NAME: SID:

Problem 1: In the RSA, suppose that Bob chooses two primes $p = 5$ and $q = 17$.

(a) Determine the values of n and $\phi(n)$:

$$n = \boxed{85} \qquad \phi(n) = \boxed{64}$$

(b) Below you are given a list of pairs e, d of private and secret exponents. For each pair determine whether this pair is correct or not. In the last row of each column write "Y" for correct and "N" for incorrect, and leave the entry empty for no answer. (Negative credit may be given for incorrect answers.) Show your work.

e	7	5	31
d	55	37	31
correct?	Y	N	Y

Explanation:
$7 \cdot 55 \equiv 1 \pmod{64}$
$5 \cdot 37 \not\equiv 1 \pmod{64}$
$31 \cdot 31 \equiv 1 \pmod{64}$

(c) Assume that Bob chooses exponents $e = 35$ and $d = 11$. Bob receives encrypted message $C = 3$. Determine the original plaintext message M (that is, decrypt C). Show your work.

$$M = \boxed{7}$$

Calculations: computing modulo 85:

$$\begin{aligned} 3^{11} &= 3 \cdot 9^5 \\ &= 3 \cdot 9 \cdot 9^4 = 27 \cdot 81^2 \\ &= 27 \cdot (-4)^2 = 27 \cdot 16 = 432 = 7. \end{aligned}$$

Problem 2: Let U_n be the number of letters printed by the procedure PrintUs(), if the input is an integer $n \geq 0$. Give a recurrence equation for U_n and solve it. Follow the instructions below.

```
**procedure** PrintUs($n$)
    **if** $n = 0$ **or** $n = 1$ **then**
        print("U")
    **else**
        PrintUs($n - 1$)
        **for** $k = 1$ **to** 6 **do** PrintUs($n-2$)
```

(a) Recurrence equation.

$$U_n = U_{n-1} + 6U_{n-2}$$
$$U_0 = 1$$
$$U_1 = 1$$

(b) Justification (at most 40 words).

The program makes one recursive call with argument $n - 1$ and six recursive calls with argument $n - 2$.

(c) Characteristic equation and its solution.

$$x^2 - x - 6 = 0$$
$$\text{roots:} \quad r_1 = 3 \quad r_2 = -2$$

(d) General solution.

$$U_n = \alpha_1 3^n + \alpha_2 (-2)^n$$

(e) Equations for the initial conditions.

$$\begin{cases} \alpha_1 + \alpha_2 & = 1 \\ 3\alpha_1 - 2\alpha_2 & = 1 \end{cases}$$

So $\alpha_1 = \frac{3}{5}$ and $\alpha_2 = \frac{2}{5}$.
(f) Final solution.

$$U_n = \tfrac{3}{5} \cdot 3^n + \tfrac{2}{5} \cdot (-2)^n$$