4096

We are given $n = \prod_{i=1}^{128} p_i$ where p_i are ~~primes~~ 32 bit primes. ~~is~~
The secret flag is encoded as an integer m. $e = 65537$ is chosen. We are also given $m^e \bmod n$.

The problem is ~~not quite~~ to find m.

$\cancel{m = ((m^e)^{\frac{1}{e}}) \bmod}$

This is just the problem of finding the e^{th} root of $m^e \bmod N$. ~~For~~
Now, ~~if N was pr~~ this problem is simple ~~if~~ in $(\bmod p)$:

$\cancel{\sqrt[e]{m^e \bmod}}$ $\sqrt[e]{x^e} \bmod p$

can be solved by finding $d = 1/e \bmod (p-1)$

Assuming e^{-1} exists mod $(p-1)$ (i.e. $e, p-1$ are coprime) (which is true as ~~e is prime~~ $e = 65537 = 2^{16}+1$ is prime)

$$(x^e)^d \bmod p = \cancel{(x^e)^d} (x^{ed}) \bmod p$$

$$= x^{k(p-1)+1} \bmod p$$

$$= \cancel{x^{kp-k+1} \bmod p}$$

$$= (x^{p-1})^k * x \bmod p$$

$$= 1^k x \bmod p = x \bmod p$$

(By Fermat's Little Theorem).

To reduce this problem to one in prime modulo, we ~~do~~ factorise n into its prime factors, (on Sage this takes 10 secs) and then:

$$
\begin{aligned}
m^e \rightsquigarrow &= x_1 \mod p_1 \\
&= x_2 \mod p_2 \\
&\vdots \\
&= x_{128} \mod p_{128}
\end{aligned}
$$

Applying the previous logic gives us

$y_1 \ldots y_{128}$ s.t.

$$
\begin{aligned}
y_1^e &= x_1 \mod p_1 \\
y_2^e &= x_2 \mod p_2 \\
&\vdots \\
\cancel{y_{128}^e} &\cancel{= x_{12}} \\
y_{128}^e &= x_{128} \mod p_{128}
\end{aligned}
$$

~~Since the C.R.T. gives us a~~
Using the C.R.T., this gives us a unique $m \ (\text{mod } \prod_{i=1}^{128} p_i)$ s.t.

$$m \mod p_i = y_i \quad \forall i \in \{1 \ldots 128\}$$

This m is the solution.

N.B. Use Sage's CRT_list() function to solve CRT systems as above.