**CS 411 HW4 Solutions**

**1** ) We have the value of the cipher c which we obtained from the server and equals to c = me . We will apply chosen cipher text attack to find the message m for this question. First, we generated a random integer r = 5 and then raise it to the power of e. Then we multiplied that number with our original c and obtained newly created cipher such that: c\_ = (c \* re )Then we sent that c\_ to the server to get the plain text version, and lets call it m\_. Then m\_ = (c \* re )d = cd \* re\*d = m \* r. then we multiplied m\_ with the multiplicative inverse of r to obtain the original m and received “Congrats!” message from the server. The message is b'Bravo: you find it. Your secret code is 64430'

**2)** Since the pin consists of 4 digit numbers, there are 10000 possible values that it can take. Therefore, we can perform exhaustive search to find the value of the pin. So, for each possible value of the pin, we tried all possible 8 bit random numbers and call RSA\_OAEP\_Enc(pin,e,N,random\_number) to check whether the returned value of the function is equals to the value of c. If they are equal, then we found the pin value. The execution time of the code lasts around 27 seconds.

**3)** The flaw in this implementation is that the number of possible k values (2\*\*16) are too small. Therefore, with brute force attack, we can find the value of the secret key k. Once we found the value of the k as 31659, we computed (modinv(h\*\*k,p) \* t) % p, and obtained the message m. The message is b'Why is Monday so far from Friday, and Friday so close to Monday?' The execution time of the code is around 40 seconds.

**4)** First, I computed the hash values of the message1 and message2 using SHA128. Then I performed the following operation to find the value of a which is the private key:

a = ((s2 \* h1 – s1 \* h2) \* modinv((s1 \* r1 – r1 \* s2),q)) % q

The value of the a is: 16887419846051932713464453144375211173350562631553254703155613922671

**5)** In order to find the value of the x, I used brute force attack with x in range 100000.

For each value of x, I performed ((s1 \* h2 – s2 \* h1 \* x) \* modinv((s1 \* r1 \* x – s1 \* s2) % q,q)) % q to find the value of the secret key a. Then I checked whether pow(g,a,p) is equal to the beta for the verification. If they are equal, then we found the actual value of the a. I found the value of the x as 127.

The value of the a is:

384680223193444082342876995407780976557870169632461355085385664072

Efe Şencan 25083