**Q1)** Since the oracle does not give us decrypted version of the C, we need to give it something that we can recover M from the decryptions it gave. I did the following:

When we send C^2 result will be M^2. Then I send C^3 and received M^3. At the last step if I multiply M^3 by M^-2 mod p I will get M mod p which is the plain text.

Following Python code did it and the results are as follows:

**Answer : Bravo! You found it. Your secret code is 22545**

metin, ekran görüntüsü, yazı tipi, yazılım içeren bir resim

Açıklama otomatik olarak oluşturuldu

Q1.py

**Q2)** Since the pin code has 10^4 possible value and since the salt can take at most 2^8 different value, key space is very small (around 2.5 million). So we can do a brute force attack to find the PIN number. Q2.py does that operation and results are as follows:

**Answer:**

**PIN NUMBER iS: 1308**

**The Salt is: 206**

metin, ekran görüntüsü, yazılım, ekran, görüntüleme içeren bir resim

Açıklama otomatik olarak oluşturuldu

**Q3) The problem with the implementation is that, at the encryption it does not select random number from a large range but only choose values from 0 to 2^16.** That makes there are around 65.000 possible k value. By implementing a brute force attack on k, we can retrieve the k value because generator is a public variable and the space we need to try is very small. If we know the k we know that . So, I implemented that solution in the Q3.py and the results are as follows:

**Answer: Be yourself, everyone else is already taken.**

metin, ekran görüntüsü, yazılım, multimedya yazılımı içeren bir resim

Açıklama otomatik olarak oluşturuldu

**Q4)** Since the r1 and r2 are equal, that implies k1 and k2 are equal. By knowing that we can do the following math:

Basically if we divide t2 by t1 in mod p we will get m1 \* inverse of m2 mod p. If we multiply that by m1 we will obtain the m2. These calculations are done in q4.py and the answer is as follows:

**Answer: m2 = “A person can change, at the moment when the person wishes to change.”**

metin, ekran görüntüsü, yazılım içeren bir resim

Açıklama otomatik olarak oluşturuldu

**Q5)** If we know the relation between k1 and k2 we can exploit that relation to find a. We know the following 2 equalities by implementation of DSA.

That means

Since all the values are known we can obtain the a from this calculation. Q5.py will solve this issue.

**Answer: 2247688824790561241309795396345367052339061811694713858910365226453**