Andrew Johnson

CS 427 Cryptography

HW5

1) Can you please post the solution to this question? ...

   Thank you!

2) $Take\ u = v = 1, r = 10, s = 2 \qquad Notice\ \gcd(r,s) \neq 1, \gcd(r,s) = 2$

   $x \equiv 1\ (mod\ 10)$
   $x \equiv 0\ (mod\ 2)$

   There is no solution to x. This is because since 2|10 so any number modded by those should be relatively equal in the modded world.

3) (a) $$\varphi(n) = (p-1)(q-1) = pq - p - q + 1$$

$$\varphi(n) = pq - (p+q) + 1 \Rightarrow p + q = N - \varphi(n) + 1$$

$$(x-p)(x-q) = x^2 - (p+q)x + pq$$

$$f(x) = x^2 - (N - \varphi(n) + 1)x + N$$

All we must do is solve $f(x) = 0$ using the quadratic formula which will factor out both p and q.

(b)

Plaintext file with word document