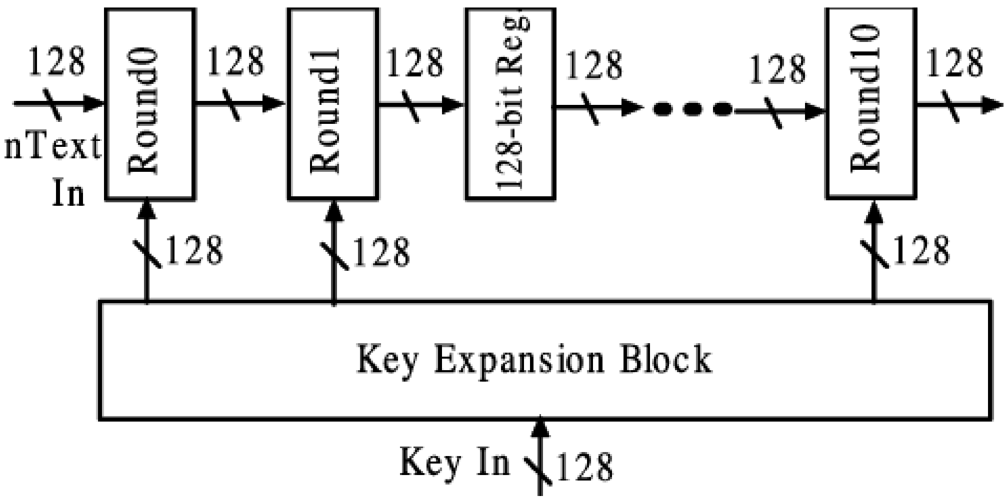
[CS304] Introduction to Cryptography and Network Security

Course Instructor: Dr. Dibyendu Roy — Winter 2023-2024

Scribed by: Priyansh Vaishnav (202151120) — Lecture 8 & 9 (Week 4)

LECTURE 8 — Date: - 13th Feb 2024

Advanced Encryption Standard:



Round Function of AES-128:

In AES-128, there are 10 round functions. The first nine functions, $f_1 = f_2 = f_3 = \ldots = f_9$, are identical, while the 10th function is different.

These nine functions consist of the following steps:

1. SubBytes
2. ShiftRows
3. MixColumns

The 10th function does not include MixColumns. If there are n round functions in AES, then $(n-1)$ functions will be the same.

SubByte:

$$S : \{0,1\}^{128} \rightarrow \{0,1\}^{128}$$

1. Let $X = x_0x_1x_2 \ldots x_{15}$, where size of $x_i =$ 8bit.

$$\begin{bmatrix} x_0 & x_4 & x_8 & x_{12} \\ x_1 & x_5 & x_9 & x_{13} \\ x_2 & x_6 & x_{10} & x_{14} \\ x_3 & x_7 & x_{11} & x_{15} \end{bmatrix} \longrightarrow \begin{bmatrix} s_{00} & s_{01} & s_{02} & s_{03} \\ s_{10} & s_{11} & s_{12} & s_{13} \\ s_{20} & s_{21} & s_{22} & s_{23} \\ s_{30} & s_{31} & s_{32} & s_{33} \end{bmatrix}$$

*Method: $S : \{0,1\}^{128} \to \{0,1\}^{128}$, where S is defined as:

$$\text{Let's say } (c_7\ c_6\ c_5\ c_4\ c_3\ c_2\ c_1\ c_0) \leftarrow (01100011)$$

- $S(s_{ij}) = (a_7\ a_6\ a_5\ a_4\ a_3\ a_2\ a_1\ a_0)$
- For $i = 0$ to 7:

$$b_i = (a_i \oplus a_{(i+4)\%8} \oplus a_{(i+5)\%8} \oplus a_{(i+6)\%8} \oplus a_{(i+7)\%8} \oplus c_i) \mod 2$$

- $(b_7\ b_6\ b_5\ b_4\ b_3\ b_2\ b_1\ b_0) = s'_{ij}$

$$\begin{bmatrix} s_{00} & s_{01} & s_{02} & s_{03} \\ s_{10} & s_{11} & s_{12} & s_{13} \\ s_{20} & s_{21} & s_{22} & s_{23} \\ s_{30} & s_{31} & s_{32} & s_{33} \end{bmatrix} \longrightarrow \begin{bmatrix} s'_{00} & s'_{01} & s'_{02} & s'_{03} \\ s'_{10} & s'_{11} & s'_{12} & s'_{13} \\ s'_{20} & s'_{21} & s'_{22} & s'_{23} \\ s'_{30} & s'_{31} & s'_{32} & s'_{33} \end{bmatrix}$$

