Date: Monday, September 24, 2002
Prof.: Dr Jean-Yves Chouinard

Design of Secure Computer Systems CSI4138/CEG4394

Notes on the Advanced Encryption Standard (AES)

1 Advanced Encryption Standard (AES)

1.1 AES History

In 1997, the National Institute of Standard and Technology (NIST) of United States initiated the development of an Advanced Encryption Standard (AES) to replace the Data Encryption Standard (DES). The objective was to develop with the industry and cryptographic community an encryption algorithm sufficiently powerful to protect government, as well as private sector, information for several years. As for DES, the algorithm should be royalty-free, publicly disclosed.

The AES algorithm was designed as a symmetric block cipher using a minimum of 128-bit input blocks and supporting 3 key sizes, that is: 128-bit, 192-bit and 256-bit keys.

In August 1998, NIST announced that 15 AES proposals were received for evaluation and comments. After an analysis of the proposed algorithms, NIST announced in April 1999 that five algorithms were retained as *finalist algorithms*. These were:

1. MARS
2. RC6
3. Rijndael
4. Serpent
5. Twofish

These algorithms were further analyzed in terms of their relative cryptographic strength and ease of implementation. In October 2000, NIST announced that the Rijndael algorithm was selected for the new AES standard. The algorithm is presently under further review, that is validation testing, and it is expected that the AES algorithm be completed for this summer. In February 2001, the NIST delivered a draft Federal Information Processing Standards (FIPS) for the specification of the Advanced Encryption Standard. On November 26, 2001, NIST announced the final specification of the Advanced Encryption Standard (FIPS PUB 197) [NIS01].

1.2 Rijndael Block Cipher Algorithm

Mathematical Background

In the AES algorithm, the operations, such as the addition and the multiplication, are performed on bytes over a *finite field*, the Galois Field GF(2^8).

Addition

The addition between two elements, or bytes, from the finite field is achieved by the addition modulo 2 of the corresponding bits in the representation of the bytes. The addition of the bytes $A = (a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8)$ and $B = (b_1, b_2, b_3, b_4, b_5, b_6, b_7, b_8)$ gives $C = A + B$ with $C = (c_1, c_2, c_3, c_4, c_5, c_6, c_7, c_8)$ where $c_i = a_i \oplus b_i$ for $1 < i < 8$. The finite field elements can also be represented in polynomial form. For instance, the sum of $A = 73_{16}$ and $B = 4E_{16}$ (in hexadecimal notation) is obtained as:

$$\begin{aligned} 73_{16} + 4E_{16} &= 3D_{16} \qquad \text{(hexadecimal notation)} \\ 01110011_2 \oplus 01001110_2 &= 00111101_2 \qquad \text{(binary notation)} \\ (x^6 + x^5 + x^4 + x + 1) + (x^6 + x^3 + x^2 + x) &= (x^5 + x^4 + x^3 + x^2 + 1) \end{aligned}$$

in polynomial notation.

Multiplication

As for the multiplication operation, it is also done over the Galois Field GF(2^8) and is obtained by the multiplication of the two elements polynomials and then reduced modulo an *irreductible polynomial* $m(x)$, which is equivalent to a prime number in the standard numbering system. As a prime number, the irreductible polynomial as only two divisors: 1 and itself, $m(x)$. For AES, this irreductible polynomial is $m(x) = (x^8 + x^4 + x^3 + x + 1)$.

Let, for example, $A = C3_{16}$ and $B = 85_{16}$, that is, $a(x) = (x^7+x^6+x+1)$ and $b(x) = (x^7+x^2+1)$. Then $C = A \cdot B$ is given by:

$$\begin{aligned} c(x) &= [a(x) \cdot b(x)] \bmod (x^8 + x^4 + x^3 + x + 1) \\ c(x) &= [(x^7 + x^6 + x + 1) \cdot (x^7 + x^2 + 1)] \bmod (x^8 + x^4 + x^3 + x + 1) \\ c(x) &= [(x^{14} + x^{13} + x^8 + x^7) + (x^9 + x^8 + x^3 + x^2) + (x^7 + x^6 + x + 1)] \bmod (x^8 + x^4 + x^3 + x + 1) \\ c(x) &= [(x^{14} + x^{13} + x^9 + x^6 + x^3 + x^2 + x + 1)] \bmod (x^8 + x^4 + x^3 + x + 1) \\ c(x) &= [(x^6 + x^5 + x^2 + x + 1) \cdot (x^8 + x^4 + x^3 + x + 1) + (x^7 + x^5 + x^3 + x^2 + x)] \\ &\quad \bmod (x^8 + x^4 + x^3 + x + 1) \\ c(x) &= (x^7 + x^5 + x^3 + x^2 + x) \end{aligned}$$

and then $c(x) = (x^7 + x^5 + x^3 + x^2 + x)$ or $C = 10101110_2$ in binary notation or, in hexadecimal notation: $C = AE_{16}$.

Construction of an (extended) Galois Fields

Let p be a prime number. Galois Field GF(p) is given by the element $\{0\}$ and the $(p-1)$ successive powers:

$$1, \alpha, \alpha^1, \alpha^2, \ldots, \alpha^{(p-1)}$$

Many computer based algorithms operate on *extensions* of the Galois Field GF(2) which consists of the two binary elements $\{0, 1\}$. Reed-Solomon error correction codes and the AES encryption algorithm, which are basically Byte-oriented algorithms, use extended Galois Field such as GF(p^m) = GF(2^8) = GF(256) that contains 256 distinct elements.

To generate such an extended Galois Field, a *primitive polynomial* $p(x)$ over GF(q) is needed. An *irreductible polynomial* $p(x)$ is a polynomial which cannot be factored into lower degree polynomials in over GF(q). An irreductible polynomial $p(x)$ of degree m is a primitive polynomial if the smallest positive integer n for which $p(x)$ divides $x^n - 1$ is $n = p^m - 1$.

