TUĞBERK DALKILIÇ

CS411 HW4 REPORT

1. $c = x^e \mod n$ By using this formula, I sent this to the server. And divide to x and transformed to byte representation

2. I factorised the number "n" manually , to find the phi number and secret key d. In decryption function, 4 digit random PIN number has resulted as 6639 successfully.

3. Message is: "Why is Monday so far from Friday, and Friday so close to Monday?

$$g^k \equiv r \quad in \mod p$$

Brute force, i found k. When k is known, then message can be found as below

$$t * h^{-k} \equiv m \; in \mod p$$

4.
Private key:
168874198460519327134644531443752111733505626315532547031556139226 71

$$a \equiv (s_i h_j - s_j h_i) * (r * (s_j - s_i))^{-1} in \mod q$$

5.

$$a \equiv (s_i hj - s_j h_i x) * (s_j r_i x - s_i r_j)^{-1} \; in \; \mod q$$

Since random number run out, $k_j = x\, k_i$, x should be such that, private key equals to public key beta.