Baby ROCA

Description

- Simple Case of ROCA
- ROCA(Return of Coppersmith Attack) is an attack on factoring RSA Modulus using Coppersmith Method, where a vulnerability lies in generating primes.
- ref) ACM-CCS 2017paper https://acmccs.github.io/papers/p1631-nemecA.pdf
- ref) CVE-2017-15361 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-15361

Exploit

Please refer to exploit.sage