)

$= 0100\ 1010 \text{ XOR } 10000000 \text{ XOR } \text{SubNib}(0101\ 1111)$

(Note: SubNib() is “apply S-Box substitution on nibbles using encryption S-Box”)

$= 1100\ 1010 \text{ XOR } \text{SubNib}(0101\ 1111)$

$= 1100\ 1010 \text{ XOR } 0001\ 0111$

$= 1101\ 1101$

$w_3 = w_2 \text{ XOR } w_1$

$= 1101\ 1101 \text{ XOR } 1111\ 0101$

$= 0010\ 1000$

$w_4 = w_2 \text{ XOR } 0011\ 0000 \text{ XOR } \text{SubNib}(\text{RotNib}(w_3))$

$= 1101\ 1101 \text{ XOR } 0011\ 0000 \text{ XOR } \text{SubNib}(1000\ 0010)$

$= 1110\ 1101 \text{ XOR } 0110\ 1010$

$= 1000\ 0111$

$w_5 = w_4 \text{ XOR } w_3$

$= 1000\ 0111 \text{ XOR } 0010\ 1000$

$= 1010\ 1111$

Now the sub-keys are:

$$\begin{aligned} \text{Key}_0 &= w_0w_1 \\ &= 0100\ 1010\ 1111\ 0101 \end{aligned}$$

$$\begin{aligned} \text{Key}_1 &= w_2w_3 \\ &= 1101\ 1101\ 0010\ 1000 \end{aligned}$$

$$\begin{aligned} \text{Key}_2 &= w_4w_5 \\ &= 1000\ 0111\ 1010\ 1111 \end{aligned}$$

1.2 Encryption

Now let's do the encryption. There is an initial operation (Add Round Key), followed by the main Round, followed by the final Round. (Note, the main difference in the real DES is that the main Round is repeated many times).

Remember, the output of each operation is used as the input to the next operation, always operating on 16-bits. The 16-bits can be viewed as a state matrix of nibbles.

1.2.1 Add Round 0 Key

$$\begin{aligned} \text{Plaintext XOR Key}_0 &= \\ &= \begin{array}{cccc} 1101 & 0111 & 0010 & 1000 \end{array} \text{ XOR } \\ &\quad \begin{array}{cccc} 0100 & 1010 & 1111 & 0101 \end{array} \\ &= \begin{array}{cccc} 1001 & 1101 & 1101 & 1101 \end{array} \end{aligned}$$

1.2.2 Round 1

Nibble Substitution (S-boxes). Each nibble in the input is used in the Encryption S-Box to generate an output nibble.

$$\begin{aligned} \text{Input} &= \begin{array}{cccc} 1001 & 1101 & 1101 & 1101 \end{array} \\ \text{Output} &= \begin{array}{cccc} 0010 & 1110 & 1110 & 1110 \end{array} \end{aligned}$$

Shift Row. Swap 2nd nibble and 4th nibble (note, in this example, its not so easy to see since 2nd and 4th nibbles are the same!)

$$= \begin{array}{cccc} 0010 & 1110 & 1110 & 1110 \end{array}$$

Mix Columns. Apply the matrix multiplication with the constant matrix, M_e , using $\text{GF}(2^4)$. For $\text{GF}(2^4)$, the addition operation is simply an XOR, and for the multiplication operation you can use a lookup table.

$$M_e = \begin{array}{cc} 1 & 4 \\ 4 & 1 \end{array}$$

$$S = \begin{array}{cc} 0010 & 1110 \\ 1110 & 1110 \end{array} = \begin{array}{cc} S_{00}' & S_{01}' \\ S_{10}' & S_{11}' \end{array}$$

$$S' = M_e \times S$$

$$\begin{aligned} S_{00}' &= 0010 \text{ XOR } (4 \times 1110) \\ &= 0010 \text{ XOR } (4 \times E) \\ &= 0010 \text{ XOR } D \\ &= 0010 \text{ XOR } 1101 \\ &= 1111 \end{aligned}$$

$$\begin{aligned} S_{10}' &= (4 \times 0010) \text{ XOR } 1110 \\ &= 1000 \text{ XOR } 1110 \\ &= 0110 \end{aligned}$$

$$\begin{aligned} S_{01}' &= 1110 \text{ XOR } (4 \times 1110) \\ &= 1110 \text{ XOR } (4 \times E) \\ &= 1110 \text{ XOR } 1101 \\ &= 0011 \end{aligned}$$

$$\begin{aligned} S_{11}' &= (4 \times 1110) \text{ XOR } 1110 \\ &= 1101 \text{ XOR } 1110 \\ &= 0011 \end{aligned}$$

$$\begin{aligned} \text{Output} &= S_{00}' S_{10}' S_{01}' S_{11}' \\ &= 1111 \ 0110 \ 0011 \ 0011 \end{aligned}$$

Add Round 1 Key.

