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:
$\phi(n) = \phi(p)\phi(q) = (251-1)(257-1) = 64000$. Using the Extended Euclidean Algorithm,

$$\begin{aligned}
64000 &= 15251 \cdot 4 + 2996 \\
15251 &= 2996 \cdot 5 + 271 \\
2996 &= 271 \cdot 11 + 15 \\
271 &= 15 \cdot 18 + 1 \\
15 &= 1 \cdot 15
\end{aligned}$$

The GCD is 1. Using back-substitution,

$$\begin{aligned}
1 &= 271 - 15 \cdot 18 \\
&= 271 - (2996 - 271 \cdot 11) \cdot 18 = 271 \cdot 199 - 2996 \cdot 18 \\
&= (15251 - 2996 \cdot 5) \cdot 199 - 2996 \cdot 18 = 15251 \cdot 199 - 2996 \cdot 1013 \\
&= 15251 \cdot 199 - (64000 - 15251 \cdot 4) \cdot 1013 = 15251 \cdot 4251 - 64000 \cdot 1013
\end{aligned}$$

Thus, $d = 4251$.

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

Solution:
Bob needs to send Alice the cipher text $2014^{15251} \pmod{64507} = 12305$.

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

Solution:
Bob's original message is $16648^{4251} \pmod{64507} = 1337$.

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:

Suppose that a is a quadratic residue mod p. Then there exists a modular residue x in p such that $x^2 \equiv a \pmod{p}$. This implies that $x^{p-1} \equiv a^{\frac{p-1}{2}} \pmod{p}$. By Fermat's little theorem, $x^{p-1} \equiv 1 \pmod{p}$, so $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

Suppose that $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Let b be a generator mod p. Then, for some integer k, $b^k = a$. This implies that $b^{\frac{k(p-1)}{2}} \equiv 1 \pmod{p}$.

As the order of b is $p-1$, $\frac{k}{2}$ must be an integer. Then, as $(b^{\frac{k}{2}})^2 \equiv a \pmod{p}$, a is a quadratic residue mod p.

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

Solution:

We can write $n = pq$ for some primes p, q such that $p, q \equiv 3 \pmod{4}$. As $\frac{p-1}{2}$ is either 1 or 3 mod 4, $(-1)^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. By the result from part a, -1 is a quadratic non-residue mod p.

AFSOC that $n-1$ is a quadratic residue mod n. Then there exists a modular residue x in p such that $x^2 \equiv n-1 \pmod{n}$. We can write $x^2 = ns + n - 1 = pqs + n - 1$ for some integer s.

This implies that $x^2 \equiv n - 1 \equiv -1 \pmod{p}$, but this is a contradiction, as we found that -1 is a quadratic non-residue mod p. Thus, $n-1$ is a quadratic non-residue mod p.

3. **Regular Show**

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

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

Solution:

L is regular. Any string $s \in \Sigma^*$ can be written as $\epsilon s \epsilon$, so $L = \Sigma^*$. The DFA that accepts L consists of one accepting state with all transitions from this state looping back to it.

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

Solution:

L is not regular.

AFSOC that L is regular. Then there exists a DFA that accepts all strings that are in L and rejects the ones that aren't. Let the number of states in this DFA be k.

Let string s_i be the string consisting of $k+2$ $0's$ concatenated with a 1 concatenated with i 0's, for all $i \in [k+1]$.

Feed these strings into the DFA. As there are only k states in the DFA, by the pigeonhole principle, there must exist two strings, s_a, s_b with $a \neq b$, that end up at the same state.

Let A be s_a concatenated with $k+2-a$ 0's, and B be s_b concatenated with $k+2-a$ 0's. Feed these strings into the DFA. As s_a, s_b ended up at the same state, A and B should also end up at the same state. But by the definition of L, A must end up at an accepting state, and B must end up at a rejecting state.

So, we have a contradiction, which means that L is not regular.

(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:

L_1 is not necessarily regular. Suppose L_1 is irregular and $L_2 = \{\epsilon\}$, which is regular. Then, $L' = L_1 \cap L_2 = \{\epsilon\}$, which is also regular.

(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:

L' is regular. Using the givens, and the fact that regular languages are closed under complement and intersection, L_2^c and $L_1 \cap L_2$ are regular. Then, as regular languages are closed under concatenation, L' must also be regular.