1. Suppose we wish to transmit the message “cs2800 rocks” using RSA. Suppose the public key has \( m = pq = 3403 \) and the exponent \( k = 17 \).

Note: for this problem, I used a spreadsheet to do the calculations. If you use calculators or spreadsheets to manipulate very large numbers, you can cause overflow, so make sure you reduce mod \( m \) as necessary to keep the numbers small. To compute \( a^k \) for large \( k \), it helps to write \( k \) in binary, and then use repeated squaring to find \( a \) to a power-of-two power. For example, to compute \( a^{52} \), I write \( 52 = 32 + 16 + 4 \), so \( a^{52} = a^{32} \cdot a^{16} \cdot a^4 \).

(a) Use the mapping

| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 |

convert the message into a string of digits, and break the digits up into groups of threes.

(b) By separately encrypting each block of 3 digits, produce the RSA cyphertext. Add leading zeros to each encrypted block so that each block of cyphertext is 4 digits long.

(c) You have managed to intercept the private key: \( p = 41 \), \( q = 83 \). Use these factors to compute \( \phi(m) \) and \( k^{-1} \). Use the algorithm you derived in question 2 of homework 8 to compute \( k^{-1} \mod \phi(m) \).

(d) Using these values, decrypt the message “0948 3332 1850 2898 2002 2692 0377 1398”.

1/1