3.1 Solve the congruencies

(c) $x^{73} \equiv 614 \pmod{1159}$ $\quad [1159 = 19 \cdot 61]$

$18 \cdot 60 = 1080$

Solve

$73x \equiv 1 \bmod 1080$

$1080 = 73(14) + 58$

$73 = 58(1) + 15$

$58 = 15(3) + 13$

$15 = 13(1) + 2$

$13 = 2(6) + 1$

$2 = 1(2) + 0$

$\gcd(73, 1080) = 1$

$1 = 13 - 6(2)$

$13 - 6(15 - 13(1)) = 13(7) - 15(6)$

$(58 - 15(3))(7) - 15(6) = 58(7) - 15(27)$

$= 58(7) - (73 - 58)(27) = 58(34) - 73(27)$

$= (1080 - 73(14))(34) - 73(27)$

$= 1080(34) - 73(475)$

$73^{-1} \equiv -475 \equiv 577 \bmod 1080$

$\rightarrow X \equiv 614^{577} \bmod 1159$

$X \equiv 158 \bmod 1159$

2.

(a) Smallest encryption exponent?

$(p-1)(q-1) = 30 \cdot 42 = 1260$

$\gcd(11, 1260) = 1$

$e = 11$.

(b) Public key?

Consists of (N, e)

$N = pq = 31 \cdot 43 = 1333$

Public key $(1333, 11)$

(c) $ed \equiv 1 \bmod 1260$

Find $11^{-1} \bmod 1260$

$1260 = 11(114) + 6$

$11 = 6(1) + 5$

$6 = 5(1) + 1$

$5 = 1(5) + 0$

$1 = 6 - 1(5)$

$1 = 6 - 1(11 - 1(6)) = 2(6) - 1(11)$

$1 = 2(1260 - 114(11)) - 1(11)$

$1 = 2(1260) - 229(11)$

$d = -229 \bmod 1260$

$d = 1260 - 229 = 1031$

$d = 1031$

(d)

$$C = m^e \equiv 29^{11} \equiv$$

$$29^{11} = 29^8 \times 29^2 \times 29^1$$

$$29^1 = 29$$
$$29^2 = 841$$
$$29^4 \equiv 841^2 \equiv 707281 \bmod 1333 = 791 \bmod 1333$$
$$29^8 \equiv 791^2 \equiv 504$$

$$504 \times 841 \times 29 = 463$$

$C = 463$

(e) $m = c^d \equiv 517^{1031} \bmod 1333$

$1031_{10} = 10000000111_2$

$m = 818$

3.7

(a) $C = m^e \equiv 892383^{103} \bmod 2038667$

$C = 45293 \bmod 2038667$

(b) d is the inverse of $e = 103 \bmod (p-1)(q-1)$

$N = 2038667 = 1301 \cdot x =$

$x = 1567$

$(1300)(1566) = 2035800$

$d \equiv 103^{-1} \bmod 2035800$

$d \equiv 810367 \bmod 2035800$

(c) $C = 317730$, Decrypt

$m = c^d \equiv 317730^{810367} \bmod 2038667$

$m = 514407$

4. Determine if a is a Fermat Witness for $n = 253$

(a) $a = 2$

(b) $a = 22$

(a) $a = 2$

$a^n \not\equiv a \bmod n$

$2^{253} \equiv 162 \bmod 253$

$162 \not\equiv 2$, So, 2 is A Fermat Witness to 253.

(b) $a = 22$

$22^{253} \equiv 22$ ✗

22 is Not A Fermat Witness to 253

5.

(a) $n = 1105$

$n-1 = 1104 = 2^4 \times 69$

$2^{69} \equiv 967$ ✓ $(\bmod 1105)$

$2^{2 \cdot 69} \equiv 829$ ✓

$2^{4 \cdot 69} \equiv 553$ ✓

$2^{8 \cdot 69} \equiv 1 \not\equiv -1$ ✓

→ 2 is A MR Witness for 1105

(b) $n = 1031$

$1031 - 1 = 1030 = 2^1 \cdot 515,\ 5 \cdot 206,\ 10 \cdot 103$

$2^{515} \equiv 1 \equiv \pm 1$ ✗ $(\bmod 1031)$

$3^{515} \equiv -1 \equiv -1$

$5^{515} \equiv -1 \equiv -1$

$7^{515} \equiv -1 \equiv -1$

2, 3, 5, 7 NOT MR WITNESS FOR 1031

(c) $n = 294409$

$294408 = 2^3 \cdot 36801$

$2^{36801} \equiv 512 \not\equiv \pm 1$ ✓ $\pmod{294409}$

$2^{2 \cdot 36801} \equiv 262144$ ✓

$2^{4 \cdot 36801} \equiv 1 \not\equiv -1$ ✓

$2^{8 \cdot 36801} \equiv 1 \not\equiv -1$ ✓

2 IS A MR WITNESS FOR 294409

6. (a) 9

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67,
71, 73, 79, 83, 89, 97 → Tot = 25

(b) $\pi(23) = 9$

(c) $\pi(100) = 25$

7. $\pi(10^6) = \dfrac{10^6}{\ln(10^6)} = 72382$