## Assignment #5 – Repeated Squaring

**Name:** Brandon Lewis

### 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: $C = M^e \bmod N$ $M = C^d \bmod N$

### Problems to Solve using Repeated Squaring for the Modular Exponentiation (Stamp, p. 98-99)

| p | q | N | (p – 1)(q – 1) | e | d | $M_e$ | C | $M_d$ |
|---|---|---|---|---|---|---|---|---|
| 3 | 11 | 33 | 2 * 10 = 20 | 3 | 7 | 15 | $9 = 15^3 \bmod 33$ | $15 = 9^7 \bmod 33$ |
| 11 | 19 | 209 | 10 * 18 = 180 | 7 | 103 | 94 | $151 = 94^7 \bmod 209$ | $94 = 151^{103} \bmod 209$ |
| 29 | 37 | 1073 | 1008 | 5 | 1613 | 752 | $229 = 752^5 \bmod 1073$ | $752 = 229^{1613} \bmod 1075$ |
| 53 | 79 | 4187 | 4108 | 5 | 7301 | 297 | $3948 = 297^5 \bmod 4187$ | $297 = 3948^{7301} \bmod 4187$ |
| 13 | 23 | 299 | 264 | 5 | 317 | 122 | $109 = 122^5 \bmod 299$ | $122 = 109^{317} \bmod 299$ |
| 17 | 31 | 527 | 480 | 7 | 823 | 387 | $395 = 387^7 \bmod 527$ | $387 = 395^{823} \bmod 527$ |
| 821 | 953 | 782413 | 780640 | 3 | 4647 | 2 | $8 = 2^3 \bmod 782413$ | $2 = 8^{4647} \bmod 782413$ |