Question 2)

Use Sage to solve the following problems:

In part (a)-(c) determine if the following signatures are good or bad:

1. N = 13962799 and e = 3 value to sign = 821 and signature = 8674413
2. N = 34300129 and e = 61 value to sign = 2478 and signature = 27535246
3. N = 5898461 and e = 23 value to sign = 419 and signature = 2607727

d) Suppose that you have an RSA modulus with prime factors p = 3181 and q = 2677 and the public exponent is 163. Calculate the signature of 521 and then verify it.

Solution to Question 2)

Use Sage to solve the following problems:

In part (a)-(c) determine if the following signatures are good or bad:

1. N = 13962799 and e = 3 value to sign = 821 and signature = 8674413

sage: N = 13962799

sage: e = 3

sage: to\_sign = 821

sage: signature = 8674413

sage: R = IntegerModRing(N)

sage: R(signature)^e

821

sage: to\_sign == R(signature)^e

True

1. N = 34300129 and e = 61 value to sign = 2478 and signature = 27535246

sage: N = 34300129

sage: e = 61

sage: to\_sign = 2478

sage: signature = 27535246

sage: R = IntegerModRing(N)

sage: R(signature)^e

6227130

sage: to\_sign == R(signature)^e

False

1. N = 5898461 and e = 23 value to sign = 419 and signature = 2607727

sage: N = 5898461

sage: e = 23

sage: to\_sign = 419

sage: signature = 2607727

sage: R = IntegerModRing(N)

sage: R(signature)^e

3959558

sage: to\_sign == R(signature)^e

False

1. Suppose that you have an RSA modulus with prime factors p = 3181 and q = 2677 and the public exponent is 163. Calculate the signature of 521 and then verify it.

sage: p = 3181

sage: q = 2677

sage: e = 163

sage: N = p\*q

sage: phi\_N = (p-1)\*(q-1)

sage: d = xgcd(e, phi\_N)[1] % phi\_N

sage: d

8092027

sage: to\_sign = 521

sage: R = IntegerModRing(N)

sage: signature = R(to\_sign)^d

sage: signature

85205

sage: to\_sign == signature^e

True