1. The RSA Is Watching You

Alice wants to use RSA encryption to allow other people to send her messages. She picks $251,257$ as her two large primes p, q and 15251 as her encryption key e.

(a) Find Alice's secret key d.

Solution:

(b) Suppose that Bob wants to send Alice the message 2014. What should his cipher text be?

Solution:

(c) Suppose that Bob sends Alice the cipher text 16648. What is Bob's original message?

Solution:

2. Why So Blum?

(a) Suppose that p is prime, and that a is a modular residue of p. Prove that a is a quadratic residue mod p iff $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

Solution:

(b) Suppose n is a Blum integer. Prove that $n-1$ is a quadratic non-residue mod n.

Solution:

3. Regular Show

Let $\Sigma = \{0, 1\}$.

(a) Is $L = \{xyx^R | x, y \in \Sigma^*\}$ regular? Explain your reasoning.

Solution:

(b) Is $L = \{x1x^R | x \in \Sigma^*\}$ regular? Explain your reasoning.

Solution:

(c) Suppose that $L' = L_1 \cap L_2$, and that L', L_2 are both regular. Is L_1 regular? Explain your reasoning.

Solution:

(d) Suppose L_1, L_2 are both regular, and that $L' = \{xyz | (x \in L_1) \wedge (y \notin L_2) \wedge (z \in L_1) \wedge (z \in L_2)\}$. Is L' regular? Explain your reasoning.

Solution: