Goal: Solve for x in the equation $h = g^x \bmod p$ using Meet-in-the-Middle attack.
$B = 2^{20}$ (around 1 million).

We are given three big numbers:
1. p (a prime number)
2. g (a generator number)
3. h (a target number).

They give you an equation: $h = g^x \bmod p$
I must find the secret number x.

Example: Imagine p=13, g=2, and h=3.
Find x such that: $2^x \bmod 13 = 3$

The answer is x = 4 because: $2^4 = 16$ and 16 mod 13 = 3, but in the homework, p,g, and h are very big numbers (over 150 digits)!

x could be any number up to 2^{40}. That's over 1 trillion possibilities. Trying all values would take many years.

Split the search into two smaller searches:
I can write: $x = x_0 \times B + x_1$ where $B=2^{20}$ and $0 \leq x_0, x_1 < B$
So: $h = g^{x0B+x1} \bmod p =(g^B)^{x0} \bmod p$
Then rearranging:

$$(g^B)^{x0} = h \times (g^{x1})^{-1} \bmod p$$

Now, x_0 is on the left side, and x_1 is on the right side. This is called a meet-in-the-middle attack.

Step 1: For every x_1 from 0 to B−1:
- Compute g^{x1} mod p.
- Find its modular inverse.
- Multiply by h mod p.
- Store the result in a hashtable.

Step 2: For every x_0 from 0 to B−1:
- Compute $(g^B)^{x0}$ mod p.
- Check if this number exists in the table.

- If yes:
  - You found x_0 and x_1.
  - Then calculate: $x = x_0 \times B + x_1$

Example:

Let me say that I have B=4. (small for the sake of simplicity)

$x = x_0 x\ 4 + x_1$ where $0 <= x_0, x_1 < 4$

we are splitting x into two parts: x_0 and x_1

Then, we will rearrange the formula to be

$$(g^B)^{x0} = h \times (g^{x1})^{-1} \bmod p$$

x	$(g^{x1}) \bmod p$	Inverse $(g^{x1})^{-1} \bmod p$	$h \times (g^{x1})^{-1} \bmod p$
0	$2^0 = 1 \bmod 13 = 1$	Inverse of 1 is 1	$3 \times 1 \bmod 13 = 3$
1	$2^1 = 2 \bmod 13 = 2$	Inverse of 2 is 7	$3 \times 7 \bmod 13 = 8$
2	$2^2 = 4 \bmod 13 = 4$	Inverse of 4 is 10	$3 \times 10 \bmod 13 = 4$
3	$2^3 = 8 \bmod 13 = 8$	Inverse of 8 is 5	$3 \times 5 \bmod 13 = 2$

Now try $(g^B)^{x0}$ mod 13 for each x_0 :

From the table, we found $x_0 = 1$ and $x_1 = 0$

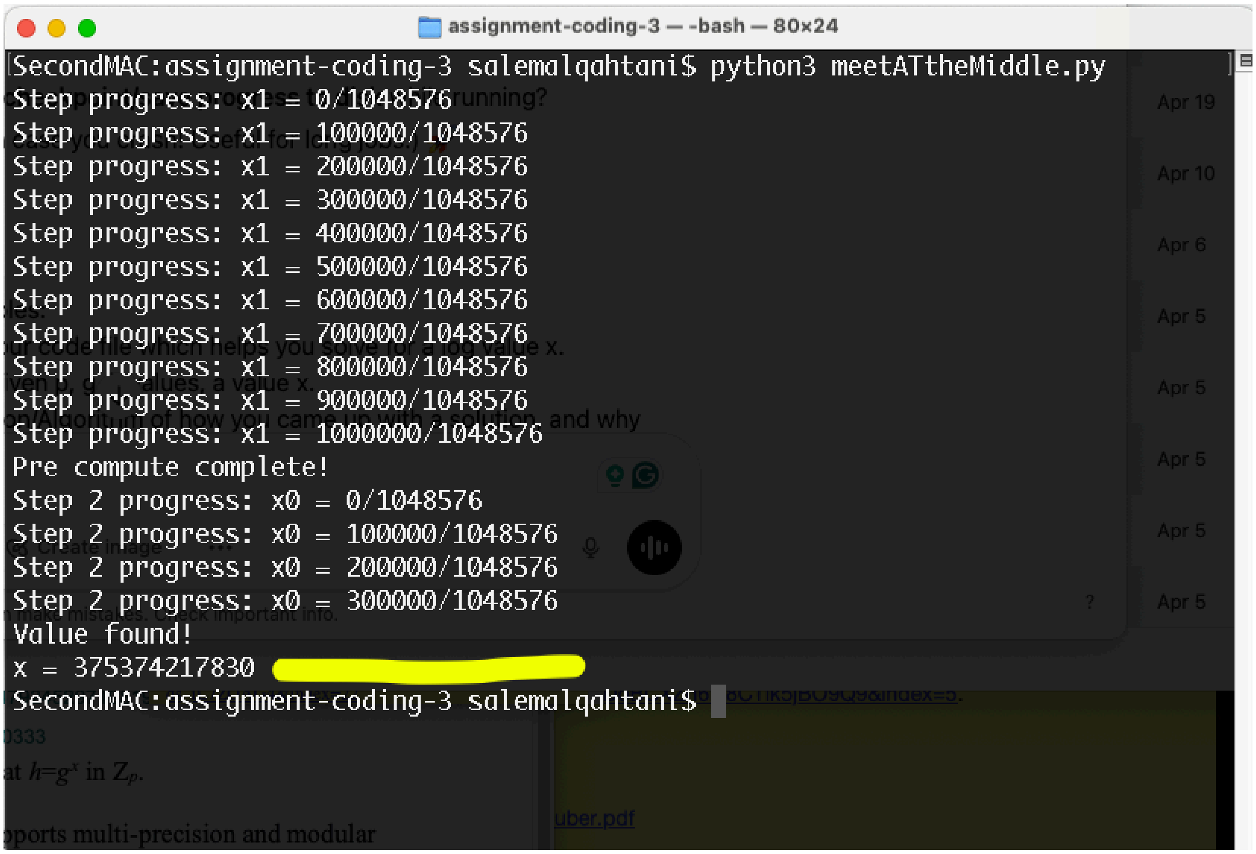
$X = x_0 \times B + x_1$

$X = 1 \times 4 + 0 = 4$

Therefore, the solution is x = 4 . And indeed: $2^4 = 16$, 16 mod 13 = 3

$2^4 = 16$, 16 mod 13 = 3

Screenshot


assignment-coding-3 — -bash — 80×24
SecondMAC:assignment-coding-3 salemalqahtani$ python3 meetATtheMiddle.py
Step progress: x1 = 0/1048576
Step progress: x1 = 100000/1048576
Step progress: x1 = 200000/1048576
Step progress: x1 = 300000/1048576
Step progress: x1 = 400000/1048576
Step progress: x1 = 500000/1048576
Step progress: x1 = 600000/1048576
Step progress: x1 = 700000/1048576
Step progress: x1 = 800000/1048576
Step progress: x1 = 900000/1048576
Step progress: x1 = 1000000/1048576
Pre compute complete!
Step 2 progress: x0 = 0/1048576
Step 2 progress: x0 = 100000/1048576
Step 2 progress: x0 = 200000/1048576
Step 2 progress: x0 = 300000/1048576
Value found!
x = 375374217830
SecondMAC:assignment-coding-3 salemalqahtani$