To form the Galois Field, one has to determine a root α of the primitive polynomial $p(x)$, that is $p(\alpha) = 0$. For instance, the primitive polynomial $p(x) = x^4 + x + 1$ can be used to form the extended Galois Field GF(2^4) = GF(16), that is for $p = 2$ and $m = 4$. Then the root α of $p(x)$ is:

$$\begin{aligned} p(\alpha) &= 0 \\ \alpha^4 + \alpha + 1 &= 0 \end{aligned}$$

and therefore: $\alpha^4 = \alpha + 1$. Table 1 illustrates how to generate the extended Galois Field GF(2^4) from the primitive polynomial $p(x)$.

Table 4 gives an extended Galois Field GF(2^8) that can be used for Reed-Solomon error control coding and for AES byte operations. The primitive polynomial $p(x) = x^8 + x^4 + x^3 + x^2 + 1$ is used and the extended Galois Field GF(2^8) is obtained with the polynomial root: $\alpha^8 = \alpha^4 + \alpha^3 + \alpha^2 + 1$.

Table 1: Galois Field $GF(2^4) = GF(16)$.

element of $GF(16)$	polynomial form	binary form	decimal form
0	0	0 0 0 0	0
1	1	0 0 0 1	1
α	α	0 0 1 0	2
α^2	α^2	0 1 0 0	4
α^3	α^3	1 0 0 0	8
α^4	$\alpha +1$	0 0 1 1	3
α^5	$\alpha^2 +\alpha$	0 1 1 0	6
α^6	$\alpha^3 +\alpha^2$	1 1 0 0	12
α^7	$\alpha^3 +\alpha +1$	1 0 1 1	11
α^8	$\alpha^2 +1$	0 1 0 1	5
α^9	$\alpha^3 +\alpha$	1 0 1 0	10
α^{10}	$\alpha^2 +\alpha +1$	0 1 1 1	7
α^{11}	$\alpha^3 +\alpha^2 +\alpha$	1 1 1 0	14
α^{12}	$\alpha^3 +\alpha^2 +\alpha +1$	1 1 1 1	15
α^{13}	$\alpha^3 +\alpha^2 +1$	1 1 0 1	13
α^{14}	$\alpha^3 +1$	1 0 0 1	9

1.3 Advanced Encryption Standard Algorithm

The Advanced Encryption Standard Algorithm encrypts a 128-bit plaintext block M into a 128-bit ciphertext block C using a *cipher key* K of either 128 bits, 192 bits or 256 bits. The different key lengths employed for AES are refered to: AES-128, AES-192, and AES-256. The algorithm operates on *bytes* and the block size for the input, output and key are represented by 32-bit words, that is 4 bytes.

The AES algorithm performs a number N_r of cryptographic rounds depending on the actual key length used as indicated in Table 2 for AES-128, AES-192 and AES-256.

Table 2: Number of cryptographic rounds N_r for AES encryption.

AES algorithm	Input/output length N_b	Key length N_k	Number of rounds N_r
AES-128	4 words	4 words	10 rounds
AES-192	4 words	6 words	12 rounds
AES-256	4 words	8 words	14 rounds

Each round consists of four *byte-oriented cryptographic transformations*:

1. Byte Substitution
2. Shifting rows of the *State Array*
3. Mixing data within a column of the State Array
4. Round Key addition to the State Array

```
 Cipher(byte in[4 * Nb],
byte out[4 * Nb], word w[Nb * (Nr + 1)])

begin byte    state[4,Nb] state = in AddRoundKey(state, w)

for round = 1 step 1 to Nr - 1 SubBytes(state) ShiftRows(state)
MixColumns(state) AddRoundKey(state, w + round * Nb) end for

SubBytes(state) ShiftRows(state) AddRoundKey(state, w + Nr * Nb)
out = state end
```

(Source: AES draft specification: http://csrc.nist.gov/encryption/aes/.)

Byte Substitution: $SubBytes()$ **transformation**

The first AES transformation is a non linear byte substitution transformation called $SubBytes()$ transformation. It operates independently on each byte. It first computes the multiplicative inverse in the finite Galois Field GF(2^8). It then applies an affine transformation on the multiplicative inverse:

$$\begin{bmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

where b_i represents the i^{th} bit of byte b.

Shifting rows of the State Array: $ShiftRows()$ **transformation**

The next transformation of the AES cipher consits in shifting the rows of the State array. The amount of shifting $shift(r, N_b)$ depends on the row number r. The input (plaintext) and output (ciphertext) blocks are 128 bit-blocks or consist of $N_b = 4$ 32-bit words.

The $ShiftRows()$ transformation can be expressed as:

$$s'_{r,c} = s_{r,(c+shift(r,N_b)) \bmod N_b}$$

where $0 \leq c < N_b$. For the first row, there is no row shifting, that is: $shift(0, N_b = 4) = 0$. For the remaining rows the amount of shifting depend on the row number:

$$\begin{aligned} shift(0,4) &= 0 \\ shift(1,4) &= 1 \\ shift(2,4) &= 2 \\ shift(3,4) &= 3 \end{aligned}$$

Mixing data within a column of the State Array: $MixColumns()$ **transformation**

The $MixColumns()$ transformation is used to Mix the data within a single column of the State matrix. The columns are represented as polynomials over the Galois Field GF(2^8). The output of the $MixColumns()$ transformation $s'(x)$ is given by the multiplication of the input column $s(x)$ with the polynomial $a(x)$ and reduced modulo $(x^4 + 1)$:

$$s'(x) = a(x) \otimes s(x) \bmod (x^4 + 1)$$

where $a(x) = 03_{16}x^3 + 01_{16}x^2 + 01_{16}x + 02_{16}$. In matrix form, this column mixing transformation can be represented as:

$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 02_{16} & 03_{16} & 01_{16} & 01_{16} \\ 01_{16} & 02_{16} & 03_{16} & 01_{16} \\ 01_{16} & 01_{16} & 02_{16} & 03_{16} \\ 03_{16} & 01_{16} & 01_{16} & 02_{16} \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix} \qquad \text{where } 0 \leq c < N_b.$$

