$A(x) = x^6 + x^5 + x^4 + x \rightarrow 01110010 \rightarrow 0x72$ $\quad a = bq + r \quad deg(b) > deg(r)$

$P(x) = x^8 + x^4 + x^3 + x + 1$

$A(x)\ A^{-1}(x) = 1 \bmod P(x)$

$A^{-1}(x) = (x^6 + x^5 + x^4 + x)^{-1} \bmod (x^8 + x^4 + x^3 + x + 1)$

Use extended Euclidean algorithm to find inverse polynomial.

$x^8 + x^4 + x^3 + x + 1 = (x^6 + x^5 + x^4 + x)q + r$

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

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

$q = x^2$:

$(x^6 + x^5 + x^4 + x)(x^2) + r = b$

$(x^8 + x^7 + x^6 + x^3) + r = x^8 + x^4 + x^3 + x + 1$

$r = (1+1)x^8 + x^7 + x^6 + x^4 + (1+1)x^3 + x + 1$

$r = x^7 + x^6 + x^4 + x + 1$

$deg(r) = 7 \not< deg(b) = 6$ not viable

$q = x^2 + 1$:

$(x^6 + x^5 + x^4 + x)(x^2 + 1) + r = a$

$(x^8 + x^7 + x^6 + x^3 + x^6 + x^5 + x^4 + x) + r = a$

$(x^8 + x^7 + (1+1)x^6 + x^5 + x^4 + x^3 + x) + r = a$

$(x^8 + x^7 + x^5 + x^4 + x^3 + x) + r = x^8 + x^4 + x^3 + x + 1$

$r = (1+1)x^8 + x^7 + x^5 + (1+1)x^4 + (1+1)x^3 + (1+1)x + 1$

$r = x^7 + x^5 + 1$

$deg(r) = 7 \not< deg(b) = 6$ not viable

$q = x^2 + x$:

$(x^6 + x^5 + x^4 + x)(x^2 + x) + r = a$

$(x^8 + x^7 + x^6 + x^3 + x^7 + x^6 + x^5 + x^2) + r = a$

$(x^8 + (1+1)x^7 + (1+1)x^6 + x^5 + x^3 + x^2) + r = a$

$(x^8 + x^5 + x^3 + x^2) + r = x^8 + x^4 + x^3 + x + 1$

$r = (1+1)x^8 + x^5 + x^4 + (1+1)x^3 + x^2 + x + 1$

$r = x^5 + x^4 + x^2 + x + 1$

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

$q = x^2 + x + 1$: (Example to show that the solution q is unique)

$(x^6 + x^5 + x^4 + x)(x^2 + x + 1) + r = a$

$(x^8 + x^7 + x^6 + x^3 + x^7 + x^6 + x^5 + x^2 + x^6 + x^5 + x^4 + x) + r = a$

$(x^8 + (1+1)x^7 + (1+1+1)x^6 + (1+1)x^5 + x^4 + x^3 + x^2 + x) + r = a$

$(x^8 + x^6 + x^4 + x^3 + x^2 + x) + r = x^8 + x^4 + x^3 + x + 1$

$r = (1+1)x^8 + x^6 + (1+1)x^4 + (1+1)x^3 + x^2 + (1+1)x + 1$

$r = x^6 + x^2 + 1$

$deg(r) = 6 \not< deg(b) = 6$ not viable

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

$x^6 + x^5 + x^4 + x = (x^5 + x^4 + x^2 + x + 1)q + r$

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

$q = x$:

$(x^5 + x^4 + x^2 + x + 1)(x) + r = a$

$(x^6 + x^5 + x^3 + x^2 + x) + r = x^6 + x^5 + x^4 + x$

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

$r = x^4 + x^3 + x^2$

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

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

$x^5 + x^4 + x^2 + x + 1 = (x^4 + x^3 + x^2)q + r$

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

$q = x$:

$(x^4 + x^3 + x^2)(x) + r = x^5 + x^4 + x^2 + x + 1$

$(x^5 + x^4 + x^3) + r = x^5 + x^4 + x^2 + x + 1$

$r = (1+1)x^5 + (1+1)x^4 + x^3 + x^2 + x + 1$

$r = x^3 + x^2 + x + 1$

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

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

$x^4 + x^3 + x^2 = (x^3 + x^2 + x + 1)q + r$

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

q = x:

$(x^3 + x^2 + x + 1)(x) + r = x^4 + x^3 + x^2$
$(x^4 + x^3 + x^2 + x) + r = x^4 + x^3 + x^2$
$r = (1+1)x^4 + (1+1)x^3 + (1+1)x^2 + x$
$r = x$
$\deg(r) = 1 < \deg(b) = 3$ viable

$x^4 + x^3 + x^2 = (x^3 + x^2 + x + 1)(x) + (x)$
$x^3 + x^2 + x + 1 = (x)q + r$

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

q = x^2:

$(x)(x^2) + r = x^3 + x^2 + x + 1$
$(x^3) + r = x^3 + x^2 + x + 1$
$r = (1+1)x^3 + x^2 + x + 1$
$r = x^2 + x + 1$
$\deg(r) = 2 \nless \deg(b) = 1$ not viable

q = $x^2 + 1$:

$(x)(x^2 + 1) + r = x^3 + x^2 + x + 1$
$(x^3 + x) + r = x^3 + x^2 + x + 1$
$r = (1+1)x^3 + x^2 + (1+1)x + 1$
$r = x^2 + 1$
$\deg(r) = 2 \nless \deg(b) = 1$ not viable

q = $x^2 + x$:

