NAME: SID:

Problem 1: In the RSA, suppose that Bob chooses $p = 7$ and $q = 13$. (a) Which of the numbers 13, 25, 27 are correct choices for e? Give a brief justification (at most 10 words for each).

We have $n = 7 \cdot 13 = 91$ and $\phi(91) = 6 \cdot 12 = 72$. So 13 and 25 are correct because they are relatively prime with $\phi(91)$, while 27 is not correct because it is not relatively prime to $\phi(91)$.

(b) Compute the secret exponent d for $e = 7$. Show your work.
$7 \cdot d \equiv 1 \pmod{72}$. We list numbers that are multiples of 7 and $72b + 1$:
$7, 14, ..., 217$
73, 145, 217.
Since $217 = 7 \cdot 31$, we have $d = 31$.

(c) Next, use the public exponent $e = 7$ to encrypt $M = 3$. Show your work.

Computing modulo 91, we get $C = 3^7 = 3 \pmod{91}$.
Part 2. Let b and n be two positive integers, such that $\gcd(b, n) = 1$ and $b^{n-1} \equiv 1 \pmod{n}$. Is n prime or composite? It may be either prime or composite.

Problem 2: Solve the recurrence $Q_n = 2Q_{n-1} + 8Q_{n-2}$, with initial conditions $Q_0 = 0$, $Q_1 = 2$.

(a) Characteristic polynomial and its roots: $x^2 - 2x - 8 = 0$. The roots are $r_1 = -2$, $r_2 = 4$.

(b) General form of the solution: $Q_n = \alpha_1 \cdot (-2)^n + \alpha_2 \cdot 4^n$.

(c) Initial condition equations and their solution:

$$\begin{aligned} \alpha_1 + \alpha_2 &= 0 \\ -2\alpha_1 + 4\alpha_2 &= 2 \end{aligned}$$

So $\alpha_1 = -\frac{1}{3}$, $\alpha_2 = \frac{1}{3}$.

(d) Final answer: $Q_n = -\frac{1}{3} \cdot (-2)^n + \frac{1}{3} \cdot 4^n$.

Problem 3: We want to tile an $n \times 1$ strip with 1×1 tiles of the following colors: green, red, light-blue, dark-blue, and sky-blue. Let T_n be the number of such tilings, in which no blue tiles are next to each other. Derive a recurrence relation for the numbers T_n. Give a justification.
The recurrence is $T_n = 2T_{n-1} + 6T_{n-2}$ for $n \geq 2$, with initial conditions $T_0 = 1$, $T_1 = 5$.

NAME: SID:

Problem 4: In the RSA, suppose that Bob chooses $p = 5$ and $q = 19$. (a) Which of the numbers 19, 25, 27 are correct choices for e? Give a brief justification (at most 10 words for each).

We have $n = 5 \cdot 19 = 95$ and $\phi(95) = 4 \cdot 18 = 72$. So 13 and 25 are correct because they are relatively prime with $\phi(91)$, while 27 is not correct because it is not relatively prime to $\phi(91)$.

(b) Compute the secret exponent d for $e = 11$. Show your work. $7 \cdot d \equiv 1 \pmod{72}$. We list numbers that are multiples of 11 and $72b + 1$:
$11, 22, ..., 649$
$73, 145, 217, 649$.
We list numbers that are multiples of 72 plus 1: 73, 145, 289, 361, 433, 505, 577, 649. Since $649 = 11 \cdot 59$, we have $d = 59$.
(c) Next, use the public exponent $e = 11$ to encrypt $M = 2$. Show your work.

Computing modulo 95, we get $C = 2^7 = 33 \pmod{95}$.
Part 2. Let k and a be two positive integers, such that $a^{k-1} \equiv 1 \pmod{k}$ and $\gcd(k, a) = 1$. Is k prime or composite? It may be either prime or composite.

Problem 5: Solve the recurrence $R_n = 3R_{n-1} + 10R_{n-2}$, with initial conditions $R_0 = 0$, $R_1 = 2$.

(a) Characteristic polynomial and its roots: $x^2 - 3x - 10 = 0$. The roots are $r_1 = -2$, $r_2 = 5$.

(b) General form of the solution: $\alpha_1 \cdot (-2)^n + \alpha_2 \cdot 5^n$.

(c) Initial condition equations and their solution:

$$\begin{aligned} \alpha_1 + \alpha_2 &= 0 \\ -2\alpha_1 + 5\alpha_2 &= 2 \end{aligned}$$

So $\alpha_1 = -\frac{2}{7}$, $\alpha_2 = \frac{2}{7}$.

(d) Final answer: $R_n = -\frac{2}{7} \cdot (-2)^n + \frac{2}{7} \cdot 7^n$.

Problem 6: We want to tile an $n \times 1$ strip with 1×1 tiles of the following colors: orange, yellow, light-green, dark-green, and red. Let A_n be the number of such tilings, in which no green tiles are next to each other. Derive a recurrence relation for the numbers A_n. Give a justification.
The recurrence is $A_n = 2A_{n-1} + 6A_{n-2}$ for $n \geq 2$, with initial conditions $A_0 = 1$, $A_1 = 5$.