Round Key addition to the State Array: $AddRoundKey()$ **transformation**

In the $AddRoundKey()$ transformation, the key bits derived from the original Cipher Key by the Key Expansion transformation are added bitwise to the State array. An initial Round Key w_0, i.e. for $round = 0$, is added prior the first cryptographic round. Then at each round, i.e. for $1 \leq round \leq N_r$, a different 32-bit Round Key w_i is added:

$$\left[s'_{0,c}, s'_{1,c}, s'_{2,c}, s'_{3,c}\right] = [s_{0,c}, s_{1,c}, s_{2,c}, s_{3,c}] \oplus \left[w_{(round \times N_b)+c}\right] \qquad \text{where } 0 \leq c < N_b.$$

AES Key Expansion

The AES algorithm generates from the *Cipher Key* (128-bit, 192-bit or 256-bit long) an initial set of N_b 32-bit words and a N_b 32-bit for each of the N_r rounds, resulting in a total of $N_b(N_r + 1)$ 32-bit words, $\{w_i\}$, for $0 \leq i < N_b(N_r+1)$. The pseudocode for the AES key expansion algorithm is given in the FIPS draft (Web site: http://csrc.nist.gov/encryption/aes/) and reproduced hereafter. Note that this is a draft document and that the final AES specification should be adopted in the summer of 2001.

The function $SubWord()$ applies the substitution transformation of the S-box on a 4-byte input word to produce a 4-byte output word.

Function $RotWord()$ performs a cyclic byte permutation on a 4-byte (32-bit) word w_i.

$$RotWord(a_0, a_1, a_2, a_3) \quad = \quad (a_1, a_2, a_3, a_0)$$

AES Key Management

As is the case for DES, the AES is a symmetric block cipher cryptosystem that requires the secure distribution of the secret key between the sender and recipient. Table 3 indicates the length of the public key for the three AES key lengths. This entries in Table 3 show the advantage of using a key exchange scheme based on Elliptic Curve Cryptography (ECC) instead of the RSA algorithm for the same level of security.

Table 3: Required RSA and Elliptic Curve Cryptography (ECC) key lengths for encryption of AES secret keys with equivalent security.

AES algorithm	AES key length	RSA key length	ECC key length
AES-128	128 bits	3,072 bits	283 bits
AES-192	192 bits	7,680 bits	409 bits
AES-256	256 bits	15,360 bits	571 bits

```
 KeyExpansion(byte key[4 *
Nk], word w[Nb * (Nr + 1)], Nk)

begin

    i=0
    while (i < Nk)
        w[i] = word[key[4*i],key[4*i+1],key[4*i+2],key[4*i+3]]
        i = i + 1
    end while

    i = Nk
    while (i < Nb * (Nr + 1))
        word temp = w[i - 1]
        if (i mod Nk = 0)
            temp = SubWord(RotWord(temp)) xor Rcon[i / Nk]
        else if (Nk = 8 and i mod Nk = 4)
            temp = SubWord(temp)
        end if
    w[i] = w[i - Nk] xor temp
    i = i + 1
    end while
end
```

(Source: AES draft specification: http://csrc.nist.gov/encryption/aes/.)

Table 4: Galois Field $GF(2^8) = GF(256)$.

element of $GF(256)$	polynomial form	binary form	decimal form
0	0	0 0 0 0 0 0 0 0	0
1	1	0 0 0 0 0 0 0 1	1
α	α	0 0 0 0 0 0 1 0	2
α^2	α^2	0 0 0 0 0 1 0 0	4
α^3	α^3	0 0 0 0 1 0 0 0	8
α^4	α^4	0 0 0 1 0 0 0 0	16
α^5	α^5	0 0 1 0 0 0 0 0	32
α^6	α^6	0 1 0 0 0 0 0 0	64
α^7	α^7	1 0 0 0 0 0 0 0	128
α^8	$\alpha^4 + \alpha^3 + \alpha^2 + 1$	0 0 0 1 1 1 0 1	29
α^9	$\alpha^5 + \alpha^4 + \alpha^3 + \alpha$	0 0 1 1 1 0 1 0	58
α^{10}	$\alpha^6 + \alpha^5 + \alpha^4 + \alpha^2$	0 1 1 1 0 1 0 0	116
α^{11}	$\alpha^7 + \alpha^6 + \alpha^5 + \alpha^3$	1 1 1 0 1 0 0 0	232
α^{12}	$\alpha^7 + \alpha^6 + \alpha^3 + \alpha^2 + 1$	1 1 0 0 1 1 0 1	205
α^{13}	$\alpha^7 + \alpha^2 + \alpha + 1$	1 0 0 0 0 1 1 1	135
α^{14}	$\alpha^4 + \alpha + 1$	0 0 0 1 0 0 1 1	19
α^{15}	$\alpha^5 + \alpha^2 + \alpha$	0 0 1 0 0 1 1 0	38
α^{16}	$\alpha^6 + \alpha^3 + \alpha^2$	0 1 0 0 1 1 0 0	76
α^{17}	$\alpha^7 + \alpha^4 + \alpha^3$	1 0 0 1 1 0 0 0	152
α^{18}	$\alpha^5 + \alpha^3 + \alpha^2 + 1$	0 0 1 0 1 1 0 1	45
α^{19}	$\alpha^6 + \alpha^4 + \alpha^3 + \alpha$	0 1 0 1 1 0 1 0	90
α^{20}	$\alpha^7 + \alpha^5 + \alpha^4 + \alpha^2$	1 0 1 1 0 1 0 0	180
α^{21}	$\alpha^6 + \alpha^5 + \alpha^4 + \alpha^2 + 1$	0 1 1 1 0 1 0 1	117
α^{22}	$\alpha^7 + \alpha^6 + \alpha^5 + \alpha^3 + \alpha$	1 1 1 0 1 0 1 0	234
α^{23}	$\alpha^7 + \alpha^6 + \alpha^3 + 1$	1 1 0 0 1 0 0 1	201
α^{24}	$\alpha^7 + \alpha^3 + \alpha^2 + \alpha + 1$	1 0 0 0 1 1 1 1	143
α^{25}	$\alpha + 1$	0 0 0 0 0 0 1 1	3
α^{26}	$\alpha^2 + \alpha$	0 0 0 0 0 1 1 0	6
α^{27}	$\alpha^3 + \alpha^2$	0 0 0 0 1 1 0 0	12
α^{28}	$\alpha^4 + \alpha^3$	0 0 0 1 1 0 0 0	24
α^{29}	$\alpha^5 + \alpha^4$	0 0 1 1 0 0 0 0	48
α^{30}	$\alpha^6 + \alpha^5$	0 1 1 0 0 0 0 0	96
α^{31}	$\alpha^7 + \alpha^6$	1 1 0 0 0 0 0 0	192