*Ex: If $S(0) = 0 = (0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ )$ then b will be $(0\ 1\ 1\ 0\ 0\ 0\ 1\ 1\ )$ *Standard Form:

- $S : \{0,1\}^{128} \to \{0,1\}^{128}$
- $S(X) = Y$, where $X = (a_7\ a_6\ a_5\ a_4\ a_3\ a_2\ a_1\ a_0)$ and $a_i \in \{0,1\}$
- $P(X) = a_0 + a_1x + a_2x^2 + \ldots + a_7x^7$
- $\deg(P(X)) < 8$

Now we have to find the multiplicative inverse of $P(X)$ under modulo $(x^8 + x^4 + x^3 + x + 1)$.
So, we have $P(X) \cdot q(X) \equiv 1 \mod (x^8 + x^4 + x^3 + x + 1)$.
This can be expressed as:

$$P(X) \cdot q(X) = 1 + h(X) \cdot (x^8 + x^4 + x^3 + x + 1)$$

Therefore,

$$1 = P(X) \cdot q(X) + h'(X) \cdot (x^8 + x^4 + x^3 + x + 1)$$

*Example: - Let $S = 01010011$. The corresponding polynomial $P(X)$ is:

$$P(X) = x^6 + x^4 + x^2 + x + 1$$

Given that $g(X) = x^8 + x^4 + x^3 + x + 1$, you can use polynomial division to find $q(X)$:

$$q(X) = \frac{g(X)}{P(X)}$$

Step 1:

$$1 = x^2 + (x + 1)(x + 1)$$

Step 2:

$$1 = x^2 + \{(x^6 + x^4 + x + 1) + x^2 \cdot (x^4 + x^2)\} \cdot (x + 1)$$

Step 3:

$$1 = (x + 1) \cdot (x^6 + x^4 + x + 1) + x^2\{1 + (x + 1) \cdot (x^4 + x^2)\}$$

Step 4:

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

Step 5:

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

Step 6:

$$1 = (x^6 + x^4 + x + 1) \cdot (x^7 + x^6 + x^3 + x) + (1 + x^5 + x^4 + x^3 + x^2) \cdot (x^8 + x^4 + x^3 + x + 1)$$

Thus, $(x^7 + x^6 + x^3 + x)$ is the inverse of $(x^6 + x^4 + x + 1)$ under modulo $(x^8 + x^4 + x^3 + x + 1)$.
Given $S(0\ 1\ 0\ 1\ 0\ 0\ 1\ 1\ ) = 1\ 1\ 0\ 0\ 1\ 0\ 1\ 0$
$SubByte(53) = ED$

ShiftRow:

$S : \{0, 1\}^{128} \rightarrow \{0, 1\}^{128}$

$$\begin{bmatrix} s_{00} & s_{01} & s_{02} & s_{03} \\ s_{10} & s_{11} & s_{12} & s_{13} \\ s_{20} & s_{21} & s_{22} & s_{23} \\ s_{30} & s_{31} & s_{32} & s_{33} \end{bmatrix} \longrightarrow \begin{bmatrix} s'_{00} & s'_{01} & s'_{02} & s'_{03} \\ s'_{11} & s'_{12} & s'_{13} & s'_{10} \\ s'_{22} & s'_{23} & s'_{20} & s'_{21} \\ s'_{33} & s'_{30} & s'_{31} & s'_{32} \end{bmatrix}$$

In the first row, there will be no change. In the second row, elements are right-shifted by 1 in a loop. In the third row, elements are right-shifted by 2 in a loop. In the fourth row, elements are right-shifted by 3 in a loop.

MixColumns Operation

The MixColumns operation in AES transforms the 4×4 state matrix $[s_{ij}]$ into a new state matrix $[s'_{ij}]$.

