**Hash Lab**

Write a program to find a number, x, which hashes to a number, y, with a given pattern of low order bits. I’ll send you a number , z, whose low order bits you want to match.

y = SHA1(x)

y = 0x1f2f33bb5d2d828f1616d1bb87

y = …01100001011011**0100011011101110000111**

bits match!

z = …11010010011110**0100011011101110000111**

z = 0x52057942e913405b6d2791bb87 **# I sent you this number**

Find an x with the most low order bits matching z in a reasonable amount of time. Time your program. How long would it take to find the full hash?

Use SHA1.

Python has a native hash library (you don’t need to use the Crypto library)

import hashlib

h = hashlib.sha1()

h.update('abc')

print h.hexdigest()

Work individually, or in groups of 2. Fill this out and email it to me, so we can both cut and paste the number.

Name: Diksha Garg ID: 2088

Number of bits matched: 26 Time it took: 107.57

Time it would take to match all bits: 2.3426671e+42

x = 0x68843a