A(x) = x6 + x5 + x4 + x → 01110010 → 0x72 a = bq + r deg(b) > deg(r)

P(x) = x8 + x4 + x3 + x + 1

A(x) A-1(x) = 1 mod P(x)

A-1(x)= (x6 + x5 + x4 + x)-1 mod (x8 + x4 + x3 + x + 1)

Use extended Euclidean algorithm to find inverse polynomial.

x8 + x4 + x3 + x + 1 = (x6 + x5 + x4 + x)q + r

Find a q such that deg(r) < deg(b):

q must be degree 2 in order for the equality to be preserved.

q = x2:

(x6 + x5 + x4 + x)(x2) + r = b

(x8 + x7 + x6 + x3) + r = x8 + x4 + x3 + x + 1

r = (1+1)x8 + x7 + x6 + x4 + (1+1)x3 + x + 1

r = x7 + x6 + x4 + x + 1

deg(r) = 7 ≮ deg(b) = 6 not viable

q = x2 + 1:

(x6 + x5 + x4 + x)(x2 + 1) + r = a

(x8 + x7 + x6 + x3 + x6 + x5 + x4 + x) + r = a

(x8 + x7 + (1+1)x6 + x5 + x4 + x3 + x) + r = a

(x8 + x7 + x5 + x4 + x3 + x) + r = x8 + x4 + x3 + x + 1

r = (1+1)x8 + x7 + x5 + (1+1)x4 + (1+1)x3 + (1+1)x + 1

r = x7 + x5 + 1

deg(r) = 7 ≮ deg(b) = 6 not viable

q = x2 + x:

(x6 + x5 + x4 + x)(x2 + x) + r = a

(x8 + x7 + x6 + x3 + x7 + x6 + x5 + x2) + r = a

(x8 + (1+1)x7 + (1+1)x6 + x5 + x3 + x2) + r = a

(x8 + x5 + x3 + x2) + r = x8 + x4 + x3 + x + 1

r = (1+1)x8 + x5 + x4 + (1+1)x3 + x2 + x + 1

r = x5 + x4 + x2 + x + 1

deg(r) = 5 < deg(b) = 6 viable

q = x2 + x + 1: (Example to show that the solution q is unique)

(x6 + x5 + x4 + x)(x2 + x + 1) + r = a

(x8 + x7 + x6 + x3 + x7 + x6 + x5 + x2 + x6 + x5 + x4 + x) + r = a

(x8 + (1+1)x7 + (1+1+1)x6 + (1+1)x5 + x4 + x3 + x2 + x) + r = a

(x8 + x6 + x4 + x3 + x2 + x) + r = x8 + x4 + x3 + x + 1

r = (1+1)x8 + x6 + (1+1)x4 + (1+1)x3 + x2 + (1+1)x + 1

r = x6 + x2 + 1

deg(r) = 6 ≮ deg(b) = 6 not viable

x8 + x4 + x3 + x + 1 = (x6 + x5 + x4 + x)(x2 + x) + (x5 + x4 + x2 + x + 1)

x6 + x5 + x4 + x = (x5 + x4 + x2 + x + 1)q + r

Find a q such that deg(r) < deg(b):

q = x:

(x5 + x4 + x2 + x + 1)(x) + r = a

(x6 + x5 + x3 + x2 + x) + r = x6 + x5 + x4 + x

r = (1+1)x6 + (1+1)x5 + x4 + x3 + x2 + (1+1)x

r = x4 + x3 + x2

deg(r) = 4 < deg(b) = 5 viable

x6 + x5 + x4 + x = (x5 + x4 + x2 + x + 1)(x) + (x4 + x3 + x2)

x5 + x4 + x2 + x + 1 = (x4 + x3 + x2)q + r

Find a q such that deg(r) < deg(b):

q = x:

(x4 + x3 + x2)(x) + r = x5 + x4 + x2 + x + 1

(x5 + x4 + x3) + r = x5 + x4 + x2 + x + 1

r = (1+1)x5 + (1+1)x4 + x3 + x2 + x + 1

r = x3 + x2 + x + 1

deg(r) = 3 < deg(b) = 4 viable

x5 + x4 + x2 + x + 1 = (x4 + x3 + x2)(x) + (x3 + x2 + x + 1)

x4 + x3 + x2 = (x3 + x2 + x + 1)q + r

Find a q such that deg(r) < deg(b):

q = x:

