Hello, Player!  
You’re going to play a CTF made by team 007, in the workshop of “implementation of cryptographic attacks”. We hope you’ll enjoy our CTF :P  
  
Some instructions-   
To play, you need access to:  
1. player.py  
2. leaked\_message.bin  
3. Internet connection

In order to start, run the player.py  
There are 5 levels -

Level 0 - introductory, to create an atmosphere of a CTF

Level 1 - implementation of the basic Bleichenbacher attack

Level 2.i for i in {1,2,3} - implementation of some optimization to the original algorithm

Level 3 - implementation of a more sophisticated attack, resistant to noisy oracle

Each level you’ll solve will grant you some score, and your goal is to maximize your overall score.

In order to access level j+1 you’ll need to solve level j.

Clarification - the only background required for this CTF is some basic python, and some mathematical notations, and as you’re familiar with it we are sure you’ll be fine (probably).

The main goal of each level i for i > 0 is to complete the code skeleton given to you. We’ll supply sources and summaries on the attacks that should be enough, but you’re always welcomed to do some googling on what isn’t clear for you. ChatGPT isn’t welcomed, and if you do use it try to not use it to solve the entire CTF for you, it’s just like reading a write up…

glhf

Yours,  
Team 007