# 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.

🕮 **Web link (Weekly activities):** https://asecuritysite.com/esecurity/unit04

Demo: <https://youtu.be/3n2TMpHqE18>

## A RSA Encryption

**A.1** 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:

*d*=

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

C = M*e* (mod N) =

Now decrypt your ciphertext with:

M = Cd (mod N) =

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

**A.2** 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/465ZX5aH3HWFFX500JSPSt0/udqjoQuAr

WA5JqB//g2GfzZe1UzH5Dz3PBbJky8GiIfLm0OXSEIgAmpvc/9NjzAgjOW56n3Mu

sjVkibc+lljw+rOo97CfJMppmtcOvehvQv+KG0LZnpibiWVmM3vT7E6kRy4gEbDu

enHPDqhsvcqTDqaduQENBFTzi1ABCACzpJgZLK/sge2rMLURUQQ6l02UrS/GilGC

ofq3WPnDt5hEjarwMMwN65Pb0Dj0i7vnorhL+fdb/J8b8QTiyp7i03dZVhDahcQ5

8afvCjQtQstY8+K6kZFzQOBgyOS5rHAKHNSPFq45MlnPo5aaDvP7s9mdMILITvlb

CFhcLoC6Oqy+JoaHupJqHBqGc48/5NU4qbt6fB1AQ/H4M+6og4OozohgkQb80Hox

YbJV4sv4vYMULd+FKOg2RdGeNMM/aWdqYo90qb/W2aHCCyXmhGHEEuok9jbc8cr/

xrWL0gDwlWpad8RfQwyVU/VZ3Eg3OseL4SedEmwOO

cr15XDIs6dpABEBAAGJAR8E

GAECAAkFAlTzi1ACGwwACgkQ7ABWURrXT0KZTgf9FUpkh3wv7aC5M2wwdEjt0rDx

nj9kxH99hhuTX2EHXuNLH+SwLGHBq5O2sq3jfP+owEhs8/Ez0j1/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>

**A.3** Bob has a private RSA key of:



And receives a ciphertext message of:

Pob7AQZZSml618nMwTpx3V74N45x/rTimUQeTl0yHq8F0dsekZgOT385Jls1HUzWCx6ZRFPFMJ1RNYR2Yh7AkQtFLVx9lYDfb/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/rTimUQeTl0yHq8F0dsekZgOT385Jls1HUzWCx6ZRFPFMJ1RNYR2Yh7AkQtFLVx9lYDfb/Q+SkinBIBX59ER3/fDhrVKxIN4S6h2QmMSRblh4KdVhyY6cOxu+g48Jh7TkQ2Ig93/nCpAnYQ="

privatekey = ''

keyDER = b64decode(privatekey)

keys = RSA.importKey(keyDER)

dmsg = keys.decrypt(b64decode(msg))

print dmsg

What is the plaintext message that Bob has been sent?

## B OpenSSL (RSA)

We will using 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:  How long did it take to generate a 1,024 bit key?  Use the following command to view the keys:  type private.pem (or cat private.pem in Linux) |
| **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 |  |
| **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 we will encrypt with our public key:  openssl rsautl -encrypt -inkey public.pem -pubin -in myfile.txt -out file.bin |  |
| **B.7** | And then decrypt with our private key:  openssl rsautl -decrypt -inkey private.pem -in file.bin -out decrypted.txt | What are the contents of decrypted.txt |

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+rm029m2f6IddtlImHrOXjNwYyt4Elkkc7AzOy899C3gpx0kJK45k/CLbPnrHvkLvtQ0AbzWEQpOKxI+tW06PcqJNmTB8ITRLqIFQ++ZanjHWMw2Odew/514y1dQ8dccCOuzeGhL2Lq9dtfhSxx+1cBLcyoSh/lQcs1HpXtpwU8JMxWJl409RQOVn3gOusp/P/0R8mz/RWkmsFsyDRLgQK+xtQxbpbodpnz5lIOPWn5LnT0si7eHmL3WikTyg+QLZ3D3m44NCeNb+bOJbfaQ2ZB+lv8C3OxylxSp2sxzPZMbrZWqGSLPjgDiFIBL [w.buchanan@napier.ac.uk](mailto:w.buchanan@napier.ac.uk)

View the private key. What is its format?

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

## 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 (and should have 256 bits).  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 y2 = x3 + 7, and with a prime number of 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>

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, NIST512p and SECP256k1:

NIST192p:

NIST512p:

SECP256k1:

By searching on the Internet, can you find where SECP256k1 is used?

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

## E Inverse of a value mod N

**E.1** 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)?

## 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:

-----BEGIN PGP PUBLIC KEY BLOCK-----

Version: OpenPGP.js v4.4.5

Comment: https://openpgpjs.org

xk0EXEOYvQECAIpLP8wfLxzgcolMpwgzcUzTlH0icggOIyuQKsHM4XNPugzU

X0NeaawrJhfi+f8hDRojJ5Fv8jBI0m/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

