Math 341 Final Project

Theo Koss

December 2020

1 Problem 14.1

(i) Produce a pair of keys and a message (a number n).

(a) $p = 17$, $q = 53$. $N = pq = 901$.

(b) $\phi(N) = 16 \cdot 52 = 832$.

(c) Let $e = 3$, check $\gcd(e, p-1) = 1$, and $\gcd(e, q-1) = 1$. Therefore $\gcd(e, \phi(N)) = 1$.

(d) Find d s.t. $ed \equiv 1 \mod \phi(N)$. $d = 555$.
$ed = 555 \cdot 3 = 1665 \equiv 1 \mod 832$.

(e) Public key$=(N, e) = (901, 3)$.
Private key$=(N, d) = (901, 555)$.

(f) Message: $n = 99$.

(ii) Encrypt the message.
$c \equiv n^e \mod N$.
$c \equiv 99^3 = 970299 \equiv 823 \mod 901$. Cyphertext: $c = 823$.

(iii) Decrypt the message.
$c^d \equiv n \mod N$.

$$c^d = 823^{555} = 99^{1665} = 99^{k(16)(52)+1}$$

In this case, $k = 2$ because $2 \cdot (16) \cdot (52) = 1664$. According to Euler's Theorem,

$$n^{\phi(N)} \equiv 1 \mod N$$

Also, in step (b) of part (i), we found

$$\phi(N) = 16 \cdot 52 = 832$$

So,

$$n^{(2 \cdot 16 \cdot 52)+1} = \underbrace{(n^{1664})}_{\equiv 1 \mod N} \cdot (n^1) \mod N = n = 99$$