Lab 4: Asymmetric (Public) Key

Objective: The key objective of this lab is to provide a practical introduction to public key encryption, and with a focus on RSA and Elliptic Curve methods. This includes the creation of key pairs and in the signing process.

🕮 **Video demo:** https://youtu.be/6T9bFA2nl3c

A RSA Encryption

A.1 The following defines a public key that is used with PGP email encryption:


```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2

mQENBFTzi1ABCADIEWchOyqRQmU4AyQAMj2Pn68Sqo9lTPdPcItwo9LbTdv1YCFz
w3qLlp2RORMP+Kpdi92CIhdUYHDmZfHZ3IWTBgo9+y/Np9UJ6tNGocrgsq4xWz15
4vX4jJRddC7QySSh9UxDpRWf9sgqEv1pah136r95ZuyjC1EXnoNxdLJtx8PliCXc
hV/v4+KfOyzYh+HDJ4xP2bt1S07dkasYZ6cA7BHYi9k4xgEwxVvYtNjSPjTsQY5R
cTayXveGafuxmhSauZKiB/2TFErjEt49Y+p07tPTLX7bhMBVbUvojtt/JeUKV6vK
R82dmOd8seUvhwOHYB0JL+3S7PgFFsLo1NV5ABEBAAG0LkJpbGwgQnVjaGFuYW4g
KE5vbmUpIDx3LmJ1Y2hhbmFuQG5hcGllci5hYy51az6JATkEEwECACMFAlTzi1AC
GwMHCwkIBwMCAQYVCAIJCgsEFgIDAQIeAQIXgAAKCRDsAFZRGtdPQi13B/9KHeFb
l1AxqbafFGRDEvx8UfPnEww4FFqWhcr8RLWyE8/COlUpB/5AS2yvojmbNFMGzURb
LGf/u1LVH0a+NHQu57u8Sv+g3bBthEPh4bKaEzBYRS/dYHOx3APFyIayfm78JVRF
zdeTOOf6PaXUTRx7iscCTkN8DUD3lg/465ZX5aH3HWFFX50OJSPStO/udqjoQuAr
WA5JqB//g2GfzZe1UzH5Dz3PBbJky8GiIfLmOOXSEIgAmpvc/9NjzAgjOW56n3Mu
sjVkibc+lljw+rOo97CfJMppmtcOvehvQv+KG0LZnpibiWVmM3vT7E6kRy4gEbDu
enHPDqhsvcqTDqaduQENBFTzi1ABCACzpJgZLK/sge2rMLURUQQ6lO2UrS/GilGC
ofq3WPnDt5hEjarwMMwN65PbODjOi7vnorhL+fdb/J8b8QTiyp7iO3dZVhDahcQ5
8afvCjQtQstY8+K6kZFzQOBgyOS5rHAKHNSPFq45MlnPo5aaDvP7s9mdMILITvlb
CFhcLoC6Oqy+JoaHupJqHBqGc48/5NU4qbt6fB1AQ/H4M+6og4OozohgkQb8OHox
YbJV4sv4vYMULd+FKOg2RdGeNMM/aWdqYo90qb/W2aHCCyXmhGHEEuok9jbc8cr/
xrWLOgDwlWpad8RfQwyVU/VZ3Eg3OseL4SedEmwOO
cr15XDIs6dpABEBAAGJAR8E
GAECAAkFAlTzi1ACGwwACgkQ7ABWURrXT0KZTgf9FUpkh3wv7aC5M2wwdEjt0rDx
nj9kxH99hhuTX2EHXuNLH+SwLGHBq5O2sq3jfP+owEhs8/EzOj1/fSKIqAdlz3mB
dbqWPjzPTY/m0It+wv3epOM75uWjD35PF0rKxxZmEf6SrjZD1sk0B9bRy2v9iWN9
9ZkuvcfH4vT++PognQLTUqNx0FGpD1agrG0lXSCtJWQXCXPfWdtbIdThBgzH4flZ
ssAIbCaBlQkzfbPvrMzdTIP+AXg6++K9SnO9N/FRPYzjUSEmpRp+ox31WymvczcU
RmyUquF+/zNnSBVgtY1rzwaYi05XfuxG0WHVHPTtRyJ5pF4HSqiuvk6Z/4z3bw==
=ZrP+
-----END PGP PUBLIC KEY BLOCK-----
```


Using the following Web page, determine the owner of the key, and the ID on the key:

https://asecuritysite.com/encryption/pgp1

By searching on-line, can you find the public key of three famous people, and view their key details, and can you discover some of the details of their keys (eg User ID, key encryption method, key size, etc)?

