Student Number: [redacted] Name: Bryan Hoang

2. (10 points)

(a) **Answer:**

To decrypt the first ciphertext block $c = 1794677960$, we compute

$$\begin{aligned}
\left(\frac{1794677960}{32411}\right) &= \left(\frac{16068}{32411}\right) \\
&= \left(\frac{2}{32411}\right)^2 \left(\frac{4017}{32411}\right) \\
&= \left(\frac{4017}{32411}\right) \\
&= \left(\frac{32411}{4017}\right) \\
&= \left(\frac{275}{4017}\right) \\
&= \left(\frac{167}{275}\right) \\
&= -\left(\frac{275}{167}\right) \\
&= -\left(\frac{108}{167}\right) \\
&= -\left(\frac{2}{167}\right)^2 \left(\frac{27}{167}\right) \\
&= \left(\frac{167}{27}\right) \\
&= \left(\frac{5}{27}\right) \\
&= \left(\frac{27}{5}\right) \\
&= \left(\frac{2}{5}\right) \\
&= -1,
\end{aligned}$$

which gives the plaintext bit $m = 1$.

Student Number: [redacted] Name: Bryan Hoang

To decrypt the second ciphertext block $c = 525734818$, we compute

$$\begin{aligned}
\left(\frac{525734818}{32411}\right) &= \left(\frac{28398}{32411}\right) \\
&= \left(\frac{2}{32411}\right)\left(\frac{3}{32411}\right)\left(\frac{4733}{32411}\right) \\
&= \left(\frac{32411}{3}\right)\left(\frac{32411}{4733}\right) \\
&= \left(\frac{2}{3}\right)\left(\frac{4013}{4733}\right) \\
&= -\left(\frac{4733}{4013}\right) \\
&= -\left(\frac{720}{4013}\right) \\
&= -\left(\frac{2}{4013}\right)^4\left(\frac{2}{4013}\right)^2\left(\frac{5}{4013}\right) \\
&= -\left(\frac{4013}{5}\right) \\
&= -\left(\frac{3}{5}\right) \\
&= -\left(\frac{5}{3}\right) \\
&= -\left(\frac{2}{3}\right) \\
&= 1,
\end{aligned}$$

which gives the plaintext bit $m = 0$.

Student Number: [redacted] Name: Bryan Hoang

To decrypt the third ciphertext block $c = 420526487$, we compute

$$\begin{aligned}\left(\frac{420526487}{32411}\right) &= \left(\frac{26173}{32411}\right)\\ &= \left(\frac{7}{32411}\right)\left(\frac{3739}{32411}\right)\\ &= \left(\frac{32411}{7}\right)\left(\frac{32411}{3739}\right)\\ &= \left(\frac{1}{7}\right)\left(\frac{2499}{3739}\right)\\ &= \left(\frac{3}{3739}\right)\left(\frac{7}{3739}\right)^2\left(\frac{17}{3739}\right)\\ &= -\left(\frac{3739}{3}\right)\left(\frac{3739}{17}\right)\\ &= -\left(\frac{1}{3}\right)\left(\frac{16}{17}\right)\\ &= -\left(\frac{2}{17}\right)^4\\ &= -1,\end{aligned}$$

which gives the plaintext bit $m = 1$.

Therefore, Alice's plaintext message is $\boxed{(1, 0, 1)}$.

(b) **Answer:**

The factorization of N is $N = pq = 47 \cdot 67$.

To decrypt the first ciphertext block $c = 2322$, we compute

$$\begin{aligned}\left(\frac{2322}{47}\right) &= \left(\frac{19}{47}\right)\\ &= -\left(\frac{47}{19}\right)\\ &= -\left(\frac{9}{19}\right)\\ &= -\left(\frac{3}{19}\right)^2\\ &= -1\end{aligned}$$

which gives the plaintext bit $m = 1$.

Student Number: [redacted] Name: Bryan Hoang

To decrypt the second ciphertext block $c = 719$, we compute

$$\begin{aligned}\left(\frac{719}{47}\right) &= \left(\frac{14}{47}\right)\\ &= \left(\frac{2}{47}\right)\left(\frac{7}{47}\right)\\ &= -\left(\frac{47}{7}\right)\\ &= -\left(\frac{5}{7}\right)\\ &= -\left(\frac{7}{5}\right)\\ &= -\left(\frac{2}{5}\right)\\ &= 1\end{aligned}$$

which gives the plaintext bit $m = 0$.
To decrypt the third ciphertext block $c = 202$, we compute

$$\begin{aligned}\left(\frac{202}{47}\right) &= \left(\frac{14}{47}\right)\\ &= \left(\frac{2}{47}\right)\left(\frac{7}{47}\right)\\ &= -\left(\frac{47}{7}\right)\\ &= -\left(\frac{5}{7}\right)\\ &= -\left(\frac{7}{5}\right)\\ &= -\left(\frac{2}{5}\right)\\ &= 1\end{aligned}$$

which gives the plaintext bit $m = 0$.
Therefore, Alice's plaintext message is $\boxed{(1, 0, 0)}$.

(c) **Answer:**
To encrypt the first message bit $m = 1$ using $r = 705130839$, we compute

$$\begin{aligned}c &\equiv ar^2 \pmod{781044643}\\ &\equiv 568980706 \cdot 705130839^2 \pmod{781044643}\\ &\equiv 517254876 \pmod{781044643}.\end{aligned}$$

To encrypt the second message bit $m = 1$ using $r = 631364468$, we compute

$$\begin{aligned}c &\equiv ar^2 \pmod{781044643}\\ &\equiv 568980706 \cdot 631364468^2 \pmod{781044643}\\ &\equiv 4308279 \pmod{781044643}\end{aligned}$$

Student Number: [redacted] Name: Bryan Hoang

To encrypt the third message bit $m = 0$ using $r = 67651321$, we compute

$$\begin{aligned} c &\equiv ar^2 \pmod{781044643} \\ &\equiv 568980706 \cdot 67651321^2 \pmod{781044643} \\ &\equiv 660699010 \pmod{781044643} \end{aligned}$$

Therefore, the ciphertext for $(1, 1, 0)$ is $\boxed{(517254876, 4308279, 660699010)}$.