Student Number: [redacted] Name: Bryan Hoang

10. (10 points)

(a) **Answer:**
$n - 1 = 1104 = 2^4 \cdot 69$.

$$\begin{aligned} 2^{69} &\equiv -138 \pmod{1105} \\ 2^{69 \cdot 2} &\equiv 259 \pmod{1105} \\ 2^{69 \cdot 4} &\equiv -324 \pmod{1105} \\ 2^{69 \cdot 8} &\equiv 1 \pmod{1105} \end{aligned}$$

Thus, 2 is a Miller-Rabin witness for the compositeness of 1105, implying that 1105 is a composite number.

(b) **Answer:**
$n - 1 = 294408 = 2^3 \cdot 36801$.

$$\begin{aligned} 2^{36801} &\equiv 512 \pmod{294409} \\ 2^{36801 \cdot 2} &\equiv -32265 \pmod{294409} \\ 2^{36801 \cdot 4} &\equiv 1 \pmod{294409} \end{aligned}$$

Thus, 2 is a Miller-Rabin witness for the compositeness of 294409 , implying that 294409 is a composite number.

(c) **Answer:**
$n - 1 = 294438 = 2^1 \cdot 147219$.

$$2^{147219} \equiv 1 \pmod{294439}$$

Thus 2 is not a Miller-Rabin witness for 29443. Nine other numbers that are not Miller-Rabin witnesses of 29443 are: 3, 4, 5, 6, 7, 8, 9, 10, 11. Therefore, 294409 is probably prime.

(d) **Answer:**
$n - 1 = 118901508 = 2^2 \cdot 29725377$.

$$\begin{aligned} 2^{29725377} &\equiv 7906806 \pmod{118901508} \\ 2^{29725377 \cdot 2} &\equiv -1 \pmod{118901508} \end{aligned}$$

Thus 2 is not a Miller-Rabin witness for 118901509. Nine other numbers that are not Miller-Rabin witnesses of 118901509 are: 3, 4, 5, 6, 7, 8, 9, 10, 11. Therefore, 118901509 is probably prime.

(e) **Answer:**
$n - 1 = 118901520 = 2^4 \cdot 7431345$.

$$\begin{aligned} 2^{7431345} &\equiv 45274074 \pmod{118901521} \\ 2^{7431345 \cdot 2} &\equiv 1758249 \pmod{118901521} \\ 2^{7431345 \cdot 8} &\equiv 1 \pmod{118901521} \\ 2^{7431345 \cdot 4} &\equiv 1 \pmod{118901521} \end{aligned}$$

Thus, 2 is a Miller-Rabin witness for the compositeness of 118901521, implying that 118901521 is a composite number.

Student Number: [redacted] Name: Bryan Hoang

(f) **Answer:**
$n - 1 = 118901526 = 2^1 \cdot 59450763$.

$$2^{59450763} \equiv 1 \pmod{118901527}$$

Thus 2 is not a Miller-Rabin witness for 118901527. Nine other numbers that are not Miller-Rabin witnesses of 118901527 are: 3, 4, 5, 6, 7, 8, 9, 10, 11. Therefore, 118901527 is probably prime.

(g) **Answer:**
$n - 1 = 118915386 = 2^1 \cdot 59457693$.

$$2^{59457693} \equiv -5081012 \pmod{118915387}$$

Thus, 2 is a Miller-Rabin witness for the compositeness of 118915387, implying that 118915387 is a composite number.