MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

UNCONCEALED RSA MESSAGES

Author: Viktor Veselovsky

October 2011

Using the RSA cipher an unconcealed message is a message m with $m^e \equiv m \bmod N$. That means the result of the encryption operation is the same as the given message. The message m is then called a fix point.

The following challenge consists of two steps. In each step a different public key is given and in each case you have to find all unconcealed messages for the particular given public key (N, e).

Among these messages there is one message (after it has been converted to HEX and then to ASCII) that is meaningful in English.

Public Key for Step I

$$N = 27384261392218465951948581266365030771996154549898816740863961927765 9$$

$$e = 15927187472979346850090281166923507769942684104980668468604464157418 61$$

Please determine all unconcealed messages (including the meaningful one), sort them by their numerical value from smallest to biggest, and then reduce their values modulo 11.
This sequence of remainders r_i can serve as verification that you found them all.

Public Key for Step II

$$N = 77782987788421433139022845954774251703141785387536663083574225996062038151688415347445650715632217790299207549041017909076 39$$

$$e = 12919621566387070678528239583265887092956520640891899547295278261267812685459937822689325523230294668071603100 85$$

For the second step of this challenge it is sufficient to determine the only unconcealed message which is a meaningful English sentence.

Formatting of the Solution

The solution is to be provided in the format: m_1,r_1,$r_2 \cdots r_i$,m_2 where

1. m_1 is the meaningful message of the first step,
2. r_1, r_2 to r_i are remainders of all ascendingly sorted unconcealed messages mod 11 from the first step, and
3. m_2 is the meaningful message you found in the second step of this challenge.

Both messages are to be entered in the form of ASCII symbols. There are no spaces before and after the commas.

Hints

For $N = p \cdot q$ and (N,e) as public key:

1. General hint:
   The number of all possible unconcealed messages can be determined by
   $(gcd(e-1, p-1)+1) \cdot (gcd(e-1, q-1)+1)$.
2. Hint for the second step:
   Both the distance between p and a specific square number and the distance between a relatively small multiple of q and the root of the same square number, that was used before, is less than 2.