**SENDING A MESSAGE CONFIDENTIALLY – PUBLIC / PRIVATE KEY ENCRYPTION**

Consider Alice wants to send Bob a message. Both of them already decided on their symmetric key. Each have their own public and private key pairs.

This how I would advise Alice to send the message to attain confidentiality.

Alice should first encrypt the private key using Pub\_key\_bob, hence she gets Pub\_key\_bob(symmetric \_key). This is taken as part 1. The message is encrypted using the private key, getting symmetric \_key(Message), which can be taken as part 2.

Part 1 and 2 is sent to Bob and he decrypts 1 first using his private\_key so as to get the symmetric key which is then used to get the message. Integrity of the message can also be tested by making Alice send a hash of the message , encrypting it and sending it along with part 2, basically as a digital signature.

By

Nihal Haneef

16CO128