CS 411-507 Cryptography

Homework #4

Yigit Kaan Tonkaz

29154

1)

It does not matter which number we choose so I selected t as 27. We have original cipher and we can also send many ciphertext so we can use following process,

encryption process by taking the power of e of t in mod n

get the adjusted ciphertext c\_

sent c\_ to server to get the new message m\_

decryption process by taking the power of d in mod n

(It is known e\*d = 1 in mod n) which gives the equation that m\_ = r\*m mod n

Then we need to divide m\_ by t to find message

A black and white screen

Description automatically generated

I found the code as 52328 and get the congrats message.

2)

Due to the 4 digit pin, we can brute forcing

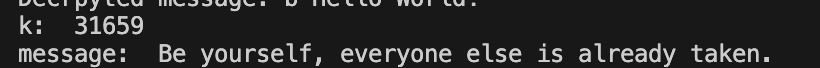
I get this results

A black background with white text

Description automatically generated

3)

We can try brute forcing because numbers are not very large by using g^k modp = r. When we found the same value for r, we can stop.



I found k as 31659 and message “Be yourself, everyone else is already taken.”

4)

We can use this formula to find the message,

m2 = (t2\*m1)/t1 (mod p)

I recover m2 as this message



5)

We can use this formula because the r values are not same,

a = (si\*hj – sj\*hi\*x) (sj\*ri\*x – si\*rj) ^-1 mod q

also we can try brute forcing to find suitable c\_ value

then I test my values and get this result

