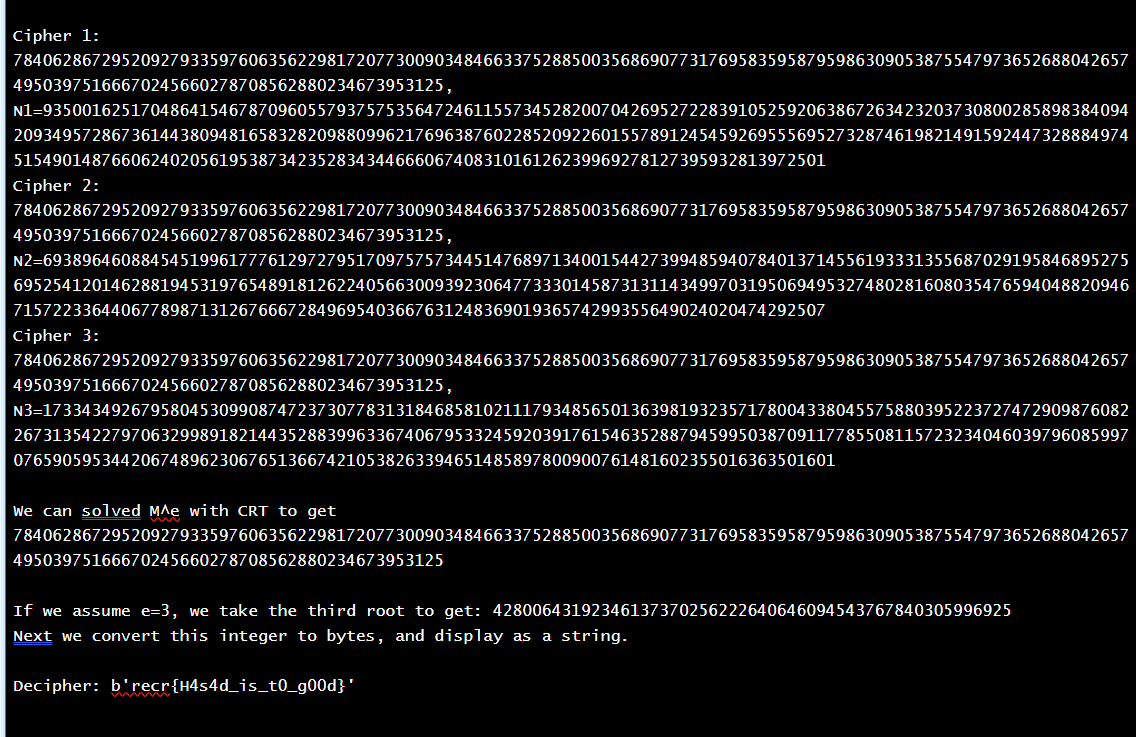
CRYPTOGRAPHY

1. Plain RSA was too easy apparently. Try this variation of RSA. (A guy just told me that the Chinese are too smart XD)

Solution:



**Explanation of Deciphered Message:**

In the given cipher result, the text b’recr{H4s4d\_t0\_g00d}’ is deciphered. The message inside the curly braces typically follows a **flag format**, which is common in **Capture the Flag (CTF)** . The characters H4s4d\_t0\_g00d can be interpreted as "Hasad is too good," where the number **4** is a substitute for the letter **A**, and **0** is a substitute for **O**. This type of substitution is a classic leetspeak (1337) pattern used in puzzles, challenges, and online communities.

**Approach:**

**1. CTF Solver Tool:**

The solution was obtained using a **CTF Solver**, a tool frequently utilized for security challenges in **Capture the Flag** competitions. CTF solvers help decrypt or decode various types of ciphers, including **RSA encrypted messages**. These tools are designed to work with known vulnerabilities or weaknesses in encryption, making it easier for security professionals to crack codes and analyze encryption algorithms in a controlled environment.

**2. Chinese Remainder Theorem (CRT):**

The **Chinese Remainder Theorem (CRT)** is an essential mathematical theorem used in several applications, including **RSA decryption**. It allows efficient computation when working with large numbers, as is common in cryptography.

* In **RSA encryption**, CRT optimizes the decryption process by breaking down large integers (modulus) into smaller, more manageable components.
* CRT is especially effective when the **public key modulus (n)** is the product of two large prime numbers (**p** and **q**), and the system can use the theorem to decrypt messages by solving multiple congruences.
* This theorem improves decryption speed significantly, making it a widely adopted technique in real-world RSA implementations.

By applying **Chinese Remainder Theorem** during RSA decryption, the tool can effectively reverse the encryption process, leading to the recovery of the original plaintext.