Crypto Week 4 - Pohlig-Hellman

Define our Finite Field and the polynomial ring for that field.

We want to find an a such that $g^a \equiv h \mod x^{11} + x^2 + 1$

```
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()
hbar = S(h)
```

First we determine the prime factors of the order, which should be 23 and 89, as given by the exercise.

```
factor(2047)
```

$$23 \cdot 89$$

We see that:

$$h^{23} \equiv x^7 + x^6 + x^3 + x^2 + 1 \mod x^{11} + x^2 + 1$$

$$h^{89} \equiv x^{10} + x^8 + x^7 + x^6 + x^5 + x^4 + x^2 + 1 \mod x^{11} + x^2 + 1$$

```
view(hbar^23)
view(hbar^89)
```

$$xbar^7 + xbar^6 + xbar^3 + xbar^2 + xbar + 1$$
$$xbar^{10} + xbar^8 + xbar^7 + xbar^6 + xbar^5 + xbar^4 + xbar^2 + 1$$

We want to find a a_{23} with $h^{23} \equiv x^{a_{23}*23} \mod x^{11} + x^2 + 1$ and a_{89} with $h^{89} \equiv x^{a_{89}*89} \mod x^{11} + x^2 + 1$.

For this, we will turn to the **Baby-Steps-Giant-Steps** algorithm. We will run this once for h^{23} with $g = x^{23}$ and once with h^{89} with $g = x^{89}$.

For simplicity, we used Sage's built-in Baby-Steps-Giant-Steps (bsgs) function. We also implemented bsgs ourselves, which you can find in it's own sage worksheet.

```
a23 = bsgs(xbar^23, hbar^23, (0, 2047))
a89 = bsgs(xbar^89, hbar^89, (0, 2047))
view(a23)
view(a89)
```

33
15

Thus, we have found that $a_{23} = 33$ and $a_{89} = 15$. We check this as follows:

```
view(xbar^(a23*23))
view(xbar^(a23*23) == hbar^23)
view(xbar^(a89*89))
view(xbar^(a89*89) == hbar^89)
```

$xbar^7 + xbar^6 + xbar^3 + xbar^2 + xbar + 1$
True
$xbar^{10} + xbar^8 + xbar^7 + xbar^6 + xbar^5 + xbar^4 + xbar^2 + 1$
True

To find the result, we first check the XGCD:

```
xgcd(23, 89)
```

$(1, 31, -8)$

Since this gives $31 \cdot 23 - 8 \cdot 89 = 1$, we can apply the Chinese Remainder Theorem to give the solution:

```
sol = crt([15, 33], [23, 89])
view(sol)
```

567

Which we can check as follows:

```
view(xbar^sol)
view(xbar^sol == hbar)
```

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