Question 1)

Use Sage to answer the following questions. Show all your sage input/output:

1. Suppose your RSA public key factors as p = 6569 and q = 8089, and the public exponent e is 11. Suppose you were sent the Ciphertext 28901722. Perform the RSA Decryption and recover the plaintext.
2. Suppose that you want to encrypt the number 449 and send it to someone with public key N =37617577, and e = 529
3. Suppose that you forgot your public exponent, but you know that the prime factors of your Key's modulus are 1723 and 5381 private exponent is 223. Find the public exponent.
4. Use sage to generate an rsa public / private key pair and perform an encryption and decryption.

Solution to question 1)

Use Sage to answer the following questions. Show all your sage input/output:

1. Suppose your RSA public key factors as p = 6569 and q = 8089, and the public exponent e is 11. Suppose you were sent the Ciphertext 28901722. Perform the RSA Decryption and recover the plaintext.
2. Suppose that you want to encrypt the number 449 and send it to someone with public key N =37617577, and e = 529
3. Suppose that you forgot your public exponent, but you know that the prime factors of your Key's modulus are 1723 and 5381 private exponent is 223. Find the public exponent.
4. Use sage to generate an rsa public / private key pair and perform an encryption and decryption.

Solution to question 1)

Use Sage to answer the following questions. Show all your sage input/output:

1. Suppose your RSA public key factors as p = 6569 and q = 8089, and the public exponent e is 11. Suppose you were sent the Ciphertext 28901722. Perform the RSA Decryption and recover the plaintext.

sage: p = 6569

sage: q = 8089

sage: N = p\*q

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

sage: d = xgcd(11,phi\_N)[1] % phi\_N

sage: R = IntegerModRing(N)

sage: d

33804899

sage: R(28901722)^d

3167473

1. Suppose that you want to encrypt the number 449 and send it to someone with public key N =37617577, and e = 529

sage: N = 37617577

sage: e = 529

sage: R = IntegerModRing(N)

sage: R(449)^e

13188084

1. Suppose that you forgot your public exponent, but you know that the prime factors of your Key's modulus are 1723 and 5381 private exponent is 223. Find the public exponent.

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

sage: p = 1723

sage: q = 5381

sage: d = 223

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

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

5982367

1. Use sage to generate an rsa public / private key pair and perform an encryption and decryption.

sage: p = random\_prime(10000); p

6323

sage: q = random\_prime(10000); q

2833

sage: N = p\*q

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

sage: R = IntegerModRing(N)

sage: e = 31

sage: gcd(e, phi\_N)

1

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

sage: d

13861087

sage: plaintext = randint(2,2500)

sage: plaintext

205

sage: ciphertext = R(plaintext)^e

sage: ciphertext

6627708

sage: plaintext == ciphertext^d

True