NAME: SID:

Problem 1: In the RSA, suppose that Bob chooses two primes $p = 7$ and $q = 11$.

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

$$n = \boxed{77} \qquad \phi(n) = \boxed{60}$$

(b) Below you are given three 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	11	7	19
d	27	43	19
correct?	N	Y	Y

Explanation:
$11 \cdot 27 \not\equiv 1 \pmod{60}$
$7 \cdot 43 \equiv 1 \pmod{60}$
$19 \cdot 19 \equiv 1 \pmod{60}$

(c) Assume that Bob chooses exponents $e = 37$ and $d = 13$. Bob receives encrypted message $C = 3$. Determine the original plaintext message M (that is, decrypt C). Show your work.

$$M = \boxed{38}$$

Calculations: computing modulo 77:

$$\begin{aligned} 3^{13} &= 3 \cdot 9^6 = 3 \cdot 81^3 \\ &= 3 \cdot 4^3 = 3 \cdot 64 \\ &= 3 \cdot (-13) = -39 = 38 \end{aligned}$$

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

```
procedure PrintVs($n$)
    if $n = 0$ or $n = 1$ then
        print(”V”)
    else
        PrintVs($n - 1$)
        PrintVs($n - 1$)
        for $k = 1$ to 8 do PrintVs($n - 2$)
```

(a) Recurrence equation.

$$
\begin{aligned}
&V_n = 2V_{n-1} + 8V_{n-2}\\
&V_0 = 1\\
&V_1 = 1
\end{aligned}
$$

(b) Justification (at most 40 words).

The program makes two recursive calls with argument $n - 1$ and eight recursive calls with argument $n - 2$.

(c) Characteristic equation and its solution.

$$
\begin{aligned}
&x^2 - 2x - 8 = 0\\
&\text{roots:} \quad r_1 = 4 \quad r_2 = -2
\end{aligned}
$$

(d) General solution.

$$V_n = \alpha_1 4^n + \alpha_2 (-2)^n$$

(e) Equations for the initial conditions.

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

So $\alpha_1 = \frac{1}{2}$ and $\alpha_2 = \frac{1}{2}$.
(f) Final solution.

$$U_n = \tfrac{1}{2} \cdot 4^n + \tfrac{1}{2} \cdot (-2)^n$$