For each column $c \in \{0, 1, 2, 3\}$:
For $i = 0$ to 3:

1. Convert the elements of column c to polynomials:

$$t_0 = \text{Binary to Polynomial } (s_{0c})$$
$$t_1 = \text{Binary to Polynomial } (s_{1c})$$
$$t_2 = \text{Binary to Polynomial } (s_{2c})$$
$$t_3 = \text{Binary to Polynomial } (s_{3c})$$

2. Perform the following polynomial multiplication and reduction modulo $x^8 + x^4 + x^3 + x + 1$:

$$u_0 = [(x \cdot t_0 + (x + 1) \cdot t_1 + 1 \cdot t_2 + 1 \cdot t_3)] \bmod (x^8 + x^4 + x^3 + x + 1)$$
$$u_1 = [(x \cdot t_2 + (x + 1) \cdot t_3 + 1 \cdot t_0 + 1 \cdot t_1)] \bmod (x^8 + x^4 + x^3 + x + 1)$$

3. Convert the resulting polynomials u_0 and u_1 back to binary:

$$s'_{0c} = \text{Polynomial to Binary } (u_0)$$
$$s'_{1c} = \text{Polynomial to Binary } (u_1)$$

The MixColumns operation can also be represented as a matrix multiplication:

$$\begin{bmatrix} x & x+1 & 1 & 1 \\ 1 & x & x+1 & 1 \\ 1 & 1 & x & x+1 \\ x+1 & 1 & 1 & x \end{bmatrix} \times \begin{bmatrix} s_{00} & s_{01} & s_{02} & s_{03} \\ s_{10} & s_{11} & s_{12} & s_{13} \\ s_{20} & s_{21} & s_{22} & s_{23} \\ s_{30} & s_{31} & s_{32} & s_{33} \end{bmatrix} = \begin{bmatrix} s'_{00} & s'_{01} & s'_{02} & s'_{03} \\ s'_{10} & s'_{11} & s'_{12} & s'_{13} \\ s'_{20} & s'_{21} & s'_{22} & s'_{23} \\ s'_{30} & s'_{31} & s'_{32} & s'_{33} \end{bmatrix}$$

. . . .

LECTURE 9 Date: - 16th Feb 2024

. . . .

The MixColumn can also be represent in decimal form:

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \times \begin{bmatrix} s_{00} & s_{01} & s_{02} & s_{03} \\ s_{10} & s_{11} & s_{12} & s_{13} \\ s_{20} & s_{21} & s_{22} & s_{23} \\ s_{30} & s_{31} & s_{32} & s_{33} \end{bmatrix} = \begin{bmatrix} s'_{00} & s'_{01} & s'_{02} & s'_{03} \\ s'_{10} & s'_{11} & s'_{12} & s'_{13} \\ s'_{20} & s'_{21} & s'_{22} & s'_{23} \\ s'_{30} & s'_{31} & s'_{32} & s'_{33} \end{bmatrix}$$

where

$$\text{x} = 0\ 0\ 0\ 0\ 0\ 0\ 1\ 0$$
$$\text{x} + 1 = 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1$$
$$1 = 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1$$

Ex.:-

$$\begin{bmatrix} s'_{00} \\ s'_{10} \\ s'_{20} \\ s'_{30} \end{bmatrix} = \begin{bmatrix} x & x+1 & 1 & 1 \\ 1 & x & x+1 & 1 \\ 1 & 1 & x & x+1 \\ x+1 & 1 & 1 & x \end{bmatrix} \times \begin{bmatrix} 95 \\ 65 \\ FD \\ F3 \end{bmatrix}$$

Find s' Matrix
Solution:

$$95 = 1\ 0\ 0\ 1\ 0\ 1\ 0\ 1 = x^7 + x^4 + x^2 + 1$$
$$65 = 0\ 1\ 1\ 0\ 0\ 1\ 0\ 1 = x^6 + x^5 + x^2 + 1$$
$$FD = 1\ 1\ 1\ 1\ 1\ 1\ 0\ 1 = x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1$$
$$F3 = 1\ 1\ 1\ 1\ 0\ 0\ 1\ 1 = x^7 + x^6 + x^5 + x^4 + x + 1$$

1. $s'_{00} = x \cdot (x^7 + x^4 + x^2 + 1) + (x+1) \cdot (x^6 + x^5 + x^2 + 1) + 1 \cdot (x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1) + 1 \cdot (x^7 + x^6 + x^5 + x^4 + x + 1)$
   $s'_{00} = x^7 + x^5 + x^3 + x^2 + 1 = 1\ 0\ 1\ 0\ 1\ 1\ 0\ 1$