By searching on-line, what is an ASCII Armored Message?

Save the public key to your Ubuntu instance mypub.asc, and run:

```
gpg mykey.asc
```

What details can you get from the key:

A.2 Bob has a private RSA key of:


```
MIICXAIBAAKBgQCwgjkeoyCXm9v6VBnUi5ihQ2knkdxGDL3GXLIUU43/froeqk7q9mtxT4AnPAaDX3f2r4STZYYiqXGsH
CUBZcI9OdvZf6YiEM5OY2jgsmqBjf2Xkp/8HgN/XDw/wD2+zebYGLLYtd2u3GXx9edqJ8kQcU9LaMH+ficFQyfq9UwTjQ
IDAQABAoGAD7L1a6Ess+9b6G7OgTANWkKJpshVZDGb63mxKRepaJEX8sRJEqLqOYDNsC+pkKO8IsfHreh4vrp9bsZuECr
B1OHSjwDBOS/fm3KEWbsaaXDUAu0dQg/JBMXAKzeATreoIYJItYgwzrJ++fuquKabAZumvOnWJyBIs2z1O3kDz2ECQQDn
n3JpHirmgVdf81yBbAJaXBXNIPzOcCth1zwFAs4EvrE35n2HvUQuRhy3ahUKXsKX/bGvWzmC2O6kbLTFEygVAkEAwxXZn
PkaAY2vuoUCN5NbLZgegrAtmU+U2woa5A0fx6uXmShqxo1iDxEC71FbNIgHBg5srsUyDj3OsloLmDVjmQJAIy7qLyOA+s
Cc6BtMavBgLx+bxCwFmsoZHOSX3l79smTRAJ/HY64RREIsLIQ1q/yW7IWBzxQ5WTHgliNZFjKBvQJBAL3t/vCJwRzOEbs
5FaB/8UwhhsrbtXlGdnkOjIGsmVOvHSf6poHqUiay/DV88pvhN11ZG8zHpeUhnaQccJ9ekzkCQDHHG9LYCOqTgsyYms//
cW4sv2nuOE1UezTjUFeqOlsgO+WN96b/M5gnv45/Z3xZxzJ4HOCJ/NRwxNOtEUkw+zY=
```


And receives a ciphertext message of:


```
Pob7AQZZSml618nMwTpx3V74N45x/rTimUQeTl0yHq8FOdsekZgOT385Jls1HUzWCx6ZRFPFMJ1RNYR2Yh7AkQtFLVx9l
YDfb/Q+SkinBIBX59ER3/fDhrVKxIN4S6h2QmMSRblh4KdVhyY6cOxu+g48Jh7TkQ2Ig93/nCpAnYQ=
```


