Project 1: RSA

Due by May 7, 2010

1. This project asks you to develop an RSA-based encryption/decryption program for the integer $n \leq 2147483647$ and $n = pq$ for distinct primes p and q. You need to write "Encryption" and "Decryption" programs separately. You might use the public key $(n, e) = (949327, 517)$, where $n = p \times q = 919 \times 1033$, to report your ciphertexts for the following messages and decrypt them (with $d = 358063$).

(a) *bear*

(b) *kangaroo*

(c) *wombat*

(d) *A koala is not a bear even if its Chinese translation means a bear without a tail*

(e) Longer test messages will be given next week.

You can make a block of 2 letters, 4 letters, or more compact block size.

***2.** Can you extend your program in Problem 1 for n up to 1024 bits?