CM1208 Competition: Weak RSA

In order to ensure security, RSA cipher was used to encrypt a message. The plaintext includes a sequence of ASCII characters, converted to a number with each character taking a byte, starting from the most significant byte. For example, the ASCII codes of 'A', 'B' and 'C' are 0x41, 0x42 and 0x43 respectively (0x represents hexadecimal numbers), so the plaintext "ABC" is converted to a number 0x414243. The number is then encrypted using RSA. The public key is known, as follows (these are normal decimal numbers):

n =
890705833763392801928493085909849490066527653077305960454032592377898323501913600893031125462243864544137924457064402335103533297216916423665234646117145931023997423425896360570742577230737961307217651990219633931169249353511646785207736401166163147037286194903519361549189906052044818132024657973026759400 79

r = 827

As you may imagine, the private key is unknown. The ciphertext C was obtained by encrypting the number associated with the plaintext using the public key.

C =

333409394304627914466114015220094687094651067901835887300970758202496560992410494003284672310096927232105864081450324843934547338154247377774266204247639938588194912188061538430441362246144508321036819587882949069568797125795124012100703423131291342967999169570708555080083425047238818775620557513554248180 16

Unfortunately (but fortunately for you as an attacker), we further know that while n is big, the key generation program was flawed that ended up using one prime number substantially smaller than the other. Write a Python program to help decode the ciphertext to recover the original message.

Send me your answer by emailing LaiY4@cardiff.ac.uk with the title *CM1208 Competition: Weak RSA*. You can use whichever approach you wish to decode the message, but you must attach your Python source code to your email to show how you approached the problem.

The deadline for you to email your solution is **5pm Tuesday Week 7.**

A prize will be awarded on **Thursday** of **Week 7**, with the winner being selected using a virtual raffle during the lecture. A student submitting a correct answer will receive one raffle ticket. Bonus tickets are available for the first correct answer, using a particularly interesting or efficient approach etc.

Hints:

- Although for the two prime numbers that make up n, one prime number is much smaller than the other, it is still fairly big. Further readings on learning central as well as the Week 3 exercises provide useful references for research. You are always encouraged to research this topic further to help come up with an effective solution.
- Although a supercomputer may be helpful, if you use an effective solution, you don't need a supercomputer to solve this problem. A normal desktop/laptop is more than enough! However, do take the scale of the problem into account before writing your code.