CSE 291I
Cryptography

May 6, 2020
Due: Friday, May 15, 2020

Homework 6

Your homework should be submitted electronically via Gradescope on the due date. Please type up your solutions to the following problems using Latex and submit as hw6-solutions.pdf, along with a Sage script called hw6-sol.py containing your code for the first part. Please credit any collaborators you worked with and any sources you used.

---

0. (a) Describe how you solved the decryption and any problems you ran into.
   (b) List some other poor security choices made by the PBP encryption.

1. This problem develops a simplified version of the Bleichenbacher attack. Consider an RSA public key (N, e) where N is an RSA modulus and e is an encryption exponent. For $x \in \mathbb{Z}_N$, consider the predicate $P_x : \mathbb{Z}_N \to \{0, 1\}$ defined as:

$$P_x(r) = \begin{cases} y \leftarrow x \cdot r \in \mathbb{Z}_N \\ \text{treat } y \text{ as an integer in the interval } [0, N) \\ \text{if } y > N/2, \text{ output 1} \\ \text{else output 0} \end{cases}$$

   (a) Show that by querying the predicate P_x at about $\log_2 N$ points, it is possible to learn the value of x.

   (b) Suppose an attacker obtains an RSA public key and an element $c \in \mathbb{Z}_N$. It wants to compute the eth root of c in $\mathbb{Z}_N$. To do so, the attacker can query an oracle that takes $z \in \mathbb{Z}$ as input, and outputs 1 when $[z^{1/e} \bmod N] > N/2$, and outputs 0 otherwise. Here $[z^{1/e} \bmod N]$ is an integer w in the interval $[0, N)$ such that $w^e \equiv z \bmod N$. Use part (a) to show how the adversary can recover the eth root of c.