CS111 Practice Quiz 2 (version 2)

Problem 1: Compute the values described below, following the instructions. You need to show all your work (write the solutions step-by-step) in order to receive credit.

(a) Compute $5^{-1} \pmod{16}$ using the method of listing multiples.

(b) Compute $3^{-1} \pmod{23}$ using Fermat's theorem and squaring.

(c) Compute $5^{160322} \operatorname{rem} 17$ using Fermat's theorem.

(d) Solve the following linear congruence equation: $7x + 3 \equiv 2x - 4 \pmod{16}$. (You are allowed to use some solutions of the above problems without recomputing.)

Problem 2: Bob chose his RSA primes to be $p = 7$, $q = 23$.

(a) Are the values of p, q chosen correctly? Justify your answer.

(b) Give the values of n and $\phi(n)$.

(c) Bob wants to choose e between 10 and 15, inclusive. Which of the values from this interval are correct? Give a complete justification for your answer.

(d) Bob eventually chooses $e = 5$ and $d = 53$. Is this choice correct? Justify your answer.

(e) Using the RSA values in parts (b) and (d), encrypt $M = 4$. Show your work.