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 $a = 00, b = 01, c = 02, \ldots, z = 25$.

   plaintext: e l e p h a n t

   in numbers: 04 11 04 15 07 00 13 19

   (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.

   plaintext: el ep ha nt

   in numbers: 0411 0415 0700 1319

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

   plaintext: el ep ha nt

   in numbers: 0411 0415 0700 1319

   $p^E \mod m$: 1816 1429 1225 1511

   Note: The blocks hide the frequency of 'e', and disguise the 'a' which is usually 0.

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'.

   We know the word isn't 'mongoose' as it is too long (not a problem if they had used padding).

   Let encrypt the block 'ra' which is encoded as 1700. This becomes $1700^{1147} \equiv 1015 \mod 2773$. This matches the ciphertext so the word must be 'rabbit' or 'racoon'.

   If we encipher the block 'bb' we get $0101^{1147} \equiv 1353 \mod 2773$. Whereas, the block 'co' becomes $0214^{1147} \equiv 2044 \mod 2773$. So the word must be 'racoon'.

   Indeed, the block 'on' becomes $1413^{1147} \equiv 2216 \mod 2773$ as expected.

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.

   Using Euclid's algorithm, we have

   $$2773 = (1386)(2) + 1$$

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

   Reverse Euclid's algorithm to get:

   $$1 = (-1386)(2) + (1)(2773)$$

   So the inverse of $x = 2$ is $x' \equiv -1386 \equiv 1387 \mod 2773$.

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

$x^E \equiv 2^{1147} \equiv 1134 \mod 2773.$

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

$$c_1\text{: } 0178\ 1735\ 0903$$

$$c_2 \equiv c_1 x^E \mod m\text{: } 2196\ 1423\ 0765$$

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

The decryption is $px \mod m$. We will now multiply by the inverse of x, i.e. multiply by $x' \equiv 1387 \mod 2273$.

$$px \mod m\text{: } 0061\ 0026\ 1208$$

$$pxx' \mod m\text{: } 1417\ 0013\ 0604$$

in letters: or an ge

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.

I will leave this as a final message for you to work out.

If you manage it, send me a message on Udemy for no prizes, except a message of congratulations and a feeling of satisfaction.