Ασκηση: Υλοποιηση AES.
Εργασια Φοιτητη: Γιωργος Μπουρλακης

Άσκηση Ασφάλειας Υπολογιστών και Δικτύων πάνω στον AES

Μπουρλάκης Γεώργιος 1054321

[https://en.wikipedia.org/wiki/Rijndael_S-box]

[http://aes.online-domain-tools.com/]

Δεδομένα:

plaintext [**0001 0203 0405 0607 0809 0A0B 0C0D 0E0F**]

key [**0101 0101 0101 0101 0101 0101 0101 0101**]

Ζητούμενα:

- 1 γύρος
- Κατάσταση (state matrix) μετά το αρχικό κλειδί (AddRoundKey)
- Μετά την πράξη SubBytes
- Μετά το ShiftRows
- Μετά την μίξη στηλών MixColumns

w[0] = (01, 01, 01, 01)

w[1] = (01, 01, 01, 01)

w[2] = (01, 01, 01, 01)

w[3] = (01, 01, 01, 01)

g(w[3]):

shift left w[3]: (01, 01, 01, 01)

byte substitution (S-Box): (7C, 7C, 7C, 7C)

adding round constant (01, 00, 00, 00): g(w[3]) = (7B, 7C, 7C, 7C)

w[4] = w[0] ⊕ g(w[3]) = (7A, 7D, 7D, 7D)

w[0]: 00000001 00000001 00000001 00000001

g(w[3]): ⊕ 01111011 01111100 01111100 01111100

01111010 01111101 01111101 01111101 = (7A, 7D, 7D, 7D)

w[5] = w[4] ⊕ w[1] = (7B, 7C, 7C, 7C)

w[4]: 01111010 01111101 01111101 01111101

w[1]: ⊕00000001 00000001 00000001 00000001

01111011 01111100 01111100 01111100 = (7B, 7C, 7C, 7C)

w[6] = w[5] ⊕ w[2] = (7A, 7D, 7D, 7D)

w[5]: 01111011 01111100 01111100 01111100

w[2]: ⊕00000001 00000001 00000001 00000001

01111010 01111101 01111101 01111101 = (7A, 7D, 7D, 7D)

w[7] = w[6] ⊕ w[3] = (7B, 7C, 7C, 7C)

w[6]: 01111010 01111101 01111101 01111101

w[3]: ⊕00000001 00000001 00000001 00000001

01111011 01111100 01111100 01111100 = (7B, 7C, 7C, 7C)

First round key: 7A 7D 7D 7D 7B 7C 7C 7C 7A 7D 7D 7D 7B 7C 7C 7C

State Matrix: $\begin{bmatrix} 00 & 04 & 08 & 0C \\ 01 & 05 & 09 & 0D \\ 02 & 06 & 0A & 0E \\ 03 & 07 & 0B & 0F \end{bmatrix}$ **No.0 Matrix:** $\begin{bmatrix} 01 & 01 & 01 & 01 \\ 01 & 01 & 01 & 01 \\ 01 & 01 & 01 & 01 \\ 01 & 01 & 01 & 01 \end{bmatrix}$

New State Matrix: $\begin{bmatrix} 01 & 05 & 09 & 0D \\ 00 & 04 & 08 & 0C \\ 03 & 07 & 0A & 0F \\ 02 & 06 & 0B & 0E \end{bmatrix}$ **(after FirstRoundKey)**

New State Matrix: $\begin{bmatrix} 62 & 77 & 6E & 6E \\ CA & 7E & C1 & 71 \\ BC & F6 & 89 & 17 \\ 02 & C1 & 18 & B5 \end{bmatrix}$ **(after SubBytes)**

New State Matrix: $\begin{bmatrix} 62 & 77 & 6E & 6E \\ 7E & C1 & 71 & CA \\ 89 & 17 & BC & F6 \\ B5 & 02 & C1 & 18 \end{bmatrix}$ **(after ShiftRows)**

Mix Column: $\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} * \begin{bmatrix} 62 & 77 & 6E & 6E \\ 7E & C1 & 71 & CA \\ 89 & 17 & BC & F6 \\ B5 & 02 & C1 & 18 \end{bmatrix} = \begin{bmatrix} 7A & A3 & 32 & 77 \\ AB & D5 & 82 & F8 \\ D1 & 9E & 24 & 7B \\ 20 & 4B & E6 & BE \end{bmatrix}$

- 2*62 (62 = 0110 0010)
  $x*(x^6+x^5+x)=x^7+x^6+x^2$ (=11000100)=C4
- 3*7E (7E = 0111 1110)
  $(x+1)*(x^6+x^5+x^4+x^3+x^2+x) = x^7+x$ (=10000010)=82
- 1*89 (89 = 1000 1001)
- 1*B5 (B5 = 1011 0101)
  C4⊕82⊕89⊕B5=**7A**

- 1*62 (62 = 0110 0010)
- 2*7E (7E = 0111 1110)
  $x*(x^6+x^5+x^4+x^3+x^2+x) = x^7+x^6+x^5+x^4+x^3+x^2$ (=11111100)=FC
- 3*89 (89 = 1000 1001)
  $(x+1)*(x^7+x^3+1) = x^7$ (=10000000)=80
- 1*B5 (B5 = 1011 0101)
  62⊕FC⊕80⊕B5=**AB**

- 1*62 (62 = 0110 0010)
- 1*7E (7E = 0111 1110)
- 2*89 (89 = 1000 1001)
  $x*(x^7+x^3+1) = x^3+1$ (=00001001)=9
- 3*B5 (B5 = 1011 0101)
  $(x+1)*(x^7+x^5+x^4+x^2+1) = x^7+x^6+x^2$ (=11000100)=C4
  62⊕7E⊕9⊕C4=**D1**

- 3*62 (62 = 0110 0010)
  $(x+1)*(x^6+x^5+x) = x^7+x^5+x^2+x$ (=10100110)=A6
- 1*7E (7E = 0111 1110)
- 1*89 (89 = 1000 1001)
- 2*B5 (B5 = 1011 0101)
  $x*(x^7+x^5+x^4+x^2+1) = x^6+x^5+x^4+1$ (=01110001)=71
  A6⊕7E⊕89⊕71=**20**

  Η παραπάνω διαδικασία έγινε τα 4 στοιχεία της 1^{ης} στήλης, και για τα υπόλοιπα ακολουθήθηκε η ίδια ακριβώς.