Before you read this document, please have this playing in the background:

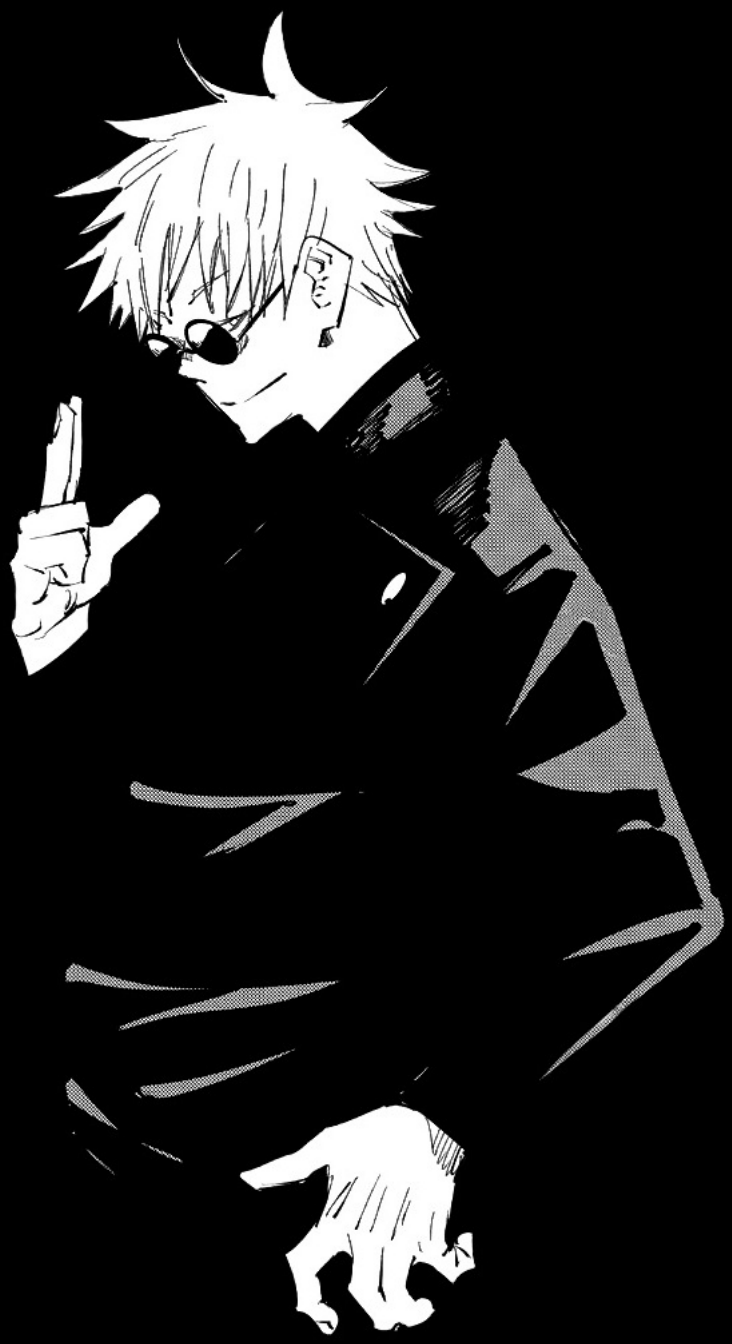
https://youtu.be/RaQGqjYcxAg

I am serious, go do it, open the link.

Alright I hope you’re ready :D

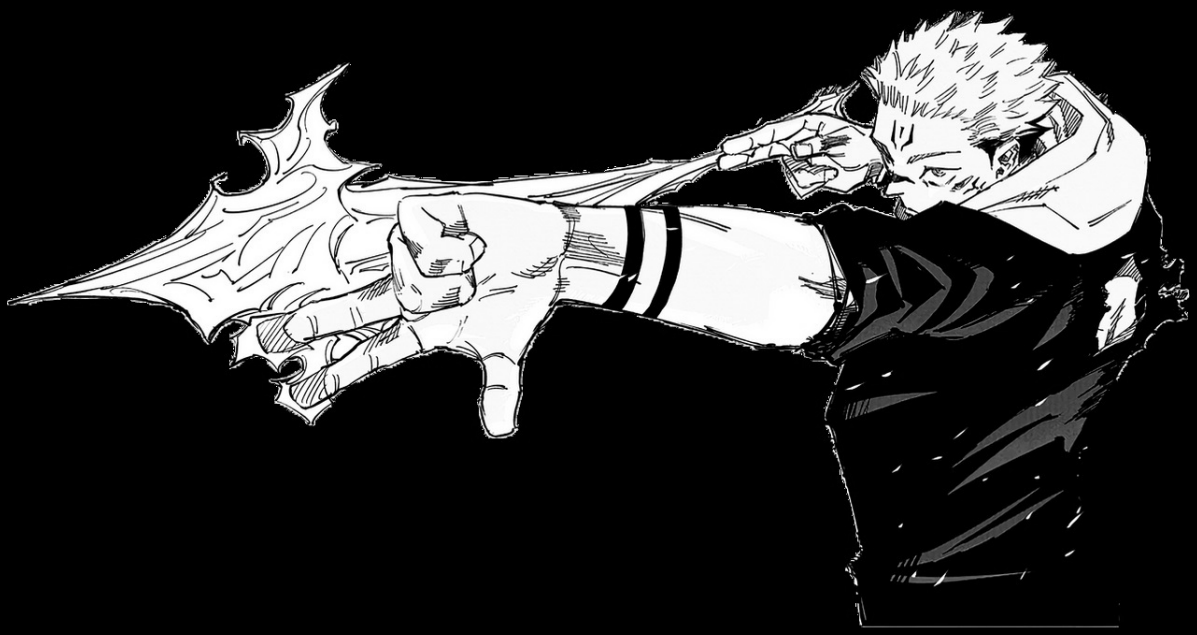
As the pentester got out his laptop and began dissecting the code he asked the challenge:

“Are you difficult to solve because your cursed technique is RSA?
Or is your cursed technique RSA because you’re difficult to solve?”



