This was another script that dealt with RSA encryption. This time it also decrypted using Chinese remainder theorem. It requires 6 arguments to use breakRSA.py.

argv[1] argv[2] argv[3] argv[4] argv[5] argv[6]  
 -e message.txt enc1.txt enc2.txt enc3.txt n\_1\_2\_3.txt  
 -c enc1.txt enc2.txt enc3.txt n\_1\_2\_3.txt cracked.txt

The usage for rsa.py is:

The g flag generates prime numbers and puts them to p.txt and q.txt to use for -e and -d

The e flag is for encrypting message.txt using p.txt and q.txt into encrypted.txt

The d flag does the opposite and decrypted.txt is the message

argv[1] argv[2] argv[3] argv[4] argv[5]  
 -g p.txt q.txt  
 -e message.txt p.txt q.txt encrypted.txt  
 -d encrypted.txt p.txt q.txt decrypted.txt