element of $GF(256)$	polynomial form	binary form	decimal form
α^{32}	$\alpha^7 + \alpha^4 + \alpha^3 + \alpha^2 + 1$	1 0 0 1 1 1 0 1	157
α^{33}	$\alpha^5 + \alpha^2 + \alpha + 1$	0 0 1 0 0 1 1 1	39
α^{34}	$\alpha^6 + \alpha^3 + \alpha^2 + \alpha$	0 1 0 0 1 1 1 0	78
α^{35}	$\alpha^7 + \alpha^4 + \alpha^3 + \alpha^2$	1 0 0 1 1 1 0 0	156
α^{36}	$\alpha^5 + \alpha^2 + 1$	0 0 1 0 0 1 0 1	37
α^{37}	$\alpha^6 + \alpha^3 + \alpha$	0 1 0 0 1 0 1 0	74
α^{38}	$\alpha^7 + \alpha^4 + \alpha^2$	1 0 0 1 0 1 0 0	148
α^{39}	$\alpha^5 + \alpha^4 + \alpha^2 + 1$	0 0 1 1 0 1 0 1	53
α^{40}	$\alpha^6 + \alpha^5 + \alpha^3 + \alpha$	0 1 1 0 1 0 1 0	106
α^{41}	$\alpha^7 + \alpha^6 + \alpha^4 + \alpha^2$	1 1 0 1 0 1 0 0	212
α^{42}	$\alpha^7 + \alpha^5 + \alpha^4 + \alpha^2 + 1$	1 0 1 1 0 1 0 1	181
α^{43}	$\alpha^6 + \alpha^5 + \alpha^4 + \alpha^2 + \alpha + 1$	0 1 1 1 0 1 1 1	119
α^{44}	$\alpha^7 + \alpha^6 + \alpha^5 + \alpha^3 + \alpha^2 + \alpha$	1 1 1 0 1 1 1 0	238
α^{45}	$\alpha^7 + \alpha^6 + 1$	1 1 0 0 0 0 0 1	193
α^{46}	$\alpha^7 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1$	1 0 0 1 1 1 1 1	159
α^{47}	$\alpha^5 + \alpha + 1$	0 0 1 0 0 0 1 1	35
α^{48}	$\alpha^6 + \alpha^2 + \alpha$	0 1 0 0 0 1 1 0	70
α^{49}	$\alpha^7 + \alpha^3 + \alpha^2$	1 0 0 0 1 1 0 0	140
α^{50}	$\alpha^2 + 1$	0 0 0 0 0 1 0 1	5
α^{51}	$\alpha^3 + \alpha$	0 0 0 0 1 0 1 0	10
α^{52}	$\alpha^4 + \alpha^2$	0 0 0 1 0 1 0 0	20
α^{53}	$\alpha^5 + \alpha^3$	0 0 1 0 1 0 0 0	40
α^{54}	$\alpha^6 + \alpha^4$	0 1 0 1 0 0 0 0	80
α^{55}	$\alpha^7 + \alpha^5$	1 0 1 0 0 0 0 0	160
α^{56}	$\alpha^6 + \alpha^4 + \alpha^3 + \alpha^2 + 1$	0 1 0 1 1 1 0 1	93
α^{57}	$\alpha^7 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha$	1 0 1 1 1 0 1 0	186
α^{58}	$\alpha^6 + \alpha^5 + \alpha^3 + 1$	0 1 1 0 1 0 0 1	105
α^{59}	$\alpha^7 + \alpha^6 + \alpha^4 + \alpha$	1 1 0 1 0 0 1 0	210
α^{60}	$\alpha^7 + \alpha^5 + \alpha^4 + \alpha^3 + 1$	1 0 1 1 1 0 0 1	185
α^{61}	$\alpha^6 + \alpha^5 + \alpha^3 + \alpha^2 + \alpha + 1$	0 1 1 0 1 1 1 1	111
α^{62}	$\alpha^7 + \alpha^6 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha$	1 1 0 1 1 1 1 0	222
α^{63}	$\alpha^7 + \alpha^5 + 1$	1 0 1 0 0 0 0 1	161

