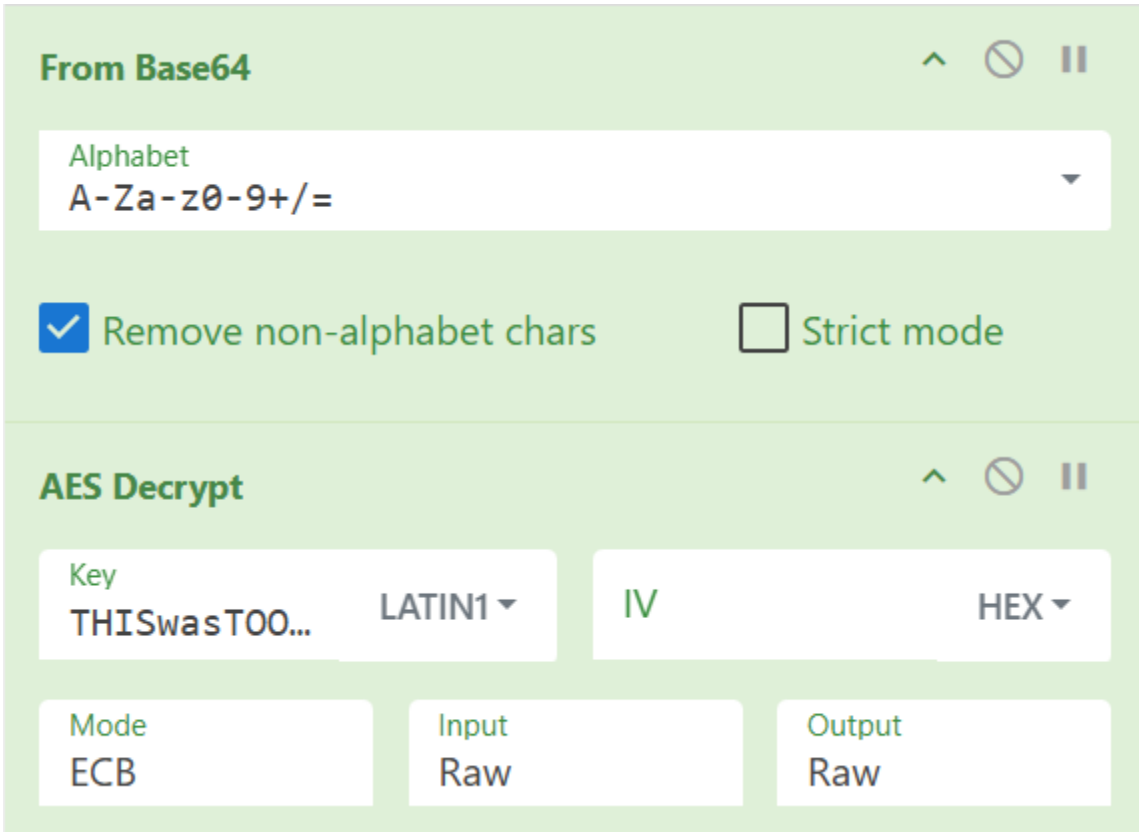
Ok, we got 4 files. An image, a PEM key and 2 txt files.

I entered the image on aperisolve and… steghide found something: “THISwasTOOiziECB”

Ok, so ECB is a reference to AES ECB, and it has exactly 16 characters so it might be a key.



In the conversation we find the sum of p and q.

If we open the PEM certificate in a pem decoder, we also find the value of n and e, where n is p*q.

Now we can find p and q!

```
from sympy import symbols, Eq, solve
S =
24722116169992465881070271199690169362455458193332180161871370678459930090250287749736220134651803789983780083709278592071250797494670685808152851319806502
P =
15218966215249805640370541417056850893626672779783398907484619319399825150163392359165457714902129117753146560301113050733872847791431764925614982862830315242541719435060963796338594545570952225330737159619432679619190737472156100146461295800748858807979656202073184814676911092346288001055027983336316742805
x = symbols('x')
solutions = solve(Eq(x**2 - S*x + P, 0), x)
p, q = solutions
print("p:", p)
```

```
print("q:", q)
```

Now, before we retrieve the flag we need to turn the secret into a digit by doing base64 -> hex and then hex -> decimal (using cyberchef then rapidtables for example)

Then, all we need to do is plug our values into dcode's RSA calculator and the flag is ours!

Made with love by: AndreiCat