

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.

For the lab session, log into [<https://vsoc.napier.ac.uk/>] using **CyberStudent@vsoc.local** and the password is:

NapierCyber1!

You will find a Ubuntu instance, and where the password is "Napier123".

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= Φ =

Now pick a value of e which does not share a factor with Φ [$\gcd(\Phi, e)=1$]:

e =

Now select a value of d , so that $(e.d) \pmod{\Phi} = 1$:

[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:

A.2 In the following we use 60-bit prime numbers:

```
from Crypto.Util.number import *
from Crypto import Random
import Crypto
import gmpy2
import sys

bits=60
msg="Hello"

if (len(sys.argv)>1):
    msg=str(sys.argv[1])
if (len(sys.argv)>2):
    bits=int(sys.argv[2])

p = Crypto.Util.number.getPrime(bits, randfunc=Crypto.Random.get_random_bytes)
q = Crypto.Util.number.getPrime(bits, randfunc=Crypto.Random.get_random_bytes)

n = p*q
PHI=(p-1)*(q-1)

e=65537
d=(gmpy2.invert(e, PHI))

m= bytes_to_long(msg.encode('utf-8'))

c=pow(m,e, n)
res=pow(c,d, n)

print "Message=%s\np=%s\nq=%s\nnd=%d\ne=%d\nN=%s\n\nPrivate key (d,n)\nPublic key (e,n)\ncipher=%s\ndecipher=%s" % (msg,p,q,d,e,n,C,(long_to_bytes(res)))
```

For a message of “goodbye”, show that you can encrypt and decrypt the message. Repeat for 120-bit, 256-bit and 512-bit prime numbers. What do you observe when running the program from the changing of the prime number size?

Can you explain the main elements of the program?

A.3 The following defines a public key that is used with PGP email encryption:

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

mQENBFTzi1ABCADIEWch0yqRQmU4AyQAMj2Pn68Sqo9lTPdPcItwo9Lbtdv1YCFz
w3qLlp2RORMP+kpdi92CIhduYHDmzfHZ3IWTBgo9+y/Np9UJ6tNGocrsq4xwz15
4vx4jJRddC7QySSh9UxDpRWF9sgqEv1pah136r95ZuyjC1EXnoNxdLJtx8Pl1CXC
hv/v4+KfOyZyH+HDJ4xP2bt1S07dkasYZ6cA7BHYi9k4xgEwxVvYtNjSPjTsQY5R
cTayXveGafuxmhSauZKiB/2TFerjEt49Y+p07tPTLX7bhMBVbUvojt/JeUKV6vK
R82dmOd8seUvhwOHYB0JL+3S7PgFFSL01NV5ABEBAAG0LJpbGwgQnVjaGFuYW4g
KE5vbmUpIDx3LmJlY2hhbmFuQG5hcGllci5hYy51az6JATKEEwECACMFA1Tzi1AC
GwMHCwkIBWMAQYVCAIJCgSEFgIDAQIEAQIXgaAAKCRDsAFZRGtdPQi13B/9KHeFb
11AXqbaFFGRDEVx8UfPnEww4FFqwhcr8RLWye8/COlUpB/5AS2yvoymbNFMGZURb
LGF/u1LVH0a+NHQu57u8Sv+g3bBthEPH4bKaEzBYRS/dYH0x3APFyIayfm78JVRF
zdeTO0f6PaxUTRx7iScCTkN8DUD3lg/465ZX5ah3HwFFX500JSPst0/udqjoQuAr
WA5JqB//g2GfzZe1UzH5Dz3PBbJky8GiIFLm00XSEIgaMpvC/9NjzAgjOW56n3Mu
sjvkiBc+lljw+r0o97CfJmPmtcOvehvQv+KG0LZnpibiWvMM3vT7E6kRy4gEbDu
enHPDqhsvcqTDqaduQENBFTzi1ABCACzpJgZLK/sge2rMLURUQQ6102Urs/GilGC
ofq3wPndt5HearwMMWn65Pb0Dj0i7VnorhL+fdb/J8b8QTiyp7i03dzVhDahcQ5
8afVcJQtQstY8+K6kZFZQ0BgYOS5rHAKHNSPFq45MlnPo5aadVp7s9mdMILITv1b
CFhcLoC6Oqy+JoahUpJqHBGqC48/5NU4qbt6fB1AQ/H4M+6og4OozohgkQb80Hox
YbJV4sv4vYmULd+FK0g2RdGeNMM/awdQYo90qb/W2aHCCyXmhGHEEuok9jbc8cr/
xrWL0gDw1Wpad8RfQwyVU/VZ3Eg30seL4SedEmw00
cr15XDis6dpABEBAAGJAR8E
GAECAAKFA1Tzi1ACGwwACgkQ7ABWURrXT0KZTgf9Fupkh3wv7ac5M2wwdEjt0rDx
nj9kxH99hhuTX2EHXunLH+SwLGHbq502sq3jfp+owEhs8/Ez0j1/fSKIqAdl73mB
dbqWPjzPTY/m0It+ww3epOM75uwjD35PF0rkxxZmEf6SrjZD1sk0B9bry2v9iwn9
9ZkuvcfH4vT++PognQLTUqNX0FGpD1agrG01XSctJWQXCXPfwdtbIdThBgZ4f1Z
ssAIBCaB1QkzfbPvrMzdtIP+AXg6++K9Sno9N/FRPYzjUSEmpRp+ox31wymvczCU
RmyUqF+/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?

A.4 Bob has a private RSA key of:

```
MIICXAIBAAKBgQCWgjkEoyCxm9v6VBnUi5ihQ2knkdxGDL3GXLIUU43/froeqk7q9mtxt4AnPAAdX3f2r4STZYYiqXGSh
CUBZCI90dvf6YiEM5OY2jgsmqBj2Xkp/8HgN/XDw/wD2+zebYGLLYtd2u3Gxx9edqJ8kQcU9LaMH+ficFyfq9UwtjQ
IDAQABAoGAD7L1a6Ess+9b6G70gTANWkKJpshvZDGB63mxKRepaJEX8sRJEqLqOYDnSC+pkK08IsfHreh4vrp9bsZuECr
B1OHSjwDB0S/fm3KEWbsaaXDUau0dQg/JBMXAKzeATreoIYJItYgwrj++fuquKabAZumvOnWjyBIs2z103kDz2ECQQDn
n3JpHirmgvdf81yBbAJaXBNIPzOCCth1zwFAs4EvrE35n2HvUQuRhy3ahUKXsKX/bGvwzmc206kbLTFEygVakeAwxxZn
PkaAY2vuoUCN5nBLZgegrAtmU+U2woa5A0fx6uXmShqxo1iDxEC71FbNIGHBg5rsUyDj30s1oLmDVjmQJAIy7qLyOA+s
Cc6BtMavBgLx+bxCWfmsOZHOSX3179smTRAJ/HY64RREISLIQ1q/yw7IWBzxQ5WTHