# CENG471 CRYPTOGRAPHY REPORT


## İlayda Özel 260201037
## Göktay İncekara 250201012


**Q1)** No.

**Q2)**

The Diffie-Hellman method is a way for two users to exchange encrypted data. It is not an encryption algorithm, it is a key-exchange algorithm. With the help of this algorithm, both users obtain a secret value. Even the Diffie-Hellman approach is followed by RSA, an asymmetric algorithm implementation of public-key cryptography. If Diffie Hellman was an encryption algorithm, then RSA would not need to use the Diffie-Hellman, because RSA itself is a data encryption algorithm.

**Q3)**

You should remove your lock and send the gift to your friend again with your friend's lock on it.

If we inspect the whole scenario: In the first transport, the gift won't be opened by the intruders thanks to your key, and on the way back to you, it won't be opened by anyone thanks to your and your friend's key. When you take the gift, remove your lock and send it again to your friend, again the intruders won't be able to open the gift because it still has the lock which belongs to your friend. In the third transport, when your friend takes the gift and removes his or her lock, now she or he will be able to open your gift and you both can be sure that there are no intruders looking or taking it.

**Q4)**

In the given scenario, if my key or my friend's key are not complex and hard enough, the attacker can break the keys or one of the keys and open your gift. If the key is made of metal, the attacker can make himself the key. The keys must be hard to forge and complex to avoid any fraud. If the key is a number combination key, the attacker can crack the code by guessing the

number. The secret number combination must be complex and hard to guess. Therefore, we should select our keys according to these risks.

If the intruder (carrier) obtains the keys in some way (either yours or your friend's), he or she will be able to open your gift in the way. If he has both of the keys he can open the gift even with both of the keys on it. If he has only one of the keys, he can open the gift at the first time that you send it or he can open it when you remove your key and send it to your friend.

If the environment is not suitable for transmission, the box can be damaged. In that way our key algorithm will be useless because our environment will fail to transmit our gift.

If the process of the transmission is not suitable, the box again can be damaged. In that way our key algorithm will be useless because the gift is not transmitted in a proper way.

The box might not be delivered to one of the parties for any reason. It might get lost or might get stolen. In this scenario, my friend won't be able to open the gift.