**Assignment #5 – Repeated Squaring Name: Tanner Waters  
  
RSA Key Generation Algorithm**

(Stamp, p.96) To generate an RSA public and private key pair, do the following:

1. Choose two large prime numbers *p* and *q* and form their product N = *pq*
2. Compute the product (*p* – 1)(*q* – 1)
3. Choose *e* relatively prime to the product (*p* – 1)(*q* – 1)
4. Compute *d*, which is the multiplicative inverse of e, so that *d* = e-1 modulo (*p* – 1)(q – 1)   
   (Note: e\*d modulo (*p* – 1)(q – 1) = 1 modulo (*p* – 1)(q – 1) )

After performing the steps above, the RSA key pair consists of the following: Public key: (N, *e*) Private key: (N, *d*)

Use the *e* value to encrypt and the *d* value to decrypt as shown in these equations: C = M*e* mod N M = C*d* mod N

**Problems to Solve using Repeated Squaring for the Modular Exponentiation (Stamp, p. 98-99)**  
p q N (p – 1)(q – 1) e d Me C Md

3 11 33 2 \* 10 = 20 3 7 15 9 = 153 mod 33 15 = 97 mod 33

11 19 209 10 \* 18 = 180 7 103 94 151 = 947 mod 209 94 = 151103 mod 209

29 37 1,073 28 \* 36= 1,008 5 1613 752 229= 7525 mod 1073 752=2291613 mod 1073

53 79 4,187 52 \* 78= 4056 5 7301 297 3948=2975 mod 4187 297=39487301 mod 4187

13 23 299 12 \* 22= 264 5 317 122 109=1225 mod 299 122=109317 mod 299

17 31 527 16 \* 30 = 480 7 823 387 395=3877 mod 527 395=397823 mod 527

821 953 782,413 820 \* 952= 780,640 3 4647 2 8=23 mod 782,413 2=84647 mod 782,413