2. $s'_{10} = 1 \cdot (x^7 + x^4 + x^2 + 1) + x \cdot (x^6 + x^5 + x^2 + 1) + (x + 1) \cdot (x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1) + 1 \cdot (x^7 + x^6 + x^5 + x^4 + x + 1)$
   $s'_{10} = x^7 + x^5 + x^4 = 0\ 1\ 1\ 0\ 0\ 0\ 0\ 0$

3. $s'_{20} = 1 \cdot (x^7 + x^4 + x^2 + 1) + 1 \cdot (x^6 + x^5 + x^2 + 1) + x \cdot (x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1) + (x + 1) \cdot (x^7 + x^6 + x^5 + x^4 + x + 1)$
   $s'_{20} = x^4 + x^3 + x^2 + x + 1 = 0\ 0\ 0\ 1\ 1\ 1\ 1\ 1$

4. $s'_{30} = (x + 1) \cdot (x^7 + x^4 + x^2 + 1) + 1 \cdot (x^6 + x^5 + x^2 + 1) + 1 \cdot (x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1) + x \cdot (x^7 + x^6 + x^5 + x^4 + x + 1)$
   $s'_{30} = x^7 + x^6 = 1\ 1\ 0\ 0\ 0\ 0\ 0\ 0$

AES-128 bit Key Scheduling Algorithm:

There are 11 Rounds $k_1, k_2, \dots, k_{11}$ Length of each round is 128 bit.
$K = \text{key}[0], \text{key}[1], \dots, \text{key}[15]$ and length of key$[i]$ is 128 bit.

Points to remember:

1. ROTWORD$(B_0, B_1, B_2, B_3) = (B_1, B_2, B_3, B_0)$, where length of B_i is 8 bits.

2. SUBWORD$(B_0, B_1, B_2, B_3) = (B'_0, B'_1, B'_2, B'_3)$.

3. Some Fixed Constants:

   (a) $R_{\text{con}}[1] = 01000000$
   (b) $R_{\text{con}}[2] = 02000000$
   (c) $R_{\text{con}}[3] = 04000000$
   (d) $R_{\text{con}}[4] = 08000000$
   (e) $R_{\text{con}}[5] = 10000000$
   (f) $R_{\text{con}}[6] = 20000000$
   (g) $R_{\text{con}}[7] = 40000000$
   (h) $R_{\text{con}}[8] = 80000000$
   (i) $R_{\text{con}}[9] = 01B00000$
   (j) $R_{\text{con}}[10] = 36000000$

Key Expansion Algorithm: -

KeyExpansion(byte key[16]) , word w[44])
{
word temp
for (i =0;i¡4;i++)
w[i] = (key[4*i],key[4*i+1],key[4*i+2],key[4*i+3]);
for(i=4;i¡44;i++)
{ temp = w[i];
if(i mod 4 == 0)
temp = SUBWORD{ROTWORD(temp) $\oplus$ $R_{con}[i/4]$};

$w[i] = w[i+4] \oplus \text{temp};$
$\}$
$\text{return}(w[0], w[1], \cdots, w[43]);$

Length of $w[i]$ is 32 bit.

$$\begin{aligned}
k_1 &= w[0]\|w[1]\|w[2]\|w[3] \\
k_2 &= w[4]\|w[5]\|w[6]\|w[7] \\
k_3 &= w[8]\|w[9]\|w[10]\|w[11] \\
&\cdots \\
k_{43} &= w[40]\|w[41]\|w[42]\|w[43]
\end{aligned}$$

Properties of AES Operations:

1. **SubByte and ShiftRow Invertibility:** Both SubByte and ShiftRow operations in AES are invertible.

2. **MixColumn Invertibility:** The MixColumn matrix operation in AES must be invertible under modulo $x^8 + x^4 + x^3 + x + 1$.

