Quiz 1 Solutions (version A)

Solution 1: In the table below you have two columns, each with a choice for p, q, the prime-number parameters in the RSA. For each column, determine the public and secret keys, and compute the encryption of $M = 5$.

Note: In both cases, you *must* use the smallest correct value of the public exponent e.

p and q	$p = 5$, $q = 19$	$p = 3$, $q = 23$
$n =$	$n = 5 \cdot 19 = 95$	$n = 3 \cdot 23 = 69$
$\phi(n) =$	$\phi(n) = 4 \cdot 18 = 72$	$\phi(n) = 2 \cdot 22 = 44$
$e =$	5	3
$d =$	$d = 5^{-1} \pmod{72} = 29$	$d = 3^{-1} \pmod{44} = 15$
public key $=$	$P = (95, 5)$	$P = (69, 3)$
secret key $=$	$S = 29$	$S = 15$
encrypt $M = 5$	$E(5) = 5^5 \operatorname{rem} 95 = 85$	$E(5) = 5^3 \operatorname{rem} 69 = 56$

Solution 2: Solve the recurrence equation $A_n = A_{n-1} + 3A_{n-2}$, for $A_0 = 0$, $A_1 = 13$. Follow the steps below.

(a) Characteristic polynomial and its roots: $x^2 - x - 3 = 0$

$r_1 = \frac{1}{2}(1 + \sqrt{13})$, $r_2 = \frac{1}{2}(1 - \sqrt{13})$

(b) General solution: $A_n = \alpha_1(\frac{1+\sqrt{13}}{2})^n + \alpha_2(\frac{1-\sqrt{13}}{2})^n$

(c) Equations for initial conditions and its solution:

$$\alpha_1 + \alpha_2 = 0$$
$$\alpha_1 \tfrac{1+\sqrt{13}}{2} + \alpha_2 \tfrac{1-\sqrt{13}}{2} = 13$$

$\alpha_1 = \sqrt{13}$, $\alpha_2 = -\sqrt{13}$

(d) Final answer: $A_n = \sqrt{13}\left[(\frac{1+\sqrt{13}}{2})^n - (\frac{1-\sqrt{13}}{2})^n\right]$