(x3 + x2 + x + 1)(x) + r = x4 + x3 + x2

(x4 + x3 + x2 + x) + r = x4 + x3 + x2

r = (1+1)x4 + (1+1)x3 + (1+1)x2 + x

r = x

deg(r) = 1 < deg(b) = 3 viable

x4 + x3 + x2 = (x3 + x2 + x + 1)(x) + (x)

x3 + x2 + x + 1 = (x)q + r

Find a q such that deg(r) < deg(b):

q = x2:

(x)(x2) + r = x3 + x2 + x + 1

(x3) + r = x3 + x2 + x + 1

r = (1+1)x3 + x2 + x + 1

r = x2 + x + 1

deg(r) = 2 ≮ deg(b) = 1 not viable

q = x2 + 1:

(x)(x2 + 1) + r = x3 + x2 + x + 1

(x3 + x) + r = x3 + x2 + x + 1

r = (1+1)x3 + x2 + (1+1)x + 1

r = x2 + 1

deg(r) = 2 ≮ deg(b) = 1 not viable

q = x2 + x:

(x)(x2 + x) + r = x3 + x2 + x + 1

(x3 + x2) + r = x3 + x2 + x + 1

r = (1+1)x3 + (1+1)x2 + x + 1

r = x + 1

deg(r) = 1 ≮ deg(b) = 1 not viable

q = x2 + x + 1:

(x)(x2 + x + 1) + r = x3 + x2 + x + 1

(x3 + x2 + x) + r = x3 + x2 + x + 1

r = (1+1)x3 + (1+1)x2 + (1+1)x + 1

r = 1

deg(r) = 0 < deg(b) = 1 viable

x3 + x2 + x + 1 = (x)(x2 + x + 1) + (1)

x8 + x4 + x3 + x + 1 = (x6 + x5 + x4 + x)(x2 + x) + (x5 + x4 + x2 + x + 1)

x6 + x5 + x4 + x = (x5 + x4 + x2 + x + 1)(x) + (x4 + x3 + x2)

x5 + x4 + x2 + x + 1 = (x4 + x3 + x2)(x) + (x3 + x2 + x + 1)

x4 + x3 + x2 = (x3 + x2 + x + 1)(x) + (x)

x3 + x2 + x + 1 = (x)(x2 + x + 1) + (1)

1 = (x3 + x2 + x + 1) + (x)(x2 + x + 1)

x = (x4 + x3 + x2) + (x3 + x2 + x + 1)(x)

x3 + x2 + x + 1 = (x5 + x4 + x2 + x + 1) + (x4 + x3 + x2)(x)

x4 + x3 + x2 = (x6 + x5 + x4 + x) + (x5 + x4 + x2 + x + 1)(x)

x5 + x4 + x2 + x + 1 = (x8 + x4 + x3 + x + 1) + (x6 + x5 + x4 + x)(x2 + x)

Solve:

1 = (x3 + x2 + x + 1) + (x)(x2 + x + 1)

Substitute (x4 + x3 + x2) + (x3 + x2 + x + 1)(x) for x:

1 = (x3 + x2 + x + 1) + ((x4 + x3 + x2) + (x3 + x2 + x + 1)(x))(x2 + x + 1)

1 = (x3 + x2 + x + 1) + ((x4 + x3 + x2)(x2 + x + 1) + (x3 + x2 + x + 1)(x3 + x2 + x))

1 = (x3 + x2 + x + 1)(x3 + x2 + x + 1) + (x4 + x3 + x2)(x2 + x + 1)

Substitute (x5 + x4 + x2 + x + 1) + (x4 + x3 + x2)(x) for x3 + x2 + x + 1:

1 = ((x5 + x4 + x2 + x + 1) + (x4 + x3 + x2)(x))(x3 + x2 + x + 1) + (x4 + x3 + x2)(x2 + x + 1)

1 = ((x5 + x4 + x2 + x + 1)(x3 + x2 + x + 1) + (x4 + x3 + x2)(x4 + x3 + x2 + x)) + (x4 + x3 + x2)(x2 + x + 1)

