Super computer.

Inspecting the source code, you are provided 3 primes: p, q, r, each 2048 bits long.

This is a maths question:

$$n = p^q r$$

$a = \text{rand}(0, n)$ is a random numbe

We are given $a \nmid p$ (a does not divide p).

$$t = a^n + (n-a)^n$$

$$= a^n + \sum_{k=0}^{n} \binom{n}{k} n^k (-a)^{n-k}$$

$$= a^n + \sum_{k=1}^{n} \binom{n}{k} n^k (-a)^{n-k} + \binom{n}{0} n^0 (-a)^n$$

$$= a^n + \sum_{k=1}^{n} \binom{n}{k} n^k (-a)^{n-k} \neq -a^n$$

(since n is odd).

$$= \sum_{k=1}^{n} \binom{n}{k} n^k (-a)^{n-k}$$

$$= \sum_{k=1}^{n} \left(\frac{n!}{k!(n-k)!} n^k (-1)^{n-k} \right) a^{n-k}$$

We can think of t as a polynomial $t(a) = \sum_{k=1}^{n} b_k a^{n-k}$. Since $a \nmid p$, we have that the polynomial can't be divided by p unless each coefficient can be divided by p. Why? (I will try to show this later).

$$t(a) = \sum_{k=1}^{n} b_k a^{n-k} \quad \text{where } b_k = \frac{n!}{k!(n-k)!} n^k (-1)^{n-k}$$

We can ignore the $(-1)^{n-k}$. It doesn't make any difference to our logic.

~~Here~~ For what k ~~is the~~ does b_k have the ~~lowest~~ fewest p factors, for $k = 1 \ldots n$.

My guess ~~was~~ was $k=1$:

$$b_{k=1} = \frac{n!}{1!(n-1)!} n^1 = \frac{n!}{(n-1)!} n = n^2$$

$$= p^{2q} r^2$$

b_1 has $2q$ many p factors.

$k > 1$ leads to both the $\frac{n!}{k!(n-k)!}$ and n^k having more p factors. Setting $k = n$ gives $b_n = \frac{n!}{n!\,0!} n^n = n^{n+1}$

which ~~basis~~ is $p^{qn+q} r^{n+1}$ has $q(n+1)$ ~~p~~ p factors.

So, $\frac{t(a)}{p^{2q}} = u(a) := \sum_{k=1}^{n} \frac{b_k}{p^{2q}} a^{n-k}$

$$= a^{n-1} + \sum_{k=2}^{n} \frac{b_k}{p^{2q}} a^{n-k}$$

Now, we know $t(a)$ can be divided by p $\boxed{2q}$ many times, ~~and~~ (at least) and if I tried that as the value to xor with the key to solve this.