Using the following code:

```
from Crypto.PublicKey import RSA
from Crypto.Util import asn1
from base64 import b64decode

msg="Pob7AQZZSml618nMwTpx3V74N45x/rTimUQeTl0yHq8FOdsekZgOT385Jls1HUzWCx6ZRFPFMJ1RNYR2Yh7AkQtF
LVx9lYDfb/Q+SkinBIBX59ER3/fDhrVKxIN4S6h2QmMSRblh4KdVhyY6cOxu+g48Jh7TkQ2Ig93/nCpAnYQ="
privatekey =
'MIICXAIBAAKBgQCwgjkeoyCXm9v6VBnUi5ihQ2knkdxGDL3GXLIUU43/froeqk7q9mtxT4AnPAaDX3f2r4STZYYiqXGs
HCUBZcI9OdvZf6YiEM5OY2jgsmqBjf2Xkp/8HgN/XDw/wD2+zebYGLLYtd2u3GXx9edqJ8kQcU9LaMH+ficFQyfq9UwTj
QIDAQABAoGAD7L1a6Ess+9b6G7OgTANWkKJpshVZDGb63mxKRepaJEX8sRJEqLqOYDNsC+pkKO8IsfHreh4vrp9bsZuEC
rB1OHSjwDBOS/fm3KEWbsaaXDUAu0dQg/JBMXAKzeATreoIYJItYgwzrJ++fuquKabAZumvOnWJyBIs2z1O3kDz2ECQQD
nn3JpHirmgVdf81yBbAJaXBXNIPzOcCth1zwFAs4EvrE35n2HvUQuRhy3ahUKXsKX/bGvWzmC2O6kbLTFEygVAkEAwxXZ
nPkaAY2vuoUCN5NbLZgegrAtmU+U2woa5A0fx6uXmShqxo1iDxEC71FbNIgHBg5srsUyDj3OsloLmDVjmQJAIy7qLyOA+
sCc6BtMavBgLx+bxCwFmsoZHOSX3l79smTRAJ/HY64RREIsLIQ1q/yW7IWBzxQ5WTHgliNZFjKBvQJBAL3t/vCJwRzOEb
s5FaB/8UwhhsrbtXlGdnkOjIGsmVOvHSf6poHqUiay/DV88pvhN11ZG8zHpeUhnaQccJ9ekzkCQDHHG9LYCOqTgsyYms/
/cW4sv2nuOE1UezTjUFeqOlsgO+WN96b/M5gnv45/Z3xZxzJ4HOCJ/NRwxNOtEUkw+zY='

keyDER = b64decode(privatekey)
keys = RSA.importKey(keyDER)

dmsg = keys.decrypt(b64decode(msg))
print dmsg
```

What is the plaintext message that Bob has been sent?

Note: You may have to install Pycrypto if this example, to do so apply the following command:

```
pip install pycrypto
```

A.3 On your VM, go into the ~/.ssh folder. Now generate your SSH keys:

```
ssh-keygen -t rsa -C "your email address"
```

The public key should look like this:


```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDLrriuNYTyWuC1IW7H6yea3hMV+rm029m2f6IddtlImHrOXjNwYyt4Elkkc7AzO
y899C3gpx0kJK45k/CLbPnrHvkLvtQ0AbzWEQpOKxI+tW06PcqJNmTB8ITRLqIFQ++ZanjHWMw2Odew/514y1dQ8dccCO
uzeGhL2Lq9dtfhSxx+1cBLcyoSh/lQcs1HpXtpwU8JMxWJl409RQOVn3gOusp/P/0R8mz/RWkmsFsyDRLgQK+xtQxbpbo
```

```
dpnz5lIOPWn5LnT0si7eHmL3WikTyg+QLZ3D3m44NCeNb+bOJbfaQ2ZB+lv8C3OxylxSp2sxzPZMbrZWqGSLPjgDiFIBL
w.buchanan@napier.ac.uk
```


View the private key. What is the **DEK-Info** part, and how would it be used to protect the key, and what information does it contain?

On your Ubuntu instance setup your new keys for ssh:

```
ssh-add ~/.ssh/id_git
```

Now create a Github account and upload your public key to Github (select Settings-> **New SSH key** or **Add SSH key**). Create a new repository on your GitHub site, and add a new file to it. Next go to your Ubuntu instance and see if you can clone of a new directory:

```
git clone ssh://git@github.com/<user>/<repository name>.git
```

If this doesn't work, try the https connection that is defined on GitHub.

