HW3 – Robert Steele

Question 1:

x = -11827825 y = 67318298

Question 2:

((623764469 . 575076109) 623764469 . 120825157)

((776512123 . 233162125) 776512123 . 637040805)

Question 3:

"Put your mask on! There is a deadly pandemic outside.   "

Kamala Harris - (412581307 . 251545759)

I found this by making a list of all the politicians public keys and looping through them to check each public key's validity. Once I found the valid key I called authenticate-and-decrypt to find the message. I could have just manually plugged in each key, but I figured this would be more interesting.

```
(define politicians (list donald-trump-public-key
                          mike-pence-public-key
                          nancy-pelosi-public-key
                          aoc-public-key
                          michael-cohen-public-key
                          ivanka-trump-public-key
                          bernie-sanders-public-key
                          kamala-harris-public-key
                          joe-biden-public-key))
(define (who-sent? message list private-key)
  (if (null? list)
      #f
      (let ((m (authenticate-and-decrypt message (car list) private-key)))
        (if (equal? m #f)
            (who-sent? message (cdr list) private-key)
            (car list)))))
(define mess (signed-message received-mystery-message received-mystery-signature))
(define politician (who-sent? mess politicians joe-biden-private-key))
(authenticate-and-decrypt mess politician joe-biden-private-key)
politician
```

Question 4:

```
(define forged-message1 "I am a TREMENDOUS fan.")
(define forged-message2 "You have small hands.")
(define forged-message3 "This is a message from future you... watch out for ice cubes.")

(define nancy-pelosi-private-key (crack-RSA nancy-pelosi-public-key))
(define bernie-sanders-private-key (crack-RSA bernie-sanders-public-key))

(define message-to-bernie (encrypt-and-sign forged-message1 donald-trump-private-key bernie-sanders-public-key))
(define message-to-trump (encrypt-and-sign forged-message2 nancy-pelosi-private-key donald-trump-public-key))
(define message-to-biden (encrypt-and-sign forged-message3 joe-biden-private-key joe-biden-public-key))

(authenticate-and-decrypt message-to-bernie donald-trump-public-key bernie-sanders-private-key)
(authenticate-and-decrypt message-to-trump nancy-pelosi-public-key donald-trump-private-key)
(authenticate-and-decrypt message-to-biden joe-biden-public-key joe-biden-private-key)
```

Output:

```
"I am a TREMENDOUS fan.  "
"You have small hands.   "
"This is a message from future you... watch out for ice cubes.   "
```

Question 5:

```
(time: 17)
100000000003
(time: 50)
1000000000039
(time: 510)
100000000000031
(time: 1508)
1000000000000037
```

Given that the time cost seems to be tripling as we add digits to prime numbers I calculated that at 50 digits we would see a time cost of around 797475583.46 years and at 100 digits we would see a time cost of around 5.725e+32 years. Which is a long time.