Modes Of Operarions: -

ECB:

ECB stands for Electronic Code Book.
Input: Key K, n-bit Plaintext $(x_1, x_2, \ldots, x_t)$
Encryption:

1. $\text{Enc}(x_i, K) = C_i$, where $1 \leq i \leq t$

Decryption:

1. $\text{Dec}(C_i, K) = x_i$, where $1 \leq i \leq t$

CBC:

CBC stands for Cipher Block Chaining.
Input: Key K, n-bit Plaintext $(x_1, x_2, \ldots, x_t)$
Encryption:

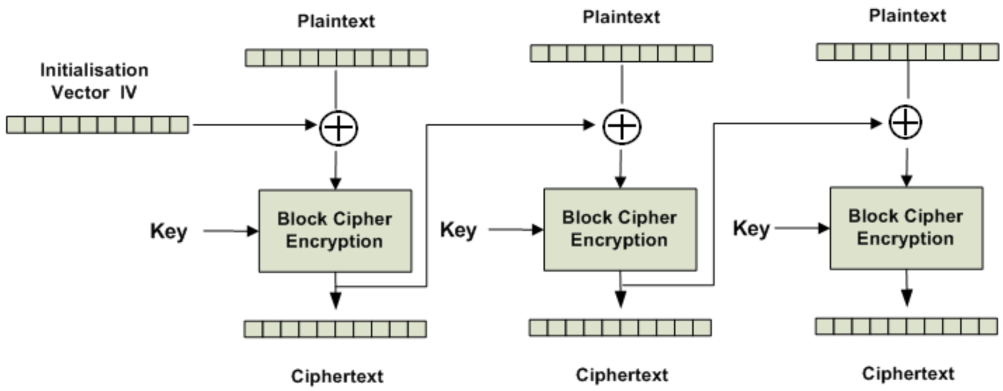
1. $C_0 = IV$ (Public parameter)

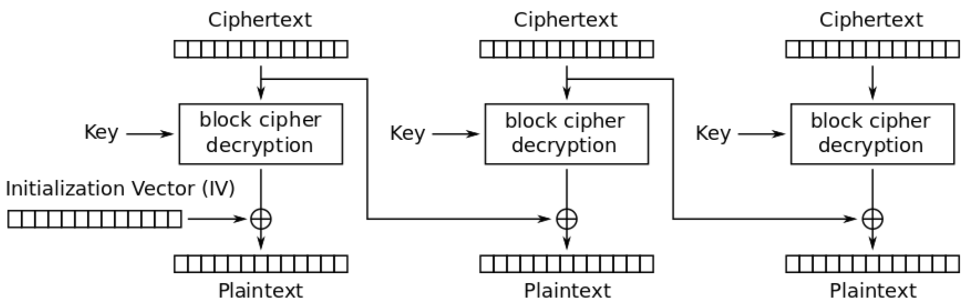
2. $C_j = \text{Enc}(C_{j-1} \oplus x_j, K)$, where $1 \leq j \leq t$

Decryption:

1. $C_0 = IV$

2. $x_j = \text{Dec}(C_j, K) \oplus C_{j-1}$, where $1 \leq i \leq t$





Cipher Block Chaining (CBC) mode decryption

Stream Cipher

Stream ciphers encrypt plaintext bitwise.

Let $M = m_0 m_1 \cdots m_l$ where $m_i \in \{0, 1\}$ be the plaintext and $K = k_0 k_1 \cdots k_l$ where $k_i \in \{0, 1\}$ be the key.

The ciphertext C is obtained by bitwise XOR (exclusive OR) of the plaintext and the key:

$$C = M \oplus K = (m_0 \oplus k_0)(m_1 \oplus k_1) \cdots (m_l \oplus k_l)$$

The encryption and decryption operations are given by:

$$\text{Encryption: } C_i = M_i \oplus K_i$$
$$\text{Decryption: } M = C \oplus K$$

1. $P(M = m_1 | C = Ch_1) = P(M = m_1)$

2. $C = M \oplus K$
$$C_1 = m_1 \oplus K$$
$$C_2 = m_2 \oplus K$$
$$\text{then } C_1 \oplus C_2 = (m_1 \oplus K) \cdot (m_2 \oplus K) = m_1 \oplus m_2$$

3. $K = k_0 k_{l-1} \cdots k_l$; $r = n - l$
   $M = m_0 \cdots m_n$
   $k_1 = K \| \cdots \| k_{r-l}$
   $C = M \oplus K$
   $C'_1 = C_0 \cdots C_{r-1}$

Important Points:

1. The length of the key (K) should be greater than or equal to the length of the message (M).
2. You cannot use the same key to encrypt different messages.
3. The length of the key (K) should be greater than or equal to the length of the message (M).