B OpenSSL (RSA)

We will use OpenSSL to perform the following:

No	Description	Result
B.1	First we need to generate a key pair with: `openssl genrsa -out private.pem 1024` This file contains both the public and the private key.	What is the type of public key method used: How long is the default key: Use the following command to view the keys: `cat private.pem`
B.2	Use following command to view the output file: `cat private.pem`	What can be observed at the start and end of the file:
B.3	Next we view the RSA key pair: `openssl rsa -in private.pem -text`	Which are the attributes of the key shown:

		Which number format is used to display the information on the attributes:
B.4	Let's now secure the encrypted key with 3-DES: `openssl rsa -in private.pem -des3 -out key3des.pem`	Why should you have a password on the usage of your private key?
B.5	Next we will export the public key: `openssl rsa -in private.pem -out public.pem -outform PEM -pubout`	View the output key. What does the header and footer of the file identify?
B.6	Now create a file named "myfile.txt" and put a message into it. Next encrypt it with your public key: `openssl rsautl -encrypt -inkey public.pem -pubin -in myfile.txt -out file.bin`	
B.7	And then decrypt with your private key: `openssl rsautl -decrypt -inkey private.pem -in file.bin -out decrypted.txt`	What are the contents of decrypted.txt

B.8	What can you observe between these two commands for differing output formats:
	
	`openssl rsautl -encrypt -inkey public.pem -pubin -in myfile.txt -out file.bin`
	
	`cat file.bin`
	
	and:
	
	`openssl rsautl -encrypt -inkey public.pem -pubin -in myfile.txt -out file.bin -hexdump`
	
	`cat file.bin`
		What can you observe in the different of the output files:

C OpenSSL (ECC)

Elliptic Curve Cryptography (ECC) is now used extensively within public key encryption, including with Bitcoin, Ethereum, Tor, and many IoT applications. In this part of the lab we will use OpenSSL to create a key pair. For this we generate a random 256-bit private key (*priv*), and then generate a public key point (*priv* multiplied by G), using a generator (*G*), and which is a generator point on the selected elliptic curve.

No	Description	Result
C.1	First we need to generate a private key with: `openssl ecparam -name secp256k1 -genkey -out priv.pem` The file will only contain the private key, as we can generate the public key from this private key. Now use "`cat priv.pem`" to view your key.	Can you view your key?
C.2	We can view the details of the ECC parameters used with: `openssl ecparam -in priv.pem -text -param_enc explicit -noout`	Outline these values: Prime (last two bytes): A: B: Generator (last two bytes): Order (last two bytes):
C.3	Now generate your public key based on your private key with: `openssl ec -in priv.pem -text -noout`	How many bits and bytes does your private key have: How many bit and bytes does your public key have (Note the 04 is not part of the elliptic curve point): What is the ECC method that you have used?

If you want to see an example of ECC, try here: https://asecuritysite.com/encryption/ecc

D Elliptic Curve Encryption

D.1 In the following Bob and Alice create elliptic curve key pairs. Bob can encrypt a message for Alice with her public key, and she can decrypt with her private key. Copy and paste the program from here:

https://asecuritysite.com/encryption/elc

Code used:

```
import OpenSSL
import pyelliptic

secretkey="password"
test="Test123"

alice = pyelliptic.ECC()
bob = pyelliptic.ECC()

print "++++Keys++++"
print "Bob's private key: "+bob.get_privkey().encode('hex')
print "Bob's public key: "+bob.get_pubkey().encode('hex')

print
print "Alice's private key: "+alice.get_privkey().encode('hex')
print "Alice's public key: "+alice.get_pubkey().encode('hex')


ciphertext = alice.encrypt(test, bob.get_pubkey())

print "\n++++Encryption++++"

print "Cipher: "+ciphertext.encode('hex')

print "Decrypt: "+bob.decrypt(ciphertext)

signature = bob.sign("Alice")

print
print "Bob verified: "+ str(pyelliptic.ECC(pubkey=bob.get_pubkey()).verify
(signature, "Alice"))
```

For a message of “Hello. Alice”, what is the ciphertext sent (just include the first four characters):

How is the signature used in this example?