element of $GF(256)$	polynomial form	binary form	decimal form
α^{64}	$\alpha^6 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1$	0 1 0 1 1 1 1 1	95
α^{65}	$\alpha^7 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha$	1 0 1 1 1 1 1 0	190
α^{66}	$\alpha^6 + \alpha^5 + 1$	0 1 1 0 0 0 0 1	97
α^{67}	$\alpha^7 + \alpha^6 + \alpha$	1 1 0 0 0 0 1 0	194
α^{68}	$\alpha^7 + \alpha^4 + \alpha^3 + 1$	1 0 0 1 1 0 0 1	153
α^{69}	$\alpha^5 + \alpha^3 + \alpha^2 + \alpha + 1$	0 0 1 0 1 1 1 1	47
α^{70}	$\alpha^6 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha$	0 1 0 1 1 1 1 0	94
α^{71}	$\alpha^7 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2$	1 0 1 1 1 1 0 0	188
α^{72}	$\alpha^6 + \alpha^5 + \alpha^2 + 1$	0 1 1 0 0 1 0 1	101
α^{73}	$\alpha^7 + \alpha^6 + \alpha^3 + \alpha$	1 1 0 0 1 0 1 0	202
α^{74}	$\alpha^7 + \alpha^3 + 1$	1 0 0 0 1 0 0 1	137
α^{75}	$\alpha^3 + \alpha^2 + \alpha + 1$	0 0 0 0 1 1 1 1	15
α^{76}	$\alpha^4 + \alpha^3 + \alpha^2 + \alpha$	0 0 0 1 1 1 1 0	30
α^{77}	$\alpha^5 + \alpha^4 + \alpha^3 + \alpha^2$	0 0 1 1 1 1 0 0	60
α^{78}	$\alpha^6 + \alpha^5 + \alpha^4 + \alpha^3$	0 1 1 1 1 0 0 0	120
α^{79}	$\alpha^7 + \alpha^6 + \alpha^5 + \alpha^4$	1 1 1 1 0 0 0 0	240
α^{80}	$\alpha^7 + \alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + 1$	1 1 1 1 1 1 0 1	253
α^{81}	$\alpha^7 + \alpha^6 + \alpha^5 + \alpha^2 + \alpha + 1$	1 1 1 0 0 1 1 1	231
α^{82}	$\alpha^7 + \alpha^6 + \alpha^4 + \alpha + 1$	1 1 0 1 0 0 1 1	211
α^{83}	$\alpha^7 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha + 1$	1 0 1 1 1 0 1 1	187
α^{84}	$\alpha^6 + \alpha^5 + \alpha^3 + \alpha + 1$	0 1 1 0 1 0 1 1	107
α^{85}	$\alpha^7 + \alpha^6 + \alpha^4 + \alpha^2 + \alpha$	1 1 0 1 0 1 1 0	214
α^{86}	$\alpha^7 + \alpha^5 + \alpha^4 + 1$	1 0 1 1 0 0 0 1	177
α^{87}	$\alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1$	0 1 1 1 1 1 1 1	127
α^{88}	$\alpha^7 + \alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha$	1 1 1 1 1 1 1 0	254
α^{89}	$\alpha^7 + \alpha^6 + \alpha^5 + 1$	1 1 1 0 0 0 0 1	225
α^{90}	$\alpha^7 + \alpha^6 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1$	1 1 0 1 1 1 1 1	223
α^{91}	$\alpha^7 + \alpha^5 + \alpha + 1$	1 0 1 0 0 0 1 1	163
α^{92}	$\alpha^6 + \alpha^4 + \alpha^3 + \alpha + 1$	0 1 0 1 1 0 1 1	91
α^{93}	$\alpha^7 + \alpha^5 + \alpha^4 + \alpha^2 + \alpha$	1 0 1 1 0 1 1 0	182
α^{94}	$\alpha^6 + \alpha^5 + \alpha^4 + 1$	0 1 1 1 0 0 0 1	113
α^{95}	$\alpha^7 + \alpha^6 + \alpha^5 + \alpha$	1 1 1 0 0 0 1 0	226

element of $GF(256)$	polynomial form	binary form	decimal form
α^{96}	$\alpha^7 + \alpha^6 + \alpha^4 + \alpha^3 + 1$	1 1 0 1 1 0 0 1	217
α^{97}	$\alpha^7 + \alpha^5 + \alpha^3 + \alpha^2 + \alpha + 1$	1 0 1 0 1 1 1 1	175
α^{98}	$\alpha^6 + \alpha + 1$	0 1 0 0 0 0 1 1	67
α^{99}	$\alpha^7 + \alpha^2 + \alpha$	1 0 0 0 0 1 1 0	134
α^{100}	$\alpha^4 + 1$	0 0 0 1 0 0 0 1	17
α^{101}	$\alpha^5 + \alpha$	0 0 1 0 0 0 1 0	34
α^{102}	$\alpha^6 + \alpha^2$	0 1 0 0 0 1 0 0	68
α^{103}	$\alpha^7 + \alpha^3$	1 0 0 0 1 0 0 0	136
α^{104}	$\alpha^3 + \alpha^2 + 1$	0 0 0 0 1 1 0 1	13
α^{105}	$\alpha^4 + \alpha^3 + \alpha$	0 0 0 1 1 0 1 0	26
α^{106}	$\alpha^5 + \alpha^4 + \alpha^2$	0 0 1 1 0 1 0 0	52
α^{107}	$\alpha^6 + \alpha^5 + \alpha^3$	0 1 1 0 1 0 0 0	104
α^{108}	$\alpha^7 + \alpha^6 + \alpha^4$	1 1 0 1 0 0 0 0	208
α^{109}	$\alpha^7 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + 1$	1 0 1 1 1 1 0 1	189
α^{110}	$\alpha^6 + \alpha^5 + \alpha^2 + \alpha + 1$	0 1 1 0 0 1 1 1	103
α^{111}	$\alpha^7 + \alpha^6 + \alpha^3 + \alpha^2 + \alpha$	1 1 0 0 1 1 1 0	206
α^{112}	$\alpha^7 + 1$	1 0 0 0 0 0 0 1	129
α^{113}	$\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1$	0 0 0 1 1 1 1 1	31
α^{114}	$\alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha$	0 0 1 1 1 1 1 0	62
α^{115}	$\alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2$	0 1 1 1 1 1 0 0	124
α^{116}	$\alpha^7 + \alpha^6 + \alpha^5 + \alpha^4 + \alpha^3$	1 1 1 1 1 0 0 0	248
α^{117}	$\alpha^7 + \alpha^6 + \alpha^5 + \alpha^3 + \alpha^2 + 1$	1 1 1 0 1 1 0 1	237
α^{118}	$\alpha^7 + \alpha^6 + \alpha^2 + \alpha + 1$	1 1 0 0 0 1 1 1	199
α^{119}	$\alpha^7 + \alpha^4 + \alpha + 1$	1 0 0 1 0 0 1 1	147
α^{120}	$\alpha^5 + \alpha^4 + \alpha^3 + \alpha + 1$	0 0 1 1 1 0 1 1	59
α^{121}	$\alpha^6 + \alpha^5 + \alpha^4 + \alpha^2 + \alpha$	0 1 1 1 0 1 1 0	118
α^{122}	$\alpha^7 + \alpha^6 + \alpha^5 + \alpha^3 + \alpha^2$	1 1 1 0 1 1 0 0	236
α^{123}	$\alpha^7 + \alpha^6 + \alpha^2 + 1$	1 1 0 0 0 1 0 1	197
α^{124}	$\alpha^7 + \alpha^4 + \alpha^2 + \alpha + 1$	1 0 0 1 0 1 1 1	151
α^{125}	$\alpha^5 + \alpha^4 + \alpha + 1$	0 0 1 1 0 0 1 1	51
α^{126}	$\alpha^6 + \alpha^5 + \alpha^2 + \alpha$	0 1 1 0 0 1 1 0	102
α^{127}	$\alpha^7 + \alpha^6 + \alpha^3 + \alpha^2$	1 1 0 0 1 1 0 0	204

