**This level will focus on implemeting an optimization of Parallel Threads Method on a BVO Oracle.**

\*The article related article can be found [here](https://www.researchgate.net/publication/220335690_Attacking_RSA-based_sessions_in_SSLTLS).

The **Bleichenbacher attack**, first discovered in 1998 by Daniel Bleichenbacher, exploits weaknesses in RSA encryption when using PKCS#1 v1.5 padding. This padding scheme, historically used in SSL/TLS, allows an adaptive chosen-ciphertext attack that enables an attacker to decrypt RSA-encrypted messages without knowledge of the private key.

**The BVO Oracle (Bleichenbacher Vulnerability Oracle)**

A **Bleichenbacher Vulnerability Oracle (BVO)** is an oracle that leaks information about the validity of a given RSA ciphertext based on how a server processes padding errors. Specifically, when interacting with a vulnerable server, an attacker can distinguish between two cases:

1. The decrypted message conforms to the PKCS#1 v1.5 padding format.
2. The decrypted message does **not** conform to the expected padding format.

The presence of this oracle enables an attacker to perform a **padding oracle attack**, where they iteratively refine their guesses about the plaintext by sending modified ciphertexts and observing the server’s responses.

**Parallel Threads Method for Optimized Attack Execution**

A more advanced optimization technique, introduced by Klíma, Pokorný, and Rosa, is the **Parallel Threads Method**. This method improves the efficiency of Step 2b in Bleichenbacher’s attack by handling multiple search intervals simultaneously in a structured cycle. The key aspects of this method are:

1. **Threaded Interval Search:** Instead of sequentially searching for a valid multiplier , separate threads are assigned to different intervals in the set , with each thread attempting Step 2c.
2. **Cyclic Execution:** If multiple intervals exist, the threads operate in a cycle, each making one oracle query per iteration. The search proceeds iteratively across all intervals.
3. **Efficient Interval Reduction:** Once a valid is found, all intervals are updated accordingly. Threads corresponding to empty intervals are eliminated, and the process continues with renumbered intervals.
4. **Guaranteed Progress:** Because at least one interval contains the correct plaintext, this method ensures that an acceptable multiplier will eventually be discovered, reducing unnecessary computations.

This approach significantly optimizes the attack by reducing redundant computations and ensuring a more efficient search process.

**CTF Challenge: Completing the Missing Lines**

In this CTF challenge, your task is to complete the missing lines in the provided Python script to successfully execute the Bleichenbacher attack using the **BVO oracle and the Parallel Threads Method**. The given script already includes:

* **Network communication setup** using sockets to interact with the vulnerable server.
* **Adaptive chosen-ciphertext attack framework**, including an iterative process to refine decryption attempts.

To solve this challenge, you must:

* Implement the **iterative searching process** to determine valid padding.
* Utilize **Parallel Threads Method** to optimize the search for valid multipliers.
* Ensure proper response handling to infer padding validity based on the server’s behavior.

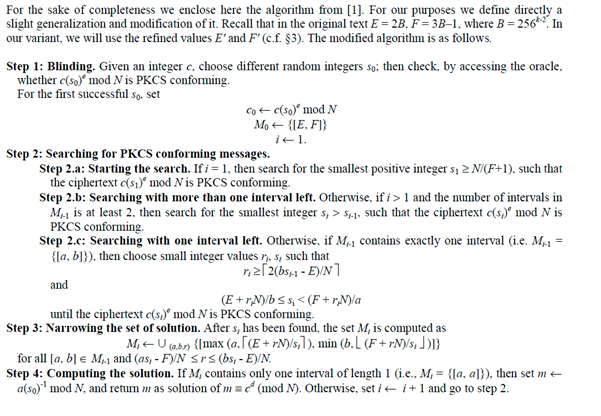
By leveraging the **BVO oracle** and **Parallel Threads Method**, you can efficiently recover the plaintext from RSA-encrypted messages and successfully complete the challenge.

Please fill in the 5 spots where it says:

‘’’Complete the missing line’’’

Good luck!

**Pseudo code for reference:**

****