D.2 Let’s say we create an elliptic curve with $y^2 = x^3 + 7$, and with a prime number of 89 ($y^2 = x^3 + 7 \pmod{89}$), generate the first five (x,y) points for the finite field elliptic curve. You can use the Python code at the following to generate them:

https://asecuritysite.com/encryption/ecc_points_real
(or for simpler code you can use https://asecuritysite.com/encryption/ecc_points3)

First five points:

D.3 Elliptic curve methods are often used to sign messages, and where Bob will sign a message with his private key, and where Alice can prove that he has signed it by using his public key. With ECC, we can use ECDSA, and which was used in the first version of Bitcoin. Enter the following code:

```
from ecdsa import SigningKey,NIST192p,NIST224p,NIST256p,NIST384p,NIST521p,SECP256k1
```

```
import base64
import sys

msg="Hello"
type = 1
cur=NIST192p

sk = SigningKey.generate(curve=cur)

vk = sk.get_verifying_key()

signature = sk.sign(msg)

print "Message:\t",msg
print "Type:\t\t",cur.name
print "========================"

print "Signature:\t",base64.b64encode(signature)

print "========================"

print "Signatures match:\t",vk.verify(signature, msg)
```

What are the signatures (you only need to note the first four characters) for a message of "Bob", for the curves of NIST192p, NIST521p and SECP256k1:

NIST192p:

NIST521p:

SECP256k1:

By searching on the Internet, can you find in which application areas that SECP256k1 is used?

What do you observe from the different hash signatures from the elliptic curve methods?

E RSA

E.1 A simple RSA program to encrypt and decrypt with RSA is given next. Prove its operation:

```
import rsa
(bob_pub, bob_priv) = rsa.newkeys(512)
ciphertext = rsa.encrypt('Here is my message', bob_pub)
message = rsa.decrypt(ciphertext, bob_priv)
print(message.decode('utf8'))
```

Remember to install "rsa" with "pip install rsa". Now add the lines following lines after the creation of the keys:

```
print bob_pub
print bob_priv
```

Can you identify what each of the elements of the public key (e,N), the private key (d,N), and the two prime number (p and q) are (if the numbers are long, just add the first few numbers of the value):   When you identity the two prime numbers (p and q), with Python, can you prove that when they are multiplied together they result in the modulus value (N): Proven Yes/No

E.2 We will follow a basic RSA process. If you are struggling here, have a look at the following page:

https://asecuritysite.com/encryption/rsa

First, pick two prime numbers:

p= q=

Now calculate N (p.q) and PHI [(p-1).(q-1)]:

N= PHI =

Now pick a value of *e* which does not share a factor with PHI [gcd(PHI,e)=1]:

e=

Now select a value of d, so that (e.d) (mod PHI) = 1:
[Note: You can use this page to find *d*: https://asecuritysite.com/encryption/inversemod]

d=

Now for a message of M=5, calculate the cipher as:

$C = M^e \pmod N =$

Now decrypt your ciphertext with:

$M = C^d \pmod N =$

Did you get the value of your message back (M=5)? If not, you have made a mistake, so go back and check.

Now run the following code and prove that the decrypted cipher is the same as the message:

```
p=11
q=3
N=p*q
PHI=(p-1)*(q-1)
e=3
for d in range(1,100):
        if ((e*d % PHI)==1): break
print e,N
print d,N
M=4
cipher = M**e % N
print cipher
message = cipher**d % N
print message
```

Select three more examples with different values of p and q, and then select e in order to make sure that the cipher will work:

E.3 In the RSA method, we have a value of e, and then determine d from (d.e) (mod PHI)=1. But how do we use code to determine d? Well we can use the Euclidean algorithm. The code for this is given at:

https://asecuritysite.com/encryption/inversemod

Using the code, can you determine the following:

Inverse of 53 (mod 120) =

Inverse of 65537 (mod 1034776851837418226012406113933120080) =

Using this code, can you now create an RSA program where the user enters the values of p, q, and e, and the program determines (e,N) and (d,N)?

E.3 Run the following code and observe the output of the keys. If you now change the key generation key from ‘PEM’ to ‘DER’, how does the output change:

```
from Crypto.PublicKey import RSA

key = RSA.generate(2048)

binPrivKey = key.exportKey('PEM')
binPubKey =  key.publickey().exportKey('PEM')
```

```
print binPrivKey
print binPubKey
```

