**Cryptography Assignment - 10**

**Pramod Aravind Byakod**

**Question 1:**

**Suppose we use the RSA cryptosystem with n, e from the last homework.**

**(a) If the cipher text c = your ID number (as a decimal integer), can you compute the plaintext?**

**(b) Suppose that you find the decryption key to be d = 879829162542850074748838973716462641470292321076843078870413133138541894315167534655428516005898396122103324293925057981802023330186106794090644952807381680714475934931163153**

**can you now compute the plaintext for your ID number?**

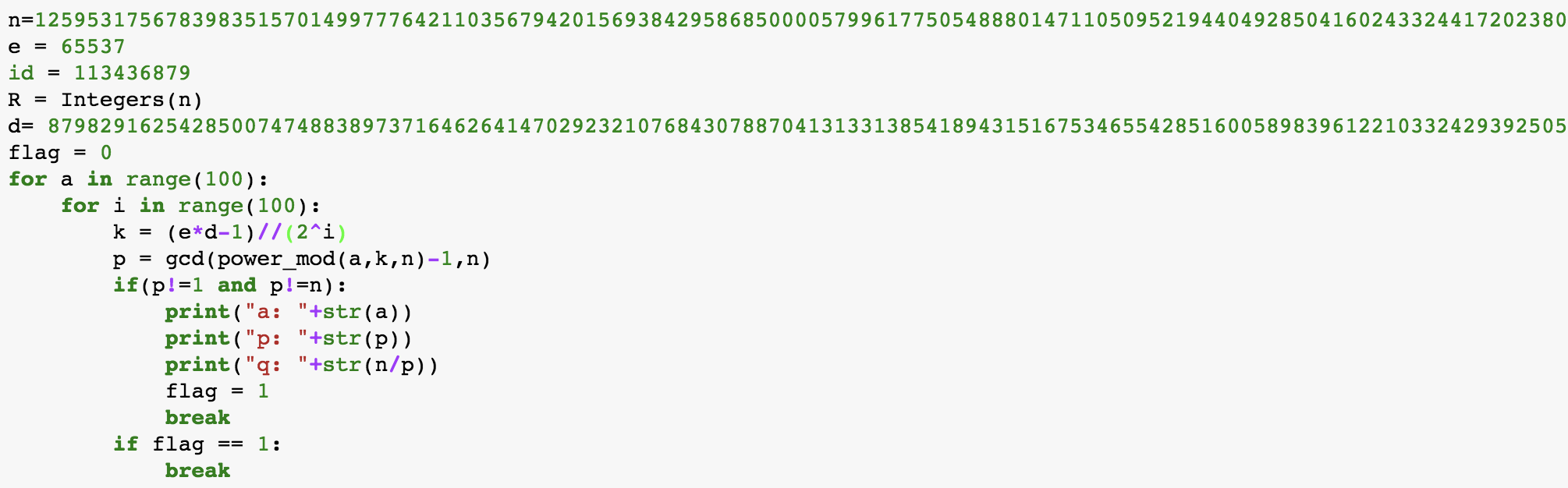
**(c) Can you factor n? If so, what are the prime factors? Use a program to explain your approach.**

**(d) Try 100 random a’s. How many of them allow you to factor n? Estimate the probability of success.**

With ID, 113436879, being a cipher text, it’s not possible to compute the plaintext and is not safe.

With d value being such a huge number, we can compute the plaintext for ID number and is safe.

**Program:**

****

**Output:**

a: 7

p: 139583468203468547958790587305879573958759862470582467047605860298560237860276207823

q: 9023502374564762856057628405217347420367023745275842765476287501762476920480485067209574327

**Yeah, we can factor n. Above p and q values are the prime factors.**

**Program:**

****

**Output:**

**The probability of success is: 52%**

**Question 2:**

**Suppose that we decide to use= 65537 as the RSA public exponent. Can we use prime numbers that are congruent to 1(mod e) to generate n? Why? Find a prime satisfying:**

**• p≡1(mode);**

**• 21000≤p≤21004;**

**• The first 9 decimal digits of p is your ID number.**

**Explain your approach.**

We know that n=p\*q, where p is the generator of n.

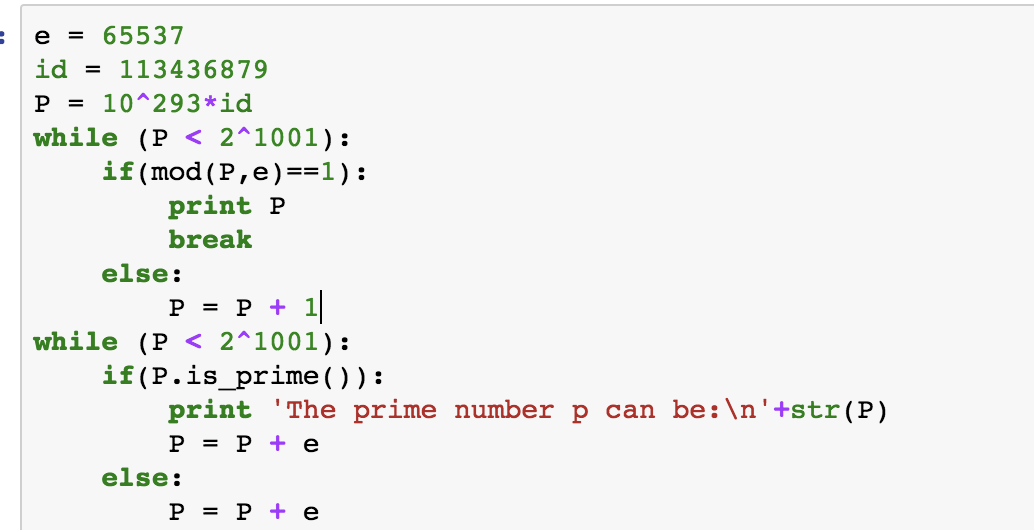
Considering p=1(mod e), in that case p-1 divides e. We can say, p-1=k\*e(k>=1).

But according to the keys definition, we have gcd (e, (p-1)(q-1))=1. In our case,

gcd (e, (p-1)(q-1)) = gcd (e, k\*e\*(q-1))= k\*(q-1) !=1.

Therefore, gcd of e and (p-1)(q-1) is not 1, **we can’t use this number to generate n**.

**Program:**



**Output:**

11343687900000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000030023

The prime number p can be:

11343687900000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000079759214393