brevi moduli

25th September 2024 / Document No. D24.102.183

Prepared By: `rasti`

Challenge Author(s): `rasti`

Difficulty: Very Easy

Classification: Official

Synopsis

- `brevi moduli` is a very easy challenge. The player has to pass five rounds to get the flag. At each round, they will have to submit the prime factors p, q of a 220-bit RSA modulus. Since the modulus is small, it can be factored by most tools, such as SageMath.

Description

- On a cold Halloween night, five adventurers gathered at the entrance of an ancient crypt. The Cryptkeeper appeared from the shadows, his voice a chilling whisper: "Five locks guard the treasure inside. Crack them, and the crypt is yours." One by one, they unlocked the crypt's secrets, but as the final door creaked open, the Cryptkeeper's eerie laughter filled the air. "Beware, for not all who enter leave unchanged."

Skills Required

- Know how to interact with TCP servers using pwntools.
- Very basic knowledge of the RSA cryptosystem and the Integer Factorization problem.

Skills Learned

- Learn how to factor small RSA moduli with SageMath (or any other tool).