F PGP

F.1 The following is a PGP key pair. Using https://asecuritysite.com/encryption/pgp, can you determine the owner of the keys (or use **gpg mykey.key**):


```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: OpenPGP.js v4.4.5
Comment: https://openpgpjs.org

xk0EXEOYvQECAIpLP8wfLxzgcolMpwgzcUzTlHOicggOIyuQKsHM4XNPugzU
X0NeaawrJhfi+f8hDRojJ5Fv8jBIOm/KwFMNTT8AEQEAAc0UYmlsbCA8Ymls
bEBob21lLmNvbT7CdQQQAQgAHwUCXEOYvQYLCQcIAwIEFQgKAgMWAgECGQEC
GwMCHgEACgkQoNsXEDYt2ZjkTAH/b6+pDfQLi6zg/Y0tHS5PPRv1323cwoay
vMcPjnWq+VfiNyXzY+UJKR1PXskzDvHMLOyVpUcjle5ChyT5LOw/ZM5NBFxD
mL0BAgDYlTsT06vVQxu3jmfLzKMAr4kLqqIuFFRCapRuHYLOjw1gJZS9p0bF
S0qS8zMEGpN9QZxkG8YEcH3gHxlrvALtABEBAAHCXwQYAQgACQUCXEOYvQIb
DAAKCRCg2xcQNi3ZmMAGAf9w/XazfELDG1W35l2zw12rKwM7rK97aFrtxz5W
XwA/5gqoVP0iQxklb9qpX7RVd6rLKu7zoX7F+sQod1sCWrMw
=cXT5
-----END PGP PUBLIC KEY BLOCK-----

-----BEGIN PGP PRIVATE KEY BLOCK-----
Version: OpenPGP.js v4.4.5
Comment: https://openpgpjs.org

xcBmBFxDmL0BAgCKSz/MHy8c4HKJTKcIM3FM05R9InIIDiMrkCrBzOFzT7oM
1F9DXmmsKyYX4vn/IQ0aIyeRb/IwSNJvysBTDU0/ABEBAAH+CQMIBNTT/OPv
TJzgvF+fLOsLsNYP64QfNHav5O744y0MLV/EZT3gsBwO9v4XF2SsZj6+EHbk
O9gWi31BAIDgSaDsJYf7xPOhp8iEWWwrUkC+jlGpdTsGDJpeYMIsVVv8Ycam
Og7MSRsL+dYQauIgtVb3dloLMPtuL59nVAYuIgD8HXyaH2vsEgSZSQn0kfvF
+dWeqJxwFM/uX5PVKcuYsroJFBEO1zas4ERfxbbwnsQgNHpjdIpueHx6/4EO
b1kmhOd6UT7BamubY7bcma1PBSv8PH31Jt8SzRRiaWxsIDxiaWxsQGhvbWUu
Y29tPsJ1BBABCAAfBQJcQ5i9BgsJBwgDAgQVCAoCAxYCAQIZAQIbAwIeAQAK
CRCg2xcQNi3ZmORMAf9vr6kN9AuLrOD9jS0dLk89G/XfbdzChrK8xw+Odar5
V+I3JfNj5QkpHU9eyTMO8cws7JWlRyOV7kKHJPks7D9kx8BmBFxDmL0BAgDY
lTsT06vVQxu3jmfLzKMAr4kLqqIuFFRCapRuHYLOjw1gJZS9p0bFS0qS8zME
GpN9QZxkG8YEcH3gHxlrvALtABEBAAH+CQMI2Gyk+BqVOgzgZX3C80JRLBRM
T4sLCHOUGlwaspe+qatOVjeEuxA5DuSs0bVMrw7mJYQZLtjNkFAT92lSwfxY
gavS/bILlw3QGA0CT5mqijKr0nurKkekKBDSGjkjVbIoPLMYHfepPOju1322
Nw4V3JQO4LBh/sdgGbRnwW3LhHEK4Qe70cuiert8C+S5xfG+T5RWADi5HR8u
UTyH8x1h0ZrOF7K0Wq4UcNvrUm6c35H6lClC4Zaar4JSN8fZPqVKLlHTVcL9
lpDzXxqxKjSO5KXXZBh5wl8EGAEIAAkFAlxDmL0CGwwACgkQoNsXEDYt2ZjA
BgH/cP12s3xCwxtVt+Zds8NdqysDO6yve2ha7cc+Vl8AP+YKqFT9IkMZJW/a
qV+0VXeqyyru86F+xfrEKHdbAlqzMA==
=5NaF
-----END PGP PRIVATE KEY BLOCK-----
```


F.2 Using the Node.js code at the following link, generate a key:

https://asecuritysite.com/encryption/openpgp

F.3 An important element in data loss prevention is encrypted emails. In this part of the lab we will use an open source standard: PGP.

