NAME: SID:

Problem 1: Below you are given five choices of parameters p, q, e, d of RSA. For each choice tell whether these parameters are correct[1] (write YES/NO). If the parameters are correct, compute the encryption of $M = 3$. If the parameters are incorrect, give a brief explanation why (at most 10 words).

p	q	e	d	correct?	Encrypt $M = 3$ if correct. Justify if not correct.
5	21	7	23	NO	21 is not prime.
13	7	5	29	YES	Here $n = 91$. So $C = 3^5 = 61 \pmod{91}$.
11	11	9	89	NO	p and q cannot be equal.
7	17	11	37	NO	We have $\phi(n) = 96$, but $11 \cdot 37 = 407 = 23 \neq 1 \pmod{96}$.
3	7	5	5	YES	Here $n = 21$. So $C = 3^5 = 12 \pmod{21}$.

[1]To clarify, correctness refers only to mathematical correctness, namely whether the parameters satisfy the assumptions from the algorithm.

Problem 2: Solve the recurrence equation $Q_n = 2Q_{n-1} + 4Q_{n-2}$, for $Q_0 = 0$, $Q_1 = 2$. Follow the steps below.

(a) Characteristic polynomial and its roots:

$$x^2 - 2x - 4 = 0$$

The roots are $r_1 = 1 + \sqrt{5}$ and $r_2 = 1 - \sqrt{5}$.

(b) General solution:

$$Q_n = \alpha_1 \cdot \left(1 + \sqrt{5}\right)^n + \alpha_2 \cdot \left(1 - \sqrt{5}\right)^n$$

(c) Equations for initial conditions and its solution:

$$\alpha_1 + \alpha_2 = 0$$
$$\alpha_1(1 + \sqrt{5}) + \alpha_2(1 - \sqrt{5}) = 2$$

So $\alpha_1 = \frac{1}{\sqrt{5}}$ and $\alpha_2 = -\frac{1}{\sqrt{5}}$.

(d) Final answer:

$$Q_n = \frac{1}{\sqrt{5}} \cdot \left(1 + \sqrt{5}\right)^n - \frac{1}{\sqrt{5}} \cdot \left(1 - \sqrt{5}\right)^n$$