Project Report 2 - Group20

Chap 1 Usage

1. When played as Master

Master can find master\_sign.py and master\_view.py in the folder “master”.

① Master can generate the RSA private and public key with master\_sign.py and command “generate\_key”. The private key will be stored in the folder “master”, the private key will be stored in the folder “pastebot.net”.

② Master can sign the file stored in the folder “pastebot.net” with master\_sign.py and command “sign”. Before signing, make sure the private key has been already stored in the folder “master”.

③ Master can view the valuables uploaded by bots with master\_view.py. Before viewing, make sure the private key has been already stored in the folder “master”.

2. When played as Bot

Bot can find bot.py in the folder “bot”. Before running the code as Bot, make sure that Master has already generate the public key and store it in the pastebot.net.

Chap 2 Method Used

Our group use RSA PKCS#1 as our valuable encryption method. Master can generate the public and private key with 2048 bits. Bot will encrypt the valuables with the public key. Master can decrypt the valuables with the private key.

Our group also use RSA PKCS#1 as our digital signature method. Only Master can use the private key to sign the files stored in the pastebot.net. Bot can verify if this file is signed by Master with the public key stored in the pastebot.net.