element of $GF(256)$	polynomial form	binary form	decimal form
α^{128}	$\alpha^7 \quad +\alpha^2 \quad +1$	1 0 0 0 0 1 0 1	133
α^{129}	$\alpha^4 \quad +\alpha^2 +\alpha +1$	0 0 0 1 0 1 1 1	23
α^{130}	$\alpha^5 \quad +\alpha^3 +\alpha^2 +\alpha$	0 0 1 0 1 1 1 0	46
α^{131}	$\alpha^6 \quad +\alpha^4 +\alpha^3 +\alpha^2$	0 1 0 1 1 1 0 0	92
α^{132}	$\alpha^7 \quad +\alpha^5 +\alpha^4 +\alpha^3$	1 0 1 1 1 0 0 0	184
α^{133}	$\alpha^6 +\alpha^5 \quad +\alpha^3 +\alpha^2 \quad +1$	0 1 1 0 1 1 0 1	109
α^{134}	$\alpha^7 +\alpha^6 \quad +\alpha^4 +\alpha^3 \quad +\alpha$	1 1 0 1 1 0 1 0	218
α^{135}	$\alpha^7 \quad +\alpha^5 \quad +\alpha^3 \quad +1$	1 0 1 0 1 0 0 1	169
α^{136}	$\alpha^6 \quad +\alpha^3 +\alpha^2 +\alpha +1$	0 1 0 0 1 1 1 1	79
α^{137}	$\alpha^7 \quad +\alpha^4 +\alpha^3 +\alpha^2 +\alpha$	1 0 0 1 1 1 1 0	158
α^{138}	$\alpha^5 \quad +1$	0 0 1 0 0 0 0 1	33
α^{139}	$\alpha^6 \quad +\alpha$	0 1 0 0 0 0 1 0	66
α^{140}	$\alpha^7 \quad +\alpha^2$	1 0 0 0 0 1 0 0	132
α^{141}	$\alpha^4 \quad +\alpha^2 \quad +1$	0 0 0 1 0 1 0 1	21
α^{142}	$\alpha^5 \quad +\alpha^3 \quad +\alpha$	0 0 1 0 1 0 1 0	42
α^{143}	$\alpha^6 \quad +\alpha^4 \quad +\alpha^2$	0 1 0 1 0 1 0 0	84
α^{144}	$\alpha^7 \quad +\alpha^5 \quad +\alpha^3$	1 0 1 0 1 0 0 0	168
α^{145}	$\alpha^6 \quad +\alpha^3 +\alpha^2 \quad +1$	0 1 0 0 1 1 0 1	77
α^{146}	$\alpha^7 \quad +\alpha^4 +\alpha^3 \quad +\alpha$	1 0 0 1 1 0 1 0	154
α^{147}	$\alpha^5 \quad +\alpha^3 \quad +1$	0 0 1 0 1 0 0 1	41
α^{148}	$\alpha^6 \quad +\alpha^4 \quad +\alpha$	0 1 0 1 0 0 1 0	82
α^{149}	$\alpha^7 \quad +\alpha^5 \quad +\alpha^2$	1 0 1 0 0 1 0 0	164
α^{150}	$\alpha^6 \quad +\alpha^4 \quad +\alpha^2 \quad +1$	0 1 0 1 0 1 0 1	85
α^{151}	$\alpha^7 \quad +\alpha^5 \quad +\alpha^3 \quad +\alpha$	1 0 1 0 1 0 1 0	170
α^{152}	$\alpha^6 \quad +\alpha^3 \quad +1$	0 1 0 0 1 0 0 1	73
α^{153}	$\alpha^7 \quad +\alpha^4 \quad +\alpha$	1 0 0 1 0 0 1 0	146
α^{154}	$\alpha^5 +\alpha^4 +\alpha^3 \quad +1$	0 0 1 1 1 0 0 1	57
α^{155}	$\alpha^6 +\alpha^5 +\alpha^4 \quad +\alpha$	0 1 1 1 0 0 1 0	114
α^{156}	$\alpha^7 +\alpha^6 +\alpha^5 \quad +\alpha^2$	1 1 1 0 0 1 0 0	228
α^{157}	$\alpha^7 +\alpha^6 \quad +\alpha^4 \quad +\alpha^2 \quad +1$	1 1 0 1 0 1 0 1	213
α^{158}	$\alpha^7 \quad +\alpha^5 +\alpha^4 \quad +\alpha^2 +\alpha +1$	1 0 1 1 0 1 1 1	183
α^{159}	$\alpha^6 +\alpha^5 +\alpha^4 \quad +\alpha +1$	0 1 1 1 0 0 1 1	115