$$\begin{aligned} &= 1111 \ 0110 \ 0011 \ 0011 \text{ XOR} \\ &\quad 1101 \ 1101 \ 0010 \ 1000 \\ &= 0010 \ 1011 \ 0001 \ 1011 \end{aligned}$$

1.2.3 Final Round

Nibble Substitution (S-boxes)

$$= 1010 \ 0011 \ 0100 \ 0011$$

Shift Row (2nd and 4th)

$$= 1010 \ 0011 \ 0100 \ 0011$$

Add Round 2 Key

$$\begin{aligned} &\quad 1010 \ 0011 \ 0100 \ 0011 \text{ XOR} \\ &\quad 1000 \ 0111 \ 1010 \ 1111 \\ &= 0010 \ 0100 \ 1110 \ 1100 \end{aligned}$$

Now we have the final ciphertext.

$$\text{Ciphertext} = 0010 \ 0100 \ 1110 \ 1100$$

1.3 Decryption

Now let's decrypt. Note that we use the same keys generated during the encryption (that is, the decryptor would generate the round sub-keys using the input key K , *using the encryption S-Box*).

Add Round 2 Key

$$\begin{array}{rcl}
 & 0010 & 0100 & 1110 & 1100 & \text{XOR} \\
 & 1000 & 0111 & 1010 & 1111 & \\
 = & 1010 & 0011 & 0100 & 0011 &
 \end{array}$$

Inverse Shift Row (same as normal)

$$= 1010 \ 0011 \ 0100 \ 0011$$

Inverse Nibble Sub (use the inverse or decryption S-box)

$$= 0010 \ 1011 \ 0001 \ 1011$$

Add Round 1 Key

$$\begin{array}{rcl}
 = & 0010 & 1011 & 0001 & 1011 & \text{XOR} \\
 & 1101 & 1101 & 0010 & 1000 & \\
 = & 1111 & 0110 & 0011 & 0011 &
 \end{array}$$

Inverse Mix Columns

$$\begin{array}{rcl}
 S & = & \begin{array}{cc} S_{00} & S_{01} \\ S_{10} & S_{11} \end{array}
 \end{array}$$

$$= \begin{array}{cc} 1111 & 0011 \\ 0110 & 0011 \end{array}$$

$$\begin{array}{rcl}
 S' & = & \begin{array}{cc} S_{00}' & S_{01}' \\ S_{10}' & S_{11}' \end{array} \\
 & = & \begin{array}{cc} 9 \times S_{00} \text{ XOR } 2 \times S_{10} & 9 \times S_{01} \text{ XOR } 2 \times S_{11} \\ 2 \times S_{00} \text{ XOR } 9 \times S_{10} & 2 \times S_{01} \text{ XOR } 9 \times S_{11} \end{array}
 \end{array}$$

$$\begin{array}{rcl}
 S_{00}' & = & (9 \times 1111) \text{ XOR } (2 \times 0110) \\
 & = & 9 \times F \text{ XOR } 2 \times 6 \\
 & = & E \text{ XOR } C \\
 & = & 1110 \text{ XOR } 1100 \\
 & = & 0010
 \end{array}$$

$$\begin{array}{rcl}
 S_{10}' & = & 2 \times 1111 \text{ XOR } 9 \times 0110 \\
 & = & 2 \times F \text{ XOR } 9 \times 6 \\
 & = & D \text{ XOR } 3 \\
 & = & 1101 \text{ XOR } 0011 \\
 & = & 1110
 \end{array}$$

$$\begin{array}{rcl}
 S_{01}' & = & 9 \times 0011 \text{ XOR } 2 \times 0011 \\
 & = & 9 \times 3 \text{ XOR } 2 \times 3 \\
 & = & 8 \text{ XOR } 6 \\
 & = & 1000 \text{ XOR } 0110 \\
 & = & 1110
 \end{array}$$

$$\begin{aligned} S_{II}' &= 2 \times 0011 \text{ XOR } 9 \times 0011 \\ &= 1110 \end{aligned}$$

$$\text{Output} = 0010 \ 1110 \ 1110 \ 1110$$

$$\begin{aligned} \text{Inverse Shift Row} \\ &= 0010 \ 1110 \ 1110 \ 1110 \end{aligned}$$

$$\begin{aligned} \text{Inverse Nibble Sub} \\ &= 1001 \ 1101 \ 1101 \ 1101 \end{aligned}$$

$$\begin{aligned} \text{Add Round 0 Key} \\ &= 1001 \ 1101 \ 1101 \ 1101 \text{ XOR} \\ &\quad 0100 \ 1010 \ 1111 \ 0101 \\ &= 1101 \ 0111 \ 0010 \ 1000 \end{aligned}$$

$$\text{Plaintext} = 1101 \ 0111 \ 0010 \ 1000$$

$$\text{Original} = 1101 \ 0111 \ 0010 \ 1000$$

The decryption worked!