HW8

Code(SageMath):

N=1259531756783983515701499777642110356794201569384295868500005799617750548880147110509521944049285041602433244172023804646590835427723055191592144638318476432867385429617360121

e = 65537

id = 113383597

#problem 1

R = Integers(n)

print("Ciphertext: "+str(R(id^e)))

#problem 3

d= 879829162542850074748838973716462641470292321076843078870413133138541894315167534655428516005898396122103324293925057981802023330186106794090644952807381680714475934931163153

flag = 0

for a in range(100):

for i in range(100):

k = (e\*d-1)//(2^i)

p = gcd(power\_mod(a,k,n)-1,n)

if(p!=1 and p!=n):

print "a: "+str(a)

print "p: "+str(p)

print "q: "+str(n/p)

flag = 1

break

if flag == 1:

break

Result:

Ciphertext:968178003421400411132841782911330496558985992097902484282132545236160455076917761233051253392581254113870298763101166386428807087285258693055736809713598057023659677463748964

a: 7

p:1395834682034685479587905873058795739587598624705824670476058602985602378602762078

q:9023502374564762856057628405217347420367023745275842765476287501762476920480485067209574327

1. Ciphertext:968178003421400411132841782911330496558985992097902484282132545236160455076917761233051253392581254113870298763101166386428807087285258693055736809713598057023659677463748964
2. Not secure. Because for the ID number which is just 9 bits, the key space is at most 10^9 (without considering the fixed number for ID number every year), which is too small.

p:1395834682034685479587905873058795739587598624705824670476058602985602378602762078

q:9023502374564762856057628405217347420367023745275842765476287501762476920480485067209574327