In this challenge, you should install a random number generator on your system with:

```
sudo apt-get install rng-tools
```

No	Description	Result
1	Create a key pair with (RSA and 2,048-bit keys): `gpg --gen-key`	

	Now export your public key using the form of:
	
	`gpg --export -a "Your name" > mypub.key`
	
	Now export your private key using the form of:
	
	`gpg --export-secret-key -a "Your name" > mypriv.key`
		How is the randomness generated?
		
		Outline the contents of your key file:

2	Now send your lab partner your public key in the contents of an email, and ask them to import it onto their key ring (if you are doing this on your own, create another set of keys to simulate another user, or use Bill's public key – which is defined at http://asecuritysite.com/public.txt and send the email to him):
	
	`gpg --import` *theirpublickey*`.key`
	
	Now list your keys with:
	
	`gpg --list-keys`
		Which keys are stored on your key ring and what details do they have:

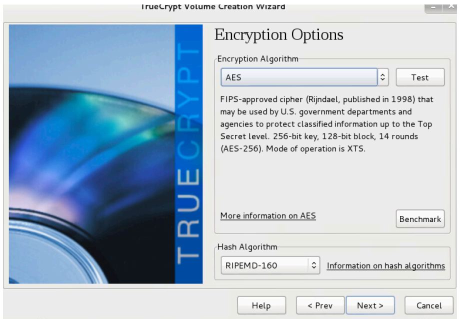
3	Create a text file, and save it. Next encrypt the file with their public key: `gpg -e -a -u "Your Name" -r "Your Lab Partner Name" hello.txt`	What does the –a option do: What does the –r option do: What does the –u option do: Which file does it produce and outline the format of its contents:
4	Send your encrypted file in an email to your lab partner, and get one back from them. Now create a file (such as myfile.asc) and decrypt the email using the public key received from them with: `gpg –d myfile.asc > myfile.txt`	Can you decrypt the message:

5	Next using this public key file, send Bill (w.buchanan@napier.ac.uk) an encrypted question (**http://asecuritysite.com/public.txt**).	Did you receive a reply:
6	Next send your public key to Bill (w.buchanan@napier.ac.uk), and ask for an encrypted message from him.	

G TrueCrypt

You can install TrueCrypt on your Ubuntu instance with:

```
sudo add-apt-repository ppa:stefansundin/truecrypt
sudo apt-get update
sudo apt-get install truecrypt
```

No	Description	Result
1	Go to your **Ubuntu** instance (User: root, Password: toor). Now **Create a new volume** and use an **encrypted file container** (use **truecrypt**) with a Standard TrueCrypt volume. When you get to the Encryption Options, run the benchmark tests and outline the results: 	**CPU (Mean)** AES: AES-Twofish: AES-Two-Seperent Serpent -AES Serpent: Serpent-Twofish-AES Twofish: Twofish-Serpent: Which is the fastest: Which is the slowest:
2	Select AES and RIPMD-160 and create a 100MB file. Finally select your password and use FAT for the file system.	What does the random pool generation do, and what does it use to generate the random key?
3	Now mount the file as a drive.	Can you view the drive on the file viewer and from the console? [Yes][No]
4	Create some files your TrueCrypt drive and save them.	Without giving them the password, can they read the file? With the password, can they read the files?

The following files have the passwords of “Ankle123”, “foxtrot”, “napier123”, “password” or “napier”. Determine the properties of the files defined in the table:

File	**Size**	**Encryption type**	**Key size**	**Files/folders on disk**	**Hidden partition (y/n)**	**Hash method**
http://asecuritysite.com/tctest01.zip (use: **wget http://asecuritysite.com/tctest01.zip** and then: **unzip tctest01.zip**)						
http://asecuritysite.com/tctest02.zip						
http://asecuritysite.com/tctest03.zip						

H Reflective statements

1.	**In ECC, we use a 256-bit private key. This is used to generate the key for signing Bitcoin transactions. Do you think that a 256-bit key is largest enough? If we use a cracker what performs 1 Tera keys per second, will someone be able to determine our private key?**

I What I should have learnt from this lab?

