Crypto week 4 - Baby Step Giant Step

Define our Finite Field and the polynomial ring for that field. We also define h, g and m.

We chose $m = round(\sqrt{2^{11}}) = 45$ because it is a nice number that will probably give us the answer.

```
R = PolynomialRing(GF(2^11, name='b'), 'x')
x = R.gen()
h = x^9 + x^8 + x^6 + x^4 + x^2 + x + 1

S = R.quotient(x^11 + x^2 + 1)
xbar = S.gen()
g = xbar

m = round(sqrt(2^11))
```

Calculate the baby steps $g^0, g^1, \ldots, g^{m-1}$.

We put this in the table tbl.

```
tbl = {}
d = 1
for i in range(0, m):
    tbl[d] = i
    d = d * g
view(tbl)
```

$\{xbar^{10} + xbar^3 + xbar : 21, 1 : 0, xbar^8 + xbar^3 + xbar : 30, xbar^4$ -

Compute $G = g^{-m}$

```
G = g^(-m)
view(G)
```

$xbar^9 + xbar^8 + xbar^7 + xbar^5 + xbar^2 + xbar$

Compute the Giant steps, $h_a, h_aG, h_aG^2, h_aG^3, \ldots$

At each step, we check if this value is in the table tbl, generated with the baby steps. If so, we have found the solution.

```
hg = h
i = 0
for j in range(0, 2^11):
    if hg in tbl:
        i = tbl[hg]
        break
    hg *= G

view(hg)
view(i)
view(j)
```

$xbar^9 + xbar^5$
27
12

We now have: i, j with $g^i = h_a \cdot G^j = h_a \cdot g^{-mj}$

Which results in: $g^{i+mj} = h_a$. Thus, we output $i + mj$.

```
a = i+m*j
view(a)
```

567

And now we check if this is indeed the answer with checking if $h = g^a$.

```
view(g^a)
view(g^a == h)
```

$xbar^9 + xbar^8 + xbar^6 + xbar^4 + xbar^2 + xbar + 1$
True