Asymmetric key cryptography or public key cryptography

#Lets see how the public key cryptography works.

#before that the lines starting with ‘#’ represents comment lines, which means not to considered as a part of code.

#i write the details of code and what it does in the comment lines.

#and the lines starting with the ‘$’ symbol indicates it is the code line, which is to be executed.

# lets start.

#creating a file in linux terminal called testfile.txt.

$touch testfile.txt

#to see the created file.

$ls

#writing something(write what ever you want here iam writing “HEY! THIS IS VINAY”) into the file that we just created using nano text editor.

$nano testfile.txt

#the above command opens the testfile.txt in edit mode write the statement “HEY! IAM VINAY”, let this be the message that you wanna send to the other person. To save it press(ctrl+s). to exit from editing press(ctrl+x).

#now generating the rsa key using des3 algorithm and saving it in to the file called private.key.

$openssl genrsa -des3 -out private.key

#the above command generates the rsa keys using des3 algorithm and stores it in the private.key.

#now it asks for the pass phrase for private.key give anything you want and remember it.(lets we gave “kali” here).

#now generating public key

$openssl rsa -in private.key -pubout-out public.key

#now type ls command you can see there are two keys one is private and other one is public key.

#lets encrypt the file named testfile.txt and store the bunch of random ascii vales in encryptedfile.txt.

$openssl rsautl -encrypt -pubin -inkey public.key -in testfile.txt -out encryptedfile.txt

#you cann’t see what is the file after encrypted unless you have the proper key to decrypt it.

#to see type the command cat encryptedfile.txt.

#now assume that file(encryptedfile.txt) to you from your friend who wanted to send some message to you.

#so decrypt it by the command below.

$openssl rsautl -decrypt -inkey private.key -in encryptedfile.txt -out decryptedfile.txt

#the above command decrypts the message using private key and stores it in the file called decyptedfile.txt.

#now lets see what is the message that is sent you from your frined.

$cat decryptedfile.txt

#the output for the above command will be HEY! THIS IS VINAY

KEEPING ALL THE COMMANDS TOGETHER

$touch testfile.txt

$nano testfile.txt

$openssl genrsa -des3 -out private.key

$openssl rsa -in private.key -pubout -out public.key

$openssl rsautl -encrypt -pubin -inkey public.key -in testfile.txt -out encyptedfile.txt

$openssl rsautl -decrypt -inkey private.key -in encryptedfile.txt -out decryptedfile.txt

$cat decryptedfile.txt

So yeah this is the sample how public key cryptography works.

Thankyou…