element of $GF(256)$	polynomial form	binary form	decimal form
α^{160}	$\alpha^7 + \alpha^6 + \alpha^5 + \alpha^2 + \alpha$	1 1 1 0 0 1 1 0	230
α^{161}	$\alpha^7 + \alpha^6 + \alpha^4 + 1$	1 1 0 1 0 0 0 1	209
α^{162}	$\alpha^7 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1$	1 0 1 1 1 1 1 1	191
α^{163}	$\alpha^6 + \alpha^5 + \alpha + 1$	0 1 1 0 0 0 1 1	99
α^{164}	$\alpha^7 + \alpha^6 + \alpha^2 + \alpha$	1 1 0 0 0 1 1 0	198
α^{165}	$\alpha^7 + \alpha^4 + 1$	1 0 0 1 0 0 0 1	145
α^{166}	$\alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1$	0 0 1 1 1 1 1 1	63
α^{167}	$\alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha$	0 1 1 1 1 1 1 0	126
α^{168}	$\alpha^7 + \alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2$	1 1 1 1 1 1 0 0	252
α^{169}	$\alpha^7 + \alpha^6 + \alpha^5 + \alpha^2 + 1$	1 1 1 0 0 1 0 1	229
α^{170}	$\alpha^7 + \alpha^6 + \alpha^4 + \alpha^2 + \alpha + 1$	1 1 0 1 0 1 1 1	215
α^{171}	$\alpha^7 + \alpha^5 + \alpha^4 + \alpha + 1$	1 0 1 1 0 0 1 1	179
α^{172}	$\alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha + 1$	0 1 1 1 1 0 1 1	123
α^{173}	$\alpha^7 + \alpha^6 + \alpha^5 + \alpha^4 + \alpha^2 + \alpha$	1 1 1 1 0 1 1 0	246
α^{174}	$\alpha^7 + \alpha^6 + \alpha^5 + \alpha^4 + 1$	1 1 1 1 0 0 0 1	241
α^{175}	$\alpha^7 + \alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1$	1 1 1 1 1 1 1 1	255
α^{176}	$\alpha^7 + \alpha^6 + \alpha^5 + \alpha + 1$	1 1 1 0 0 0 1 1	227
α^{177}	$\alpha^7 + \alpha^6 + \alpha^4 + \alpha^3 + \alpha + 1$	1 1 0 1 1 0 1 1	219
α^{178}	$\alpha^7 + \alpha^5 + \alpha^3 + \alpha + 1$	1 0 1 0 1 0 1 1	171
α^{179}	$\alpha^6 + \alpha^3 + \alpha + 1$	0 1 0 0 1 0 1 1	75
α^{180}	$\alpha^7 + \alpha^4 + \alpha^2 + \alpha$	1 0 0 1 0 1 1 0	150
α^{181}	$\alpha^5 + \alpha^4 + 1$	0 0 1 1 0 0 0 1	49
α^{182}	$\alpha^6 + \alpha^5 + \alpha$	0 1 1 0 0 0 1 0	98
α^{183}	$\alpha^7 + \alpha^6 + \alpha^2$	1 1 0 0 0 1 0 0	196
α^{184}	$\alpha^7 + \alpha^4 + \alpha^2 + 1$	1 0 0 1 0 1 0 1	149
α^{185}	$\alpha^5 + \alpha^4 + \alpha^2 + \alpha + 1$	0 0 1 1 0 1 1 1	55
α^{186}	$\alpha^6 + \alpha^5 + \alpha^3 + \alpha^2 + \alpha$	0 1 1 0 1 1 1 0	110
α^{187}	$\alpha^7 + \alpha^6 + \alpha^4 + \alpha^3 + \alpha^2$	1 1 0 1 1 1 0 0	220
α^{188}	$\alpha^7 + \alpha^5 + \alpha^2 + 1$	1 0 1 0 0 1 0 1	165
α^{189}	$\alpha^6 + \alpha^4 + \alpha^2 + \alpha + 1$	0 1 0 1 0 1 1 1	87
α^{190}	$\alpha^7 + \alpha^5 + \alpha^3 + \alpha^2 + \alpha$	1 0 1 0 1 1 1 0	174
α^{191}	$\alpha^6 + 1$	0 1 0 0 0 0 0 1	65

element of $GF(256)$	polynomial form	binary form	decimal form
α^{192}	$\alpha^7 \quad +\alpha$	1 0 0 0 0 0 1 0	130
α^{193}	$\alpha^4 +\alpha^3 \quad +1$	0 0 0 1 1 0 0 1	25
α^{194}	$\alpha^5 +\alpha^4 \quad +\alpha$	0 0 1 1 0 0 1 0	50
α^{195}	$\alpha^6 +\alpha^5 \quad +\alpha^2$	0 1 1 0 0 1 0 0	100
α^{196}	$\alpha^7 +\alpha^6 \quad +\alpha^3$	1 1 0 0 1 0 0 0	200
α^{197}	$\alpha^7 \quad +\alpha^3 +\alpha^2 \quad +1$	1 0 0 0 1 1 0 1	141
α^{198}	$\alpha^2 +\alpha +1$	0 0 0 0 0 1 1 1	7
α^{199}	$\alpha^3 +\alpha^2 +\alpha$	0 0 0 0 1 1 1 0	14
α^{200}	$\alpha^4 +\alpha^3 +\alpha^2$	0 0 0 1 1 1 0 0	28
α^{201}	$\alpha^5 +\alpha^4 +\alpha^3$	0 0 1 1 1 0 0 0	56
α^{202}	$\alpha^6 +\alpha^5 +\alpha^4$	0 1 1 1 0 0 0 0	112
α^{203}	$\alpha^7 +\alpha^6 +\alpha^5$	1 1 1 0 0 0 0 0	224
α^{204}	$\alpha^7 +\alpha^6 \quad +\alpha^4 +\alpha^3 +\alpha^2 \quad +1$	1 1 0 1 1 1 0 1	221
α^{205}	$\alpha^7 \quad +\alpha^5 \quad +\alpha^2 +\alpha +1$	1 0 1 0 0 1 1 1	167
α^{206}	$\alpha^6 \quad +\alpha^4 \quad +\alpha +1$	0 1 0 1 0 0 1 1	83
α^{207}	$\alpha^7 \quad +\alpha^5 \quad +\alpha^2 +\alpha$	1 0 1 0 0 1 1 0	166
α^{208}	$\alpha^6 \quad +\alpha^4 \quad +1$	0 1 0 1 0 0 0 1	81
α^{209}	$\alpha^7 \quad +\alpha^5 \quad +\alpha$	1 0 1 0 0 0 1 0	162
α^{210}	$\alpha^6 \quad +\alpha^4 +\alpha^3 \quad +1$	0 1 0 1 1 0 0 1	89
α^{211}	$\alpha^7 \quad +\alpha^5 +\alpha^4 \quad +\alpha$	1 0 1 1 0 0 1 0	178
α^{212}	$\alpha^6 +\alpha^5 +\alpha^4 +\alpha^3 \quad +1$	0 1 1 1 1 0 0 1	121
α^{213}	$\alpha^7 +\alpha^6 +\alpha^5 +\alpha^4 \quad +\alpha$	1 1 1 1 0 0 1 0	242
α^{214}	$\alpha^7 +\alpha^6 +\alpha^5 +\alpha^4 +\alpha^3 \quad +1$	1 1 1 1 1 0 0 1	249
α^{215}	$\alpha^7 +\alpha^6 +\alpha^5 \quad +\alpha^3 +\alpha^2 +\alpha +1$	1 1 1 0 1 1 1 1	239
α^{216}	$\alpha^7 +\alpha^6 \quad +\alpha +1$	1 1 0 0 0 0 1 1	195
α^{217}	$\alpha^7 \quad +\alpha^4 +\alpha^3 \quad +\alpha +1$	1 0 0 1 1 0 1 1	155
α^{218}	$\alpha^5 \quad +\alpha^3 \quad +\alpha +1$	0 0 1 0 1 0 1 1	43
α^{219}	$\alpha^6 \quad +\alpha^4 \quad +\alpha^2 +\alpha$	0 1 0 1 0 1 1 0	86
α^{220}	$\alpha^7 \quad +\alpha^5 \quad +\alpha^3 +\alpha^2$	1 0 1 0 1 1 0 0	172
α^{221}	$\alpha^6 \quad +\alpha^2 \quad +1$	0 1 0 0 0 1 0 1	69
α^{222}	$\alpha^7 \quad +\alpha^3 \quad +\alpha$	1 0 0 0 1 0 1 0	138
α^{223}	$\alpha^3 \quad +1$	0 0 0 0 1 0 0 1	9

element of $GF(256)$	polynomial form	binary form	decimal form
α^{224}	$\alpha^4 + \alpha$	0 0 0 1 0 0 1 0	18
α^{225}	$\alpha^5 + \alpha^2$	0 0 1 0 0 1 0 0	36
α^{226}	$\alpha^6 + \alpha^3$	0 1 0 0 1 0 0 0	72
α^{227}	$\alpha^7 + \alpha^4$	1 0 0 1 0 0 0 0	144
α^{228}	$\alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + 1$	0 0 1 1 1 1 0 1	61
α^{229}	$\alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha$	0 1 1 1 1 0 1 0	122
α^{230}	$\alpha^7 + \alpha^6 + \alpha^5 + \alpha^4 + \alpha^2$	1 1 1 1 0 1 0 0	244
α^{231}	$\alpha^7 + \alpha^6 + \alpha^5 + \alpha^4 + \alpha^2 + 1$	1 1 1 1 0 1 0 1	245
α^{232}	$\alpha^7 + \alpha^6 + \alpha^5 + \alpha^4 + \alpha^2 + \alpha + 1$	1 1 1 1 0 1 1 1	247
α^{233}	$\alpha^7 + \alpha^6 + \alpha^5 + \alpha^4 + \alpha + 1$	1 1 1 1 0 0 1 1	243
α^{234}	$\alpha^7 + \alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha + 1$	1 1 1 1 1 0 1 1	251
α^{235}	$\alpha^7 + \alpha^6 + \alpha^5 + \alpha^3 + \alpha + 1$	1 1 1 0 1 0 1 1	235
α^{236}	$\alpha^7 + \alpha^6 + \alpha^3 + \alpha + 1$	1 1 0 0 1 0 1 1	203
α^{237}	$\alpha^7 + \alpha^3 + \alpha + 1$	1 0 0 0 1 0 1 1	139
α^{238}	$\alpha^3 + \alpha + 1$	0 0 0 0 1 0 1 1	11
α^{239}	$\alpha^4 + \alpha^2 + \alpha$	0 0 0 1 0 1 1 0	22
α^{240}	$\alpha^5 + \alpha^3 + \alpha^2$	0 0 1 0 1 1 0 0	44
α^{241}	$\alpha^6 + \alpha^4 + \alpha^3$	0 1 0 1 1 0 0 0	88
α^{242}	$\alpha^7 + \alpha^5 + \alpha^4$	1 0 1 1 0 0 0 0	176
α^{243}	$\alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + 1$	0 1 1 1 1 1 0 1	125
α^{244}	$\alpha^7 + \alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha$	1 1 1 1 1 0 1 0	250
α^{245}	$\alpha^7 + \alpha^6 + \alpha^5 + \alpha^3 + 1$	1 1 1 0 1 0 0 1	233
α^{246}	$\alpha^7 + \alpha^6 + \alpha^3 + \alpha^2 + \alpha + 1$	1 1 0 0 1 1 1 1	207
α^{247}	$\alpha^7 + \alpha + 1$	1 0 0 0 0 0 1 1	131
α^{248}	$\alpha^4 + \alpha^3 + \alpha + 1$	0 0 0 1 1 0 1 1	27
α^{249}	$\alpha^5 + \alpha^4 + \alpha^2 + \alpha$	0 0 1 1 0 1 1 0	54
α^{250}	$\alpha^6 + \alpha^5 + \alpha^3 + \alpha^2$	0 1 1 0 1 1 0 0	108
α^{251}	$\alpha^7 + \alpha^6 + \alpha^4 + \alpha^3$	1 1 0 1 1 0 0 0	216
α^{252}	$\alpha^7 + \alpha^5 + \alpha^3 + \alpha^2 + 1$	1 0 1 0 1 1 0 1	173
α^{253}	$\alpha^6 + \alpha^2 + \alpha + 1$	0 1 0 0 0 1 1 1	71
α^{254}	$\alpha^7 + \alpha^3 + \alpha^2 + \alpha$	1 0 0 0 1 1 1 0	142

References

[NIS01] NIST. Data Encryption Standard (AES). Technical Report FIPS PUB 197, National Institute of Standards and Technology, Washington DC, November 2001.