Student Number: 270201072
Student Number: 290201098

-CENG 471 HOMEWORK-2 REPORT-

1.) After we receive the gift with two locks, we may now unlock our lock, and send it back to our friend. They will be the only one with the key to open the gift

2.) The problem is, we don't exactly know whether it was our friend that locked the gift. A man in the middle may have read the note, locked the gift, and sent it back to us to steal it.

3.) Because in Diffie-Hellman key exchange key is not shared explicitly, both the sender and receiver generates their own private keys and compute their own public keys by using publicly known elements p (modulo) and g (generator). Then send their public keys to each other. When they take modular exponentiation with their private keys as exponent and public keys as base values, they will calculate the same shared secret key implicitly.

4.) No, DES is now considered as legacy encryption algorithm, even if Triple DES provides better security if properly configured it is also outdated due to its internal function similarity (Feistal function) and this sturcture is vulnerable to cryptanalitic attacks. Main reason that the DES is not a standard encryption algorithm anymore is that it uses small key sizes like 56 bits which is vulnerable to brute-force attacks with todays computational power. Today it is mostly replaced by AES as a standard by NIST.