SOEN 321

(Although these questions will be solved with you during the tutorial, you should try solving them by yourself before the tutorial)

Prob. 1

a) Evaluate the following:

gcd(621, 345)	Ans. 69
gcd(11316,1221)	Ans. 3
23^{-1} mod 67	Ans. 35
32^{-1} mod 167	Ans 47

gcd(16,56)
gcd(161,535)
161^{-1} mod 536
16^{-1} mod 533

Prob. 2

Find x that simultaneously satisfy the following congruent equations

a)

$x \equiv 3$ mod 7
$x \equiv 5$ mod 11
$x \equiv 9$ mod 13

Ans. x=269

b)

$x \equiv 2$ mod 7
$x \equiv 3$ mod 11

Ans. x=58

Prob. 3

Consider an RSA system with p=7, q=11 and e=13. Find the plaintext corresponding to c=17.

Ans. d=37 and m=52

Prob. 4

Consider an RSA system in which the attacker knows that n_1 and n_2 has the form $n_1=pq_1=16637$ and $n_2=pq_2=17399$. Show how the attacker can break this system.

Ans. Eve evaluates p=gcd(n1,n2)