The key things learnt:

- The basics of the RSA method.
- The process of generating RSA and Elliptic Curve key pairs.
- To illustrate how the private key is used to sign data, and then using the public key to verify the signature.

Additional

The following is code which performs RSA key generation, and the encryption and decryption of a message (https://asecuritysite.com/encryption/rsa_example):

```
from Crypto.PublicKey import RSA
from Crypto.Util import asn1
from base64 import b64decode
from base64 import b64encode
from Crypto.Cipher import PKCS1_OAEP
import sys

msg = "hello..."

if (len(sys.argv)>1):
```

```
        msg=str(sys.argv[1])

key = RSA.generate(1024)

binPrivKey = key.exportKey('PEM')
binPubKey =  key.publickey().exportKey('PEM')

print
print "====Private key==="
print binPrivKey
print
print "====Public key==="
print binPubKey

privKeyObj = RSA.importKey(binPrivKey)
pubKeyObj =  RSA.importKey(binPubKey)


cipher = PKCS1_OAEP.new(pubKeyObj)
ciphertext = cipher.encrypt(msg)

print
print "====Ciphertext==="
print b64encode(ciphertext)

cipher = PKCS1_OAEP.new(privKeyObj)
message = cipher.decrypt(ciphertext)


print
print "====Decrypted==="
print "Message:",message
```

Can you decrypt this:

FipV/rvWDyUareWl4g9pneIbkvMaeulqSJk55M1VkiEsCRrDLq2fee8g2oGrwxx2j6KH+VafnLfn+QFByIKDQKy+GoJQ3
B5bD8QSzPpoumJhdSILcOdHNSzTseuMAM1CSBawbddL2KmpW2zmeiNTrYeA+T6xE9JdgOFrZOUrtKw=

The private key is:

-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQCqRucTX4+UBgKxGUV5TB3A1hZnUwazkLlsUdBbM4hXoO+n3O7v
jk1UfhItDrVgkl3Mla7CMpyIadlOhSzn8jcvGdNY/Xc+rV7BLfR8FeatOIXGqV+G
d3vDXQtsxCDRnjXGNHfWZCypHn1vqVDulB2q/xTyWcKgC61Vj8mMiHXcAQIDAQAB
AoGAA7ZYA1jqAG6N6hG3xtU2ynJG1F0MoFpfY7hegOtQTAv6+mXoSUC8K6nNkgq0
2Zrw5vm8cNXTPWyEi4Z+9bxjusU8B3P2s8w+3t7NN0vDM18hiQL2loS0s7HLlGzb
IgkBclJS6b+B8qF2YtOoLaPrWke2uV0TPZGRVLBGAkCw4YECQQDFhZNqWWTFgpzn
/qrVYvw6dtn92CmUBT+8pxgaEUEBF41jAOyR4y97pvM85zeJ1Kcj7VhW0cNyBzEN
ItCNme1dAkEA3LBoaCjJnEXwhAJ8OJ0S52RT7T+3LI+rdPKNomZW0vZZ+F/SvY7A
+vOIGQaUenvK1PRhbefJraBvVN+d0O9a9QJBAJWwLxGPgYD1BPgD1W81PrUH0RhA
svHMMItFjkxi+wJa2PlIf//nTdrFoNxs1XgMwkXF3wacnSNTM+cilS5akrkCQQCa
ol02BsZl4rfJt/gUrzMMwcbw6YFPDwhDtKU7ktvpjEa0e2gt/HYKIVROvMaTIGSa
XPZbzVsKdu0rmlh7NRJ1AkEAttA2r5H88nqH/9akdE9Gi7oO5Yvd8CM2Nqp5Am9g
CoZf0lNZQS/X2avLEiwtNtEvUbLGpBDgbvnNotoYspjqpg==
-----END RSA PRIVATE KEY-----