Evan Colon
2021A967

Assignment 3

1) $17^{-1} \bmod 101$

$101 = 17 \cdot 5 + 16$
$17 = 16 \cdot 1 + 1$

$17^{-1} \equiv 6 \bmod 101$

$1 = 17 - 16 \cdot 1$
$1 = 17 - (101 - 17 \cdot 5) \cdot 1$
$= 17 \cdot 6 - 101$
$\equiv$

b) $357^{-1} \bmod 1234$

$1234 = 357 \cdot 3 + 163$
$357 = 163 \cdot 2 + 31$
$163 = 31 \cdot 5 + 8$
$31 = 8 \cdot 3 + 7$
$8 = 7 \cdot 1 + 1$

$1 = 8 - 7 \cdot 1$
$= 8 - (31 - 8 \cdot 3) = 8 \cdot 4 - 31$
$= (163 - 31 \cdot 5) \cdot 4 - 31 = 163 \cdot 4 - 31 \cdot 21$
$= 163 \cdot 4 - 21(357 - 2 \cdot 163)$
$= 163 \cdot 46 - 21 \cdot 357$
$= 46(1234 - 357 \cdot 3) - 21 \cdot 357$
$= 46 \cdot 1234 - 159 \cdot 357$

$1234 - 159 = 1075$

$357^{-1} \equiv 1075 \bmod 1234$

2) GCD (57, 93)

$93 = 57 \cdot 1 + 36$
$57 = 36 \cdot 1 + 21$
$36 = 21 \cdot 1 + 15$
$21 = 15 \cdot 1 + 6$
$15 = 6 \cdot 2 + 3 \rightarrow$ GCD (57, 93) = 3
$6 = 3 \cdot 2 + 0$

$3 = 15 - 2 \cdot 6 = 15 - 2(21 - 15) = 15 \cdot 3 - 2 \cdot 21$
$= 3 \cdot (36 - 21) - 2 \cdot 21 = 3 \cdot 36 - 5 \cdot 21$
$= 3 \cdot 36 - 5(57 - 36) = 8 \cdot 36 - 5 \cdot 57$
$= 8 \cdot (93 - 57) - 5 \cdot 57 = 8 \cdot 93 - 13 \cdot 57$

$\therefore s = -13$ and $t = 8$

3) $\phi 41 = 41 - 1 = 40$

$\phi 27$

$27 = 3^3$

$\phi = 27 \times (1 - \frac{1}{3}) = 2(\frac{27}{3}) = 18$

$\phi 440$

$440 = 2^3 \times 5 \times 11$

$\phi 440 = 440 \times (\frac{1}{2}) \times (\frac{4}{5}) \times (\frac{10}{11})$

$= 160$

2) $q = 71$, $g = 7$, $Y_B = 3$, $k = 2$ $M = 30$

$C_1 = g^k \bmod q = 49 \bmod 71 = 49$

$C_2 = (30 \cdot 3^2) \bmod 71 = 270 \bmod 71 = 57$

The ciphertext is (49, 57)

b) $C = (59, C2)$ $M = 30$

$C_2 = (M \cdot Y_B{}^k) \bmod q$

$C_2 = (30 \cdot 3^k) \bmod 71$ $7^{11} \bmod 71 = 59$

$k = 31$

$C_2 = (30 \cdot 3^{31}) \bmod 71$

$C_2 = 810 \bmod 71 = 24$

$C = (59, 29)$

$x_1 = -3 \quad y_1 = 9$
$x_2 = -2 \quad y_2 = 8$

3) $(P+Q)$

$\lambda = \frac{y_2 - y_1}{x - x_1} = \frac{8-9}{-2+3} = -1$

$x_3 = \lambda^2 - (-3) - (-2) = 6 \qquad P+Q = (6, -18)$
$y_3 = \lambda(-3 - 6) - 9 = -18$

$\frac{2P}{\lambda} = \frac{3(-3)^2}{2 \cdot 4} = \frac{3}{2}$

$x_3 = (\frac{3}{2})^2 - 2(-3) = \frac{9}{4} + 6 = \frac{33}{4}$

$y_3 = \frac{3}{2}(-\frac{12}{4} - \frac{33}{4}) - 9$

$= \frac{3(-45)}{2 \cdot 4} - 9 = -\frac{135}{8} - \frac{72}{8} = \frac{207}{8} = -24$