$(x)(x^2 + x) + r = x^3 + x^2 + x + 1$
$(x^3 + x^2) + r = x^3 + x^2 + x + 1$
$r = (1+1)x^3 + (1+1)x^2 + x + 1$
$r = x + 1$
$\deg(r) = 1 \nless \deg(b) = 1$ not viable

q = $x^2 + x + 1$:

$(x)(x^2 + x + 1) + r = x^3 + x^2 + x + 1$
$(x^3 + x^2 + x) + r = x^3 + x^2 + x + 1$
$r = (1+1)x^3 + (1+1)x^2 + (1+1)x + 1$
$r = 1$
$\deg(r) = 0 < \deg(b) = 1$ viable

$x^3 + x^2 + x + 1 = (x)(x^2 + x + 1) + (1)$

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

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

Solve:

$1 = (x^3 + x^2 + x + 1) + (x)(x^2 + x + 1)$

Substitute $(x^4 + x^3 + x^2) + (x^3 + x^2 + x + 1)(x)$ for x:

$1 = (x^3 + x^2 + x + 1) + ((x^4 + x^3 + x^2) + (x^3 + x^2 + x + 1)(x))(x^2 + x + 1)$
$1 = (x^3 + x^2 + x + 1) + ((x^4 + x^3 + x^2)(x^2 + x + 1) + (x^3 + x^2 + x + 1)(x^3 + x^2 + x))$
$1 = (x^3 + x^2 + x + 1)(x^3 + x^2 + x + 1) + (x^4 + x^3 + x^2)(x^2 + x + 1)$

Substitute $(x^5 + x^4 + x^2 + x + 1) + (x^4 + x^3 + x^2)(x)$ for $x^3 + x^2 + x + 1$:

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

Substitute $(x^6 + x^5 + x^4 + x) + (x^5 + x^4 + x^2 + x + 1)(x)$ for $x^4 + x^3 + x^2$:

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

Substitute $(x^8 + x^4 + x^3 + x + 1) + (x^6 + x^5 + x^4 + x)(x^2 + x)$ for $x^5 + x^4 + x^2 + x + 1$:

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

$A(x) = x^6 + x^5 + x^4 + x \rightarrow 01110010 \rightarrow 0x72$

$A^{-1}(x) = x^7 + x^4 + x^2 + x + 1 \rightarrow 10010111 \rightarrow 0x97$

$$
\begin{vmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{vmatrix} \quad x \quad \begin{vmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{vmatrix} + \begin{vmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{vmatrix} = \begin{vmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{vmatrix}
$$

$$
\begin{vmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{vmatrix} \quad x \quad \begin{vmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{vmatrix} + \begin{vmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{vmatrix} = \begin{vmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{vmatrix}
$$

$b_0 = (1)(1) + (0)(1) + (0)(1) + (0)(0) + (1)(1) + (1)(0) + (1)(0) + (1)(1) + 1 = (1+1+1)+1 = 0$

$b_1 = (1)(1) + (1)(1) + (0)(1) + (0)(0) + (0)(1) + (1)(0) + (1)(0) + (1)(1) + 1 = (1+1+1)+1 = 0$

$b_2 = (1)(1) + (1)(1) + (1)(1) + (0)(0) + (0)(1) + (0)(0) + (1)(0) + (1)(1) + 0 = (1+1+1+1) = 0$

$b_3 = (1)(1) + (1)(1) + (1)(1) + (1)(0) + (0)(1) + (0)(0) + (0)(0) + (1)(1) + 0 = (1+1+1+1) = 0$

$b_4 = (1)(1) + (1)(1) + (1)(1) + (1)(0) + (1)(1) + (0)(0) + (0)(0) + (0)(1) + 0 = (1+1+1+1) = 0$

$b_5 = (0)(1) + (1)(1) + (1)(1) + (1)(0) + (1)(1) + (1)(0) + (0)(0) + (0)(1) + 1 = (1+1+1)+1 = 0$

$b_6 = (0)(1) + (0)(1) + (1)(1) + (1)(0) + (1)(1) + (1)(0) + (1)(0) + (0)(1) + 1 = (1+1)+1 = 1$

$b_7 = (0)(1) + (0)(1) + (0)(1) + (1)(0) + (1)(1) + (1)(0) + (1)(0) + (1)(1) + 0 = (1+1) = 0$

$B(x) = 01000000 \rightarrow 0x40$

Therefore, 0x72 maps to 0x40.

	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
10	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
20	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
30	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
40	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
50	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
60	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
70	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
80	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
90	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a0	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b0	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c0	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d0	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e0	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f0	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Check:

$(x^6 + x^5 + x^4 + x)(x^7 + x^4 + x^2 + x + 1) = 1$

$(x^{13} + x^{12} + x^{11} + x^8) + (x^{10} + x^9 + x^8 + x^5) + (x^8 + x^7 + x^6 + x^3) + (x^7 + x^6 + x^5 + x^2) + (x^6 + x^5 + x^4 + x)$

$x^{13} + x^{12} + x^{11} + x^{10} + x^9 + (1+1+1)x^8 + (1+1)x^7 + (1+1+1)x^6 + (1+1+1)x^5 + x^4 + x^3 + x^2 + x = 1 \bmod P(x)$

$(x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + x^2 + x) \bmod P(x) = 1$

$x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + x^2 + x \rightarrow 11111101111110$ $P(x) \rightarrow 100011011$

```
11111101111110
100011011
---------
01110000011110
 100011011
 ---------
 0110110101110
  100011011
  ---------
  010101110110
   100011011
   ---------
   00100011010
     100011011
     ---------
     000000001   Value equals 1, so the polynomials are inverses of each other.
```