The challenge then replied:

"Stand proud, you are strong. But you're a fool for thinking you can beat the king of curses. **Arm yourself**."



For unbeknownst to the pentester, the challenge had transformed the plaintext by passing it into an obscure polynomial function before performing multiple RSA encryptions on it.

In that moment, the challenge could've saved itself, but it did not know 2 key things:

- The first is to always bet on the pentester.
- The second is that the pentester knew Chinese Remainder Theorem.

The pentester combined his techniques:

- Chinese Remainder Theorem - To recover the output of the obscure function
- Sympy - To parse the 4th degree polynomial into Python (or not hehehe)
- Equation Solving - To construct f(x) = f(AES_KEY) and solve for x (the key)

And then, he unleashed a force that all men should fear:

Domain Expansion: Asymmetry

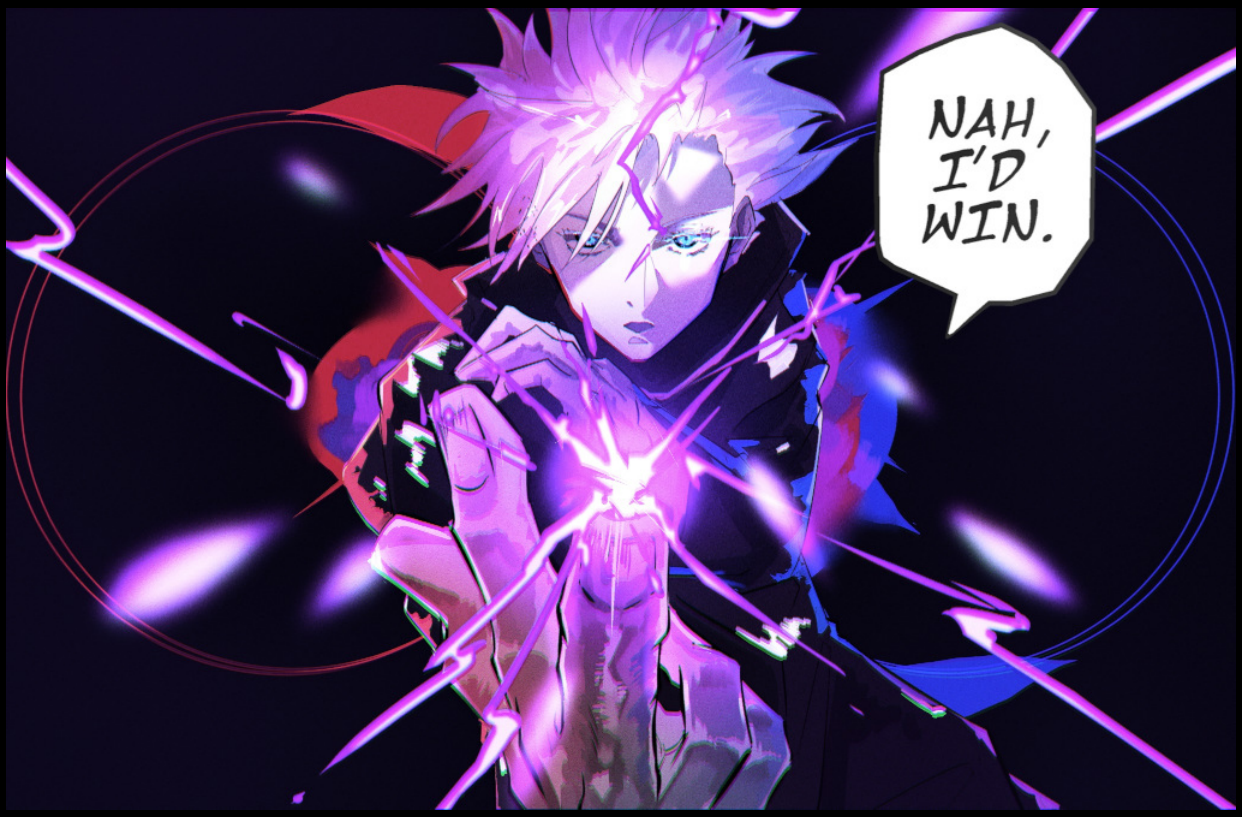
The pentester's domain: Asymmetry. It is an exceptionally refined domain that undermines symmetric ciphers. In a battle where the opponent's domain is AES based, Asymmetry is sure to overtake it. The adversary has absolutely no chance of victory.

In a battle of domains, cursed techniques are rendered practically useless, hence why Asymmetry is such a powerful trump card in this case.

The challenge's cursed technique "Repeated RSA", which is an asymmetric cipher, is irrelevant. When both parties expand their domains, the battle will ONLY be decided according to whose domain is stronger. If the challenge's domain was an asymmetric cipher, the battle would be much closer in terms of power.

In addition, inside your own domain, your attacks are guaranteed to hit the opponent within a predetermined radius (100 meters). The challenge could no longer escape.

The pentester, knowing that his Domain is far superior to that of the challenge's, stood proud, and arrogantly struck his final pose:



FLAG{n4h_I'd_w1n_~_s4t0ru_G0Jo}

Bonus:
https://youtu.be/jPZlabsAlVM