0g7MSRsL+dYQauIgtVb3dloLMPtuL59nVAYuIgD8HXyaH2vsEgSZSQn0kfvF

+dWeqJxwFM/uX5PVKcuYsroJFBEO1zas4ERfxbbwnsQgNHpjdIpueHx6/4EO

b1kmhOd6UT7BamubY7bcma1PBSv8PH31Jt8SzRRiaWxsIDxiaWxsQGhvbWUu

Y29tPsJ1BBABCAAfBQJcQ5i9BgsJBwgDAgQVCAoCAxYCAQIZAQIbAwIeAQAK

CRCg2xcQNi3ZmORMAf9vr6kN9AuLrOD9jS0dLk89G/XfbdzChrK8xw+Odar5

V+I3JfNj5QkpHU9eyTMO8cws7JWlRyOV7kKHJPks7D9kx8BmBFxDmL0BAgDY

lTsT06vVQxu3jmfLzKMAr4kLqqIuFFRCapRuHYLOjw1gJZS9p0bFS0qS8zME

GpN9QZxkG8YEcH3gHxlrvALtABEBAAH+CQMI2Gyk+BqVOgzgZX3C80JRLBRM

T4sLCHOUGlwaspe+qatOVjeEuxA5DuSs0bVMrw7mJYQZLtjNkFAT92lSwfxY

gavS/bILlw3QGA0CT5mqijKr0nurKkekKBDSGjkjVbIoPLMYHfepPOju1322

Nw4V3JQO4LBh/sdgGbRnwW3LhHEK4Qe70cuiert8C+S5xfG+T5RWADi5HR8u

UTyH8x1h0ZrOF7K0Wq4UcNvrUm6c35H6lClC4Zaar4JSN8fZPqVKLlHTVcL9

lpDzXxqxKjS05KXXZBh5wl8EGAEIAAkFAlxDmL0CGwwACgkQoNsXEDYt2ZjA

BgH/cP12s3xCwxtVt+Zds8NdqysDO6yve2ha7cc+Vl8AP+YKqFT9IkMZJW/a

qV+0VXeqyyru86F+xfrEKHdbAlqzMA==

=5NaF

-----END PGP PRIVATE KEY BLOCK-----

**F.2** Using the code at the following link, generate your own key:

<https://asecuritysite.com/encryption/openpgp>

**F.3** An import element in data loss prevention is encrypted emails. In this part of the lab we will use an open source standard: PGP. On your instance, install GPG from:

<http://gpg4win.org/download.html>

|  |  |  |
| --- | --- | --- |
| **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:  **gpg --import** theirpubickey**.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](mailto:w.buchanan@napier.ac.uk)) a question (http://asecuritysite.com/public.txt):  -----BEGIN PGP PUBLIC KEY BLOCK-----  Version: BCPG C# v1.6.1.0  mQENBFTvF+gBCACkpcMPybSe1NTE1hDg86gPcQqoT8kD9oS/ankGwbB4R5zT+3Ny  MZWZwT43lL99R7sfkluglwVkqko74Lemy9pBF/rbWeWev6mCR3z1V3yTTv3zP1V5  tLcz3K65flRHPQU/FzxqH1T4kaH6dDiL/UuKKcyYMxXNnqERitJPU7ZJVhqeM3gi  4cG4znKY5fw8bdSpNC//pgkDzEaWYJFdyq/KqCwRK5r/Egj7FVHaLGC37lDgZKR5  dBoIVaOTfXykJLe3Vc3dIv9LU58U3YHqsc/w6X4E5R/eEnp0IwKyb7oXdrFOM5ud  DSoJ7aT24IqZW678vNtufGdr4OD+BF5r2UZpABEBAAG0GHcuYnVjaGFuYW5hQG5h  cGllci5hYy51a4kBHAQQAQIABgUCVO8X6AAKCRBOV4Uk9xMsXJgNB/4jfAnXLHjZ  +I4z3Hhqn9UMokU6Q4cQtrGX0OhelymKZTMXNoSKhT5fB9GBlIIbwMkZHxcUNmUB  PuAwq+RAhFqtRkcH3x1a5eNBhEvcfi9hS2ls43gfsrXjMzekY6dyzD/ePM7HvihJ  vrsQNZNI7ZIaP5viCZFgQqmwYQA1LCrEy/xpSXBNrqrOwuti+2+xeZsswitYLAzA  ryDMgCG9GPuSfkmvatYJJrl5QAhj1p0FKERhL1/h3bh18i8Llh1K9tEBxIJf4ZIy  ivV1bX5G36jciOrKCLi7/m6xhHh86brRQA++qwUdXU/3MMqvRwuinSO9NYeVCf6Y  V66cJqTgdR1F  =uiw7  -----END PGP PUBLIC KEY BLOCK----- | Did you receive a reply: |
| **6** | Next send your public key to Bill ([w.buchanan@napier.ac.uk](mailto:w.buchanan@napier.ac.uk)). |  |

## G TrueCrypt

|  |  |  |
| --- | --- | --- |
| **No** | **Description** | **Result** |
| **1** | Go to your Ubuntu instance. Now **Create a new volume** and use an **encrypted file container** (use tc\_*yourname*) with a Standard TrueCrypt volume.  When you get to the Encryption Options, run the 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.  Next dismount your drive, and copy the file to the provided USB stick. Give the USB stick to your neighbour, and see if they can view the file contents. | 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> |  |  |  |  |  |  |
| <http://asecuritysite.com/tctest02.zip> |  |  |  |  |  |  |
| http://asecuritysite.com/tctest03.zip |  |  |  |  |  |  |

Now with **truecrack** see if you can determine the password on the volumes. Which TrueCrypt volumes can truecrack?

## 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?**

**2. If someone takes our elliptic curve public key, how might they determine our public key?**

## G 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.

## Notes

To setup your Python to run Python 2.7:

sudo update-alternatives --set python /usr/bin/python2.7

To install a Python library use:

easy\_install libname

or:

pip install libname