Assignment 1

CS 4801 Cryptography

* Number 1 on this homework is in a separate word document file attached on Canvas.

2a(i) $27 \cdot 13 \equiv 351 \bmod 23$

$6 \bmod 23$

$23\overline{)351}$ → 15, -23, 121, -115, 6

2a(ii) $17 \cdot 13 \equiv 221 \bmod 23$

$14 \bmod 23$

$23\overline{)221}$ → 9, -207, 14

2a(iii) $28 \equiv 4 \quad 15 \equiv 3$

$4 \cdot 3 \bmod 12 = 12 \bmod 12$

$0 \bmod 12$

$12\overline{)28}$ → $2R4$, -24, 4

$12\overline{)15}$ → $1R3$, -12, 3

$12\overline{)420}$ → 35, -36, 60, -60, 0

2a(iv) $15 \cdot 29 \bmod 23 + 11 \cdot 15 \bmod 23$

$435 \bmod 23 + 165 \bmod 23$

$21 \bmod 23 + 4 \bmod 23$

$25 \bmod 23 \equiv 2 \bmod 23$

$23\overline{)435}$ → $18R21$, -23, 205, -184, 21

$23\overline{)165}$ → 7, -161, 4

2b(i) Possibilities: $17 \times 1 + 1 = 18$, $17 \times 2 + 1 = 35$, $17 \times 3 + 1 = 52$

$4 \times 13 = 52$ So answer is $13 \bmod 17$

2b(ii) Possibilities: $17 \times 1 + 1 = 18$, $17 \times 2 + 1 = 35$ ←

$7 \times 5 = 35$ So answer is $5 \bmod 17$

2b(iii) Possibilities: $37 \times 1 + 1 = 38$, $37 \times 2 + 1 = 75$ ←

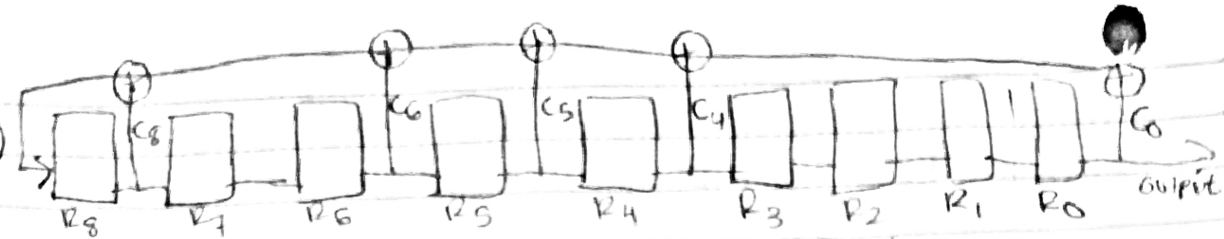
$5 \times 15 = 75$ So answer is $15 \bmod 37$

2b(iv) NO inverses exist because $\gcd(10, 15) \neq 1$.

3. modulo 36 means there are elements from $\{0, 1, 2, \ldots, 35\}$. If $a^{-1} \bmod n$ where $\gcd(a, n) \neq 1$, then there are no multiplicative inverses. So, based on this property, inverses are:

$\{2, 3, 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, 22, 24, 26, 27, 28, 30, 32, 33, 34\}$

4a)



b)

$x^8+x^6+x^5+x^4+1$ → initial state

C_8	C_7	C_6	C_5	C_4	C_3	C_2	C_1	C_0	Output
0	0	1	0	1	1	0	0	0	
0	0	0	1	0	1	1	0	0	0
1	0	0	0	1	0	1	1	0	0
0	1	0	0	0	1	0	1	1	0
1	0	1	0	0	0	1	0	1	1
1	1	0	1	0	0	0	1	0	1
0	1	1	0	1	0	0	0	1	0
1	0	1	1	0	1	0	0	0	1
1	1	0	1	1	0	1	0	0	0
1	1	1	0	1	1	0	1	0	0
1	1	1	1	0	1	1	0	1	0
0	1	1	1	1	0	1	1	0	1
1	0	1	1	1	1	0	1	1	0
1	1	0	1	1	1	1	0	1	1
0	1	1	0	1	1	1	1	0	1
0	0	1	1	0	1	1	1	1	0
1	0	0	1	1	0	1	1	1	1
0	1	0	0	1	1	0	1	1	1
0	0	1	0	0	1	1	0	1	1
0	0	0	1	0	0	1	1	0	1
1	0	0	0	1	0	0	1	1	0
1	1	0	0	0	1	0	0	1	1
									1
									0
									0
									1
									0
									0
									0
									1
									1

4c)

f: 1 0 0 0 1 0 0 1 1 0 1 1 1 1 0 1 1 0 1 0 0 0 1 0 1 1 0 0 0

1 1 1 0 1 1 1 0 0 0 0 0 1 1 0 1 1 1 0 1 1 0 1 0 0 1 1 1 1 1 0

0 0 1 0 1 0 0 0 1 1 1 0 0 0 1 0 1 0 1 1 1 0 0 1 0 1 1 0 0 1 1 0