$2P = (\frac{33}{4}, \frac{207}{8})$

4) $Z_{23}: y^2 = x^3 + x + 1 \bmod 23$ at $P = (3, 10)$

$(P+Q): x_3 = \lambda^2 - x_1 - x_2$

Previous P $\quad y_3 = \lambda(x_1 - x_3) - y_1$

$P = (3,10) \quad 2P = (7,12) \quad 3P = (19,5) \quad 4P = (17,3) \quad 5P = (9,16) \quad 6P = (12,4)$
$7P = (11,3) \quad 8P = (13,16) \quad 9P = (0,1) \quad 10P = (6,4) \quad 11P = (18,20) \quad 12P = (5,4)$
$13P = (1,7) \quad 14P = (4,0) \quad 15P = (1,8) \quad 16P = (5,19) \quad 17P = (18,3) \quad 18P = (6,19)$
$19P = (0,22) \quad 20P = (13,7) \quad 21P = (11,20) \quad 22P = (12,19) \quad 23P = (9,7) \quad 24P = (17,20)$
$25P = (19,18) \quad 26P = (3,11) \quad 27P = (3,13)$

5a) $x_p = y^{d_p} \bmod p$ $\quad x_q = y^{d_q} \bmod q$ $\quad n = pq$

and $d_p = d \bmod (p-1)$ $\quad d_q = d \bmod (q-1)$

As per euler theorm, $a^{\phi n} \equiv 1 \bmod n$ for $p, q \phi p = p-1$
using that logic:

$$y^d \equiv y^{d \bmod (p-1)} \bmod p$$

$$y^d \equiv y^{d \bmod (q-1)} \bmod q$$

As p and q not be coprime,
We then have the following congruences:

$M_p \equiv 1 \bmod p$
$M_p \equiv 0 \bmod q$
and
$M_q \equiv 0 \bmod p$
$M_q \equiv 1 \bmod q$

To find x that satisfies
$x = (m_{pq} \cdot x_p + m_q \cdot x_q) \bmod n$

Our result is $y^d \bmod n$ proving
that Algorithm 1 returns the same value
as X

6) $p = 1511 \quad q = 2003 \quad d = 1234577$

$d_p = d \bmod (p-1)$
$= 1234577 \bmod (1510)$
$d_p = 907$

$d_q = d \bmod (q-1)$
$= 1234577 \bmod (2002)$
$d_q = 1345$

$M_p = q^{-1} \bmod p$
$= 2003^{-1} \bmod 1511$

$1511 - 734 = 777$

$M_p = 777$

$2003 = 1511 \cdot 1 + 492$
$1511 = 492 \cdot 3 + 35$
$492 = 35 \cdot 14 + 2$
$35 = 2 \cdot 17 + 1$

$1 = 35 - 2 \cdot 17 = 35 - (492 - 35 \cdot 14) \cdot 17$
$= 35 \cdot 239 - 492 \cdot 17 = (1511 - 492 \cdot 3) \cdot 239 - 492 \cdot 17$
$= 1511 \cdot 239 - 492 \cdot 734 =$
$= 1511 \cdot 239 - (2003 - 1511) \cdot 734$
$\Rightarrow -2003 \cdot 734$

$M_q = 1511^{-1} \bmod 2003$ From previous q → $1511 \cdot 973 \equiv$

$\therefore M_q = 973$

c) $y = 152702$

$X_p = 152702^{977} \bmod 1511 = 242$ $n = 2003 \cdot 1511 = 3,026,533$

$X_q = 152702^{1345} \bmod 2003 = 1087$

$X = (777 \cdot 2003 \cdot 242 + 973 \cdot 1511 \cdot 1087) \bmod 3026533$
$= 1443247$

6) $h(x) = xA = y$
find $X: (x_1, x_2, x_3, x_4, x_5, x_6, x_7)$

$$\begin{pmatrix} x_1 + x_2 + x_3 + x_4 \\ x_2 + x_3 + x_4 + x_5 \\ x_3 + x_4 + x_5 + x_6 \\ x_4 + x_5 + x_6 + x_7 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}$$

Preimages: $(0,0,0,0,1,1,0)$
$(1,1,0,0,0,0,1)$
$(1,0,1,0,0,1,0)$
$(1,0,0,1,0,1,0)$
$(0,1,1,0,1,0,0)$
$(0,1,0,1,1,0,1)$
$(0,0,1,1,1,0,1)$
$(1,1,1,1,0,0,0)$