Robert (Robbie) Knowles MATH 135 Fall 2020: WA10

Q01A To start we know that $1147 = 31 \cdot 37$, we also thus know that $(p-1)(q-1) = 30 \cdot 36 = 1080$. To find d we need to solve:

$$47d \equiv 1 \pmod{1080}$$

Setting up the LDE we get:

$$1080x + 47d = 1$$

Solving using EEA we get that:

x	d	r	q
1	0	1080	0
0	1	47	0
1	-22	46	22
-1	23	1	1
47	-1080	0	46

Hence we get that our solution for d is 23, which satisfies $1 < 23 < 1080$. The private key will thus be of the form:

$$(23, 1147)$$

Q01B We know the the cipher text will be of the form:

$$C_1 \equiv M_1^e \text{ (mod n)}$$
$$C_1 \equiv 2^{47} \pmod{1147}$$
$$C_1 \equiv 2^{45} \cdot 2^2 \pmod{1147}$$
$$C_1 \equiv (2^{15})^3 \cdot 2^2 \pmod{1147}$$

We know that $2^{15} = 32768$, which is equivalent to $652 \pmod{1147}$. This means our equation becomes:

$$C_1 \equiv (652)^3 \cdot 2^2 \pmod{1147}$$
$$C_1 \equiv (277167808)(4) \pmod{1147}$$
$$C_1 \equiv (993)(4) \pmod{1147}$$
$$C_1 \equiv (3972) \pmod{1147}$$
$$C_1 \equiv 531 \pmod{1147}$$

Since $0 \leq 531 < 1147$, 531 is our cipher text C_1.

Q01C We know the the plain text will be of the form:

$$\begin{aligned}
M_2 &\equiv C_2^d \text{ (mod n)}\\
M_2 &\equiv 3^{23} \pmod{1147}\\
M_2 &\equiv 3^{22} \cdot 3 \pmod{1147}\\
M_2 &\equiv (3^{11})^2 \cdot 3 \pmod{1147}
\end{aligned}$$

We know that $3^{11} = 177147$, which is equivalent to 509 (mod 1147). This means our equation becomes:

$$\begin{aligned}
M_2 &\equiv (509)^2 \cdot 3 \pmod{1147}\\
M_2 &\equiv (259081)3 \pmod{1147}\\
M_2 &\equiv (1006)(3) \pmod{1147}\\
M_2 &\equiv (3018) \pmod{1147}\\
M_2 &\equiv 724 \pmod{1147}
\end{aligned}$$

Since $0 \leq 724 < 1147$, 724 is our plain text text M_2.