SOEN 321
Exercise 1 (With Solution)

Prob. 1 Consider the affine cipher in which the ciphertext c is given by C= a P + b mod 26. The cryptanalyst observed the following plaintext/ciphertext pairs (p,c): (1,10) and (2,17).

1. Recover the key (a,b) used in the encryption system above.
2. What is the ciphertext corresponding to the plaintext p=3?

Answer: a=7, b=3, ciphertext=24

Prob. 2 Consider the Hill cipher in which the ciphertext is related to the plaintext using the form

(c1 c2)= (p1 p2) $\begin{pmatrix} k1 & k2 \\ k3 & k4 \end{pmatrix}$. mod 26

The cryptanalyst observed the following plaintext/ciphertext pairs (p1 p2)/(c1 c2):
(1 2)/(16 23) and (3 3)/(1 16).

Determine the key corresponding to this system.

Key= [2 5]
[7 9]

Prob. 3

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. 4
Find x that simultaneously satisfy the following congruent equations
a)
$x \equiv 3 \bmod 7$
$x \equiv 5 \bmod 11$
$x \equiv 9 \bmod 13$

Ans. x=269

b)
$x \equiv 2 \bmod 7$
$x \equiv 3 \bmod 11$

Ans. x=58

Prob. 5
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. 6
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)