Exercises: RSA

Note: For these exercises, you might want to use something like WolframAlpha for the computations: http://www.wolframalpha.com/
For example, to calculate $2^{10} \mod 15$ *type "2^10 mod 15".*

1. Encrypt the word 'lion' using RSA with modulus $m = 1241$ and encryption key $E = 5$. The result will be four numbers between 0 and 1240.

2. (a) We want to create an RSA scheme with two primes $q_1 = 23$ and $q_2 = 179$. What is the modulus m?

   (b) Using this scheme, calculate the value of A.

   (c) Using this scheme, what is the smallest possible choice of encryption key E?

   (d) Use RSA and the smallest encryption key to encrypt the word 'badger'.

3. Decrypt the numbers '178, 163, 92, 161, 0, 106' using RSA with modulus $m = 187$ and decryption key $D = 3$. The resulting numbers should be turned back into letters of the alphabet.

Questions 4 and 5 continue on the next pages.

4. (a) We want to create an RSA scheme with two primes $q_1 = 61$ and $q_2 = 223$. What is the modulus m?

   (b) Using this scheme, calculate the value of A.

   (c) If the encryption key is $E = 1903$, what is the decryption key D?

   (d) Use RSA and the decryption key to decrypt the numbers '12521, 12397, 10139, 99'.

5. (a) We want to create an RSA scheme with two primes $q_1 = 113$ and $q_2 = 257$. What is the modulus m?

   (b) Using this scheme, calculate the value of A.

   (c) If the encryption key is $E = 18847$, what is the decryption key D?

(d) Use RSA and the decryption key to decrypt the numbers '27105, 6618, 0, 2549, 5757, 6496'.