**CS411/507 HW#4**

**Melih Utku Eksi, 23841,** [**mutku@sabanciuniv.edu**](mailto:mutku@sabanciuniv.edu)

**Q1)** Here we know that encrypted PIN has 4 digits. We need to find the R value that corresponds to the encryption function where R equals a random integer between 2\*\*7 and 2\*\*8 – 1 (k0 = 8 and R = random.randint(2\*\*(k0-1), 2\*\*k0 - 1).

So, we can apply brute force to get the PIN. Trying every possible R and every possible PIN between 1000 – 9999 and checking if they are equal to the given ciphertext using encryption function.

R is 157 and PIN is 5377.

**Q2)** In the encryption function, k is given a random integer between 1 and 2\*\*16 – 1. Since we know the values of g, p and r, we can apply brute force to find out k.

Found k = 17106. After that the second missing piece modular inverse of h\*\*k. Now we know the values h, k and p applying modinv function we can find inverse of h\*\*k which equals 21544490089832216808308331319858540081496426686327159697934566494456896122678783934289942511159118535387215740734123568454049466127172977648991549952804928046015294301116475551022590359054101472806177602513365484586670572061046115461644803844036767259566663632888024277264102550943997457333378166275287252966.

Now we can go for the message and converting it into bytes will give us the plaintext. m = (inverse of h\*\*k times t) mod p.

This gives us m equals 3356366513591938179202454688524890539966506364615741171676962160942064295810867763650735855139356337022790316030665447642707682606.

Converting it to the bytes give us the message which is

b'My favorite machine at the gym is the vending machine.'

**Q3)** **:** This symbol represents the ticket between Cliff who is client and Grant which is the ticket granting server. After Cliff logins to the system, Grant issues Cliff a ticket in order to use a particular service which is specified as S in the response. Ticket has the information, from which Cliff and Simon generates a shared key. If the identity of the server was not included, then Cliff can use the ticket for any server maybe for servers for which he did not have authorization to access.

**Q5)** From the last lecture slide of ch10\_handout, we can see how to find alfa. Using the last equation, I found the alfa value = 482061878283805054797834433118192109249147480995.

In that equation hi and hj values are missing. To compute those values, I used the pow(g, si(or sj), p) from the KeyGen function.

Lastly, with the given Sig\_Ver function, I checked those alfa values if the signature verified or not. In conclusion they verified.