Exercises: Breaking RSA

Note: In these exercises we will encode letters as two-digit numbers, with $a = 00, b = 01, c = 02, \ldots, z = 25$.

Note: The following ciphertexts contain no form of padding, which makes them breakable using the methods described in the course.

Note: We still recommend performing the calculations with something like WolframAlpha, http://wolframalpha.com/

1. (a) Encode the word 'elephant' as two-digit numbers, with $a = 00, b = 01, c = 02, \ldots, z = 25$.

   (b) Split the word into blocks of two letters, and write the numerical values of each block. These should be four numbers between 0000 and 2525.

   (c) Encrypt these blocks using RSA with modulus $m = 2773$ and encryption key $E = 1147$.

2. A stolen ciphertext reads '1015, 2044, 2216'. It was sent using RSA, without padding, and a public key of $m = 2773$ and $E = 1147$.
   Work out the original message using a chosen-plaintext attack. We think the ciphertext is one of four possible words: 'baboon', mongoose', 'rabbit' or 'racoon'.

3. A stolen ciphertext, c_1, reads '0178, 1735, 0903'. It was sent using RSA, without padding, and a public key of $m = 2773$ and $E = 1147$.
   I decide to use a chosen-ciphertext attack, using $x = 2$.

   (a) Show x and m are coprime.

   (b) What is the multiplicative inverse of x modulo m?

(c) What is $x^E \mod m$?

(d) Create a second cipher $c_2 \equiv c_1 x^E \mod m$.

(e) I am able to have c_2 deciphered, and receive the decryption '0061, 0026, 1208'. What was the original message?

4. A stolen ciphertext reads

'0925, 0970, 0087, 1101, 0780, 1241, 0657, 0542, 0364'.

It was sent using RSA, without padding, and a public key of $m = 2773$ and $E = 1147$.

Factorise the modulus and work out the original message.