1 = (x5 + x4 + x2 + x + 1)(x3 + x2 + x + 1) + (x4 + x3 + x2)(x4 + x3 + (1+1)x2 + (1+1)x + 1)

1 = (x5 + x4 + x2 + x + 1)(x3 + x2 + x + 1) + (x4 + x3 + x2)(x4 + x3 + 1)

Substitute (x6 + x5 + x4 + x) + (x5 + x4 + x2 + x + 1)(x) for x4 + x3 + x2:

1 = (x5 + x4 + x2 + x + 1)(x3 + x2 + x + 1) + ((x6 + x5 + x4 + x) + (x5 + x4 + x2 + x + 1)(x))(x4 + x3 + 1)

1 = (x5 + x4 + x2 + x + 1)(x3 + x2 + x + 1) + ((x6 + x5 + x4 + x)(x4 + x3 + 1) + (x5 + x4 + x2 + x + 1)(x5 + x4 + x)

1 = (x5 + x4 + x2 + x + 1)(x5 + x4 + x3 + x2 + (1+1)x + 1) + (x6 + x5 + x4 + x)(x4 + x3 + 1)

1 = (x5 + x4 + x2 + x + 1)(x5 + x4 + x3 + x2 + 1) + (x6 + x5 + x4 + x)(x4 + x3 + 1)

Substitute (x8 + x4 + x3 + x + 1) + (x6 + x5 + x4 + x)(x2 + x) for x5 + x4 + x2 + x + 1:

1 = ((x8 + x4 + x3 + x + 1) + (x6 + x5 + x4 + x)(x2 + x))(x5 + x4 + x3 + x2 + 1) + (x6 + x5 + x4 + x)(x4 + x3 + 1)

1 = ((x8 + x4 + x3 + x + 1)(x5 + x4 + x3 + x2 + 1) + (x6 + x5 + x4 + x)(x7 + x6 + x5 + x4 + x2 + x6 + x5 + x4 + x3 + x)) + (x6 + x5 + x4 + x)(x4 + x3 + 1)

1 = ((x8 + x4 + x3 + x + 1)(x5 + x4 + x3 + x2 + 1) + (x6 + x5 + x4 + x)(x7 + (1+1)x6 + (1+1)x5 + (1+1)x4 + x3 + x2 + x)) + (x6 + x5 + x4 + x)(x4 + x3 + 1)

1 = ((x8 + x4 + x3 + x + 1)(x5 + x4 + x3 + x2 + 1) + (x6 + x5 + x4 + x)(x7 + x3 + x2 + x)) + (x6 + x5 + x4 + x)(x4 + x3 + 1)

1 = (x8 + x4 + x3 + x + 1)(x5 + x4 + x3 + x2 + 1) + (x6 + x5 + x4 + x)(x7 + x4 + (1+1)x3 + x2 + x + 1)

1 = (x8 + x4 + x3 + x + 1)(x5 + x4 + x3 + x2 + 1) + (x6 + x5 + x4 + x)**(x7 + x4 + x2 + x + 1)**

A(x) = x6 + x5 + x4 + x → 01110010 → 0x72

A-1(x) = x7 + x4 + x2 + x + 1 → 10010111 → 0x97

| 1 0 0 0 1 1 1 1 | | x0 | | 1 | | b0 |

| 1 1 0 0 0 1 1 1 | | x1 | | 1 | | b1 |

| 1 1 1 0 0 0 1 1 | | x2 | | 0 | | b2 |

| 1 1 1 1 0 0 0 1 | x | x3 | + | 0 | = | b3 |

| 1 1 1 1 1 0 0 0 | | x4 | | 0 | | b4 |

| 0 1 1 1 1 1 0 0 | | x5 | | 1 | | b5 |

| 0 0 1 1 1 1 1 0 | | x6 | | 1 | | b6 |

| 0 0 0 1 1 1 1 1 | | x7 | | 0 | | b7 |

| 1 0 0 0 1 1 1 1 | | 1 | | 1 | | b0 |

| 1 1 0 0 0 1 1 1 | | 1 | | 1 | | b1 |

| 1 1 1 0 0 0 1 1 | | 1 | | 0 | | b2 |

| 1 1 1 1 0 0 0 1 | x | 0 | + | 0 | = | b3 |

| 1 1 1 1 1 0 0 0 | | 1 | | 0 | | b4 |

| 0 1 1 1 1 1 0 0 | | 0 | | 1 | | b5 |

| 0 0 1 1 1 1 1 0 | | 0 | | 1 | | b6 |

| 0 0 0 1 1 1 1 1 | | 1 | | 0 | | b7 |

b0 = (1)(1) + (0)(1) + (0)(1) + (0)(0) + (1)(1) + (1)(0) + (1)(0) + (1)(1) + 1 = (1+1+1)+1 = 0

