MysteryTwister C3
A CRYPTO CHALLENGE BY CRYPTOOL

NOT-SO-SECRET MESSAGE FROM MALAWI – PART I (RSA)

by Ed Schaefer

Level II Problem

May 2010

Level II problem by Ed Schaefer

Not-so-secret message from Malawi – Part I.

For RSA to be safe, you need to pick your parameters n and e carefully. I forgot about that when I asked my friend Atipatsa in Malawi to encrypt a message for me using my RSA parameters

N = 316033...
and *e* = 17.

The cipher text he sent is
CT = 655373...

The complete parameters can be found in this additional file: parameters.txt

Find the plaintext number. Turn it into a binary string. The highest order bits are padding. Consider the 200 lowest order bits (this should be the same as dividing by 2^{200} and finding the remainder). That is the plaintext message encoded with ASCII, which is the codeword.

For example:
If the plaintext number were 15030639 = $(11100101\ 01011001\ 01101111)_2$ and I used the 16 lowest order bits 01011001 01101111 then that would be the ASCII encoding of *Yo*.

May 2010

MysteryTwister C3
A CRYPTO CHALLENGE BY CRYPTOOL