Usage Guide

Welcome to our CTF Challenge!

In order to run the challenge, you need to make sure you have the following:

1. Access to nova (or whatever other remote server the game's host sets up the CTF's servers on)
2. Python installed on your computer along with the following packages:
   a. Requests
   b. Crypto

To start the challenge simply run python client.py, and it will instruct you from there.

You are welcome (and encouraged) to use the user_help_functions folder, which contains wrappers for some of the stages (for example sending messages to the servers), and helpful functions to the game in general.

The challenge takes place entirely inside the terminal, but do not worry - even if it closes, our server remembers in which stage of the challenge you were, and you won't have to go through prior stages again.

Background

The basis of the challenge is the Bleichenbacher attack - a powerful cryptographic attack that was invented in the late 90s, and used even along the 2000s and 2010s.

The attack targets the TLS, a protocol used to create a secure channel between a server and a client (or 2 users, each playing one of the roles). Specifically, it attacks the RSA key exchange, which uses the asymmetric RSA encryption to pass along a symmetric key.

Due to RSA's multiplicative homomorphism (meaning 2*E(x) = E(2*x), where E(x) is the encryption of x), the key exchange must be used with a padding scheme (otherwise someone could, for example, charge you twice the amount of money you agreed upon). This padding scheme stands at the core of Bleichenbacher's attack.

The attack's goal - find the symmetric key passed during the exchange between an honest user and a server, and use it to read all of the user's messages, and even impersonate them.

The attack is based upon a padding oracle, a component which tells us if some ciphertext has a valid padding under the encryption (meaning, given C = E(x), does x have a valid padding).

The Challenge

Our challenge focuses on side channels - information leaked from servers unwillingly (and usually unknowingly), that allows an attacker an entry way or a clue for some piece of information they need to gain access to things they shouldn't.

In our challenge, we create a series of servers, each leaking different pieces of information allowing you to build a padding oracle from. Your goal - create a good padding oracle from each vulnerable server presented to you, prove it’s working, and implement the original attack using a fast oracle, to reveal the CTF’s final message.