CIS 3362 11/24/25

Q5

need determinant mod inverse

$det = 18 \times 12 - 11 \times 17$

$= 216 - 187$

$= 29$, $29^{-1} \bmod 64$ is needed for the formula

Q8

$4^8 = (2^2)^8 = 2^{16}$

S1, 15 appears in row 0 col 5

So 1st 6 bits of input could be

0 0101 0

Q10

Row 3 Col 4

formula sheet

Skit matrix

$$R3 \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \quad \begin{bmatrix} 01 & A9 & E9 & 29 \\ 84 & 39 & F3 & 6A \\ C9 & C3 & 2B & B3 \\ A3 & 47 & C1 & 9D \end{bmatrix}$$

Col 4

$01 \times 29 + 01 \times 6A + 02 \times B3 + 03 \times 9D$

Fermat Factoring

$$496597 = \cancel{x \cdot y}\ a \cdot b$$

$$= (x+y)(x-y)$$

$$= x^2 - y^2$$

$$x^2 = y^2 + 496597$$

$$x > \sqrt{496597} \approx 704.69$$

x	$x^2 - 496597$	Is square?
705	428	x
706	1839	x
707	3252	x
708	4667	x
709	6084	yes = 78

$$496597 = (709+78)(709-78)$$

$$= 787 \times 631$$

Q15

(a) $x=5, \quad y^2 = (x^3 + 3x + 8) \bmod 47$

1. $5^3 + 3(5) + 8 \bmod 47$

$= 125 + 15 + 8$

$= 148 \equiv \underline{\underline{7}} \pmod{47}$

Calculate $7^{\frac{47-1}{2}} = 7^{\underline{\underline{23}}} \bmod 47$

$7^2 \equiv 49 \equiv 2 \bmod 47$

$(7^{10}) \equiv (7^2)^5 \equiv 2^5 \equiv 32 \bmod 47$

$(7^{12}) \equiv (7^2)^6 \equiv 2^6 \equiv 64 \equiv \boxed{17} \bmod 47$

$7^{23} \equiv 7^{10} \times 7^{12} \times 7 \equiv 32 \times 17 \times 7$

$\equiv 1 \bmod 47$ ✓

(b) $a c^{\frac{p+1}{4}} = 7^{\frac{47+1}{4}} = 7^{12} \equiv 17 \bmod 47$

from part (a) work!

pts are $\boxed{(5, 17)}$, $(5, 47-17)$

$\boxed{(5, 30)}$

✓ $17^2 \equiv 7 \bmod 47$ } Double

✓ $30^2 \equiv 7 \bmod 47$ } Check