b1 = (1)(1) + (1)(1) + (0)(1) + (0)(0) + (0)(1) + (1)(0) + (1)(0) + (1)(1) + 1 = (1+1+1)+1 = 0

b2 = (1)(1) + (1)(1) + (1)(1) + (0)(0) + (0)(1) + (0)(0) + (1)(0) + (1)(1) + 0 = (1+1+1+1) = 0

b3 = (1)(1) + (1)(1) + (1)(1) + (1)(0) + (0)(1) + (0)(0) + (0)(0) + (1)(1) + 0 = (1+1+1+1) = 0

b4 = (1)(1) + (1)(1) + (1)(1) + (1)(0) + (1)(1) + (0)(0) + (0)(0) + (0)(1) + 0 = (1+1+1+1) = 0

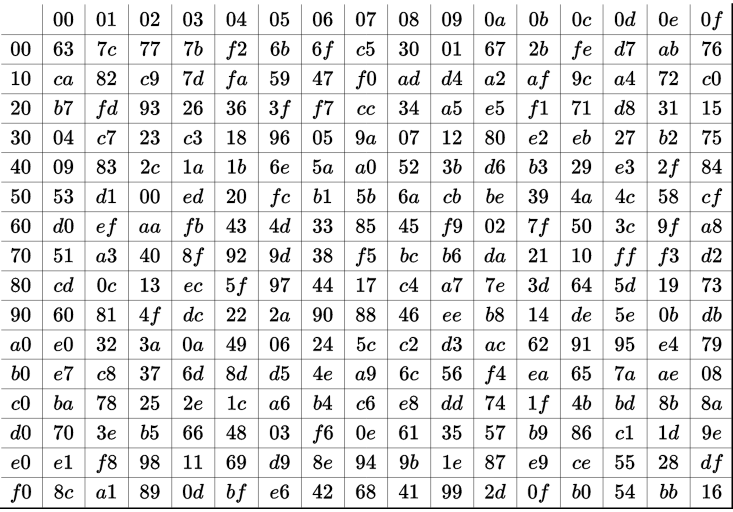
b5 = (0)(1) + (1)(1) + (1)(1) + (1)(0) + (1)(1) + (1)(0) + (0)(0) + (0)(1) + 1 = (1+1+1)+1 = 0

b6 = (0)(1) + (0)(1) + (1)(1) + (1)(0) + (1)(1) + (1)(0) + (1)(0) + (0)(1) + 1 = (1+1)+1 = 1

b7 = (0)(1) + (0)(1) + (0)(1) + (1)(0) + (1)(1) + (1)(0) + (1)(0) + (1)(1) + 0 = (1+1) = 0

B(x) = 01000000 → 0x40

Therefore, 0x72 maps to 0x40.



Check:

(x6 + x5 + x4 + x)(x7 + x4 + x2 + x + 1) = 1

(x13 + x12 + x11 + x8) + (x10 + x9 + x8 + x5) + (x8 + x7 + x6 + x3) + (x7 + x6 + x5 + x2) + (x6 + x5 + x4 + x)

x13 + x12 + x11 + x10 + x9 + (1+1+1)x8 + (1+1)x7 + (1+1+1)x6 + (1+1+1)x5 + x4 + x3 + x2 + x = 1 mod P(x)

(x13 + x12 + x11 + x10 + x9 + x8 + x6 + x5 + x4 + x3 + x2 + x) mod P(x)= 1

x13 + x12 + x11 + x10 + x9 + x8 + x6 + x5 + x4 + x3 + x2 + x → 11111101111110 P(x) → 100011011

11111101111110

100011011

---------

01110000011110

100011011

---------

0110110101110

100011011

---------

010101110110

100011011

---------

00100011010

100011011

---------

000000001 Value equals 1, so the polynomials are inverses of each other.