NAME: SID:

Problem 1: In the RSA, suppose that Bob chooses $p = 3$ and $q = 43$. (a) Determine three correct values of the public exponent e. Justify briefly their correctness (at most 20 words.)

Solution: $\phi(n) = (p-1) \cdot (q-1) = 2 \times 42 = 2^2 \cdot 3 \cdot 7$

We know that e should be relatively prime to $\phi(n)$, i.e., $gcd(e, \phi(n))$ should be 1. Numbers 5, 11 and 13 satisfy this condition and hence are possible values of e.

(b) For one of the e's you selected, compute the corresponding secret exponent d. Show your work.

Solution: The secret key, $d = e^{-1} \pmod{\phi(n)}$. For $e = 5$, $d = 5^{-1} \pmod{84} = 17$ (since $17 \times 5 = 85 \equiv 1 \pmod{84}$).

Problem 2: Solve the recurrence $S_n = 7S_{n-1} - 10S_{n-2}$, with initial conditions $S_0 = 1$, $S_1 = 2$.

(a) Characteristic polynomial and its roots:

$x^2 - 7x + 10 = 0$
or, $(x - 2)(x - 5) = 0$

So, the roots are 2 and 5.

(b) General form of the solution:

$S_n = c_1 \cdot 2^n + c_2 \cdot 5^n$

(c) Initial condition equations and their solution:

$S_0 = 1 : c_1 + c_2 = 1$
$S_1 = 2 : 2 \cdot c_1 + 5 \cdot c_2 = 2$

We solve these two equations to get, $c_1 = 1$ and $c_2 = 0$

(d) Final answer:

Plugging in values of c_1 and c_2 into the general form of the solution gives:

$S_n = 2^n$