MATH 253: CRACK RSA

DAN YASAKI

Be a Bad Guy

I have encrypted one of the answer to the RSA question on Test 3, using public key

$$N = 191147927718986609689229466631454649812986246276667354864188503638807260703436799058776201365135161278134258296128109200046702912984568752800330221777752773957404540495707851421041$$

$$e = 65537$$

I tried to email this to Agent X, who proofreads my tests, but the message was accidentally posted to our class website. It is your turn to be the Bad Guy. You are not the intended receiver, here is a chance to try out your number theory kung-fu.

As a Bad Guy, you must decrypt the message. Once you succeed, you will get a list of integers forming the decrypted message. Understanding the message at this point is easy. Just chop each number into consecutive blocks of size 2, and each block corresponds to a character in ASCII. Python allows you to convert from ASCII to text and back using `chr` and `ord`.

The public key (N, e) and intercepted message are in a text file located at

`http://www.uncg.edu/mat/faculty/d_yasaki/teaching/mat253/documents/secret/yasaki.txt`

where `yasaki` is replaced by your last name (all lowercase).

Good luck, and don't get arrested. (Don't worry. This is not a violation of the UNCG Academic Integrity Policy.)

Department of Mathematics and Statistics, The University of North Carolina at Greensboro, Greensboro, NC 27402-6170, USA

E-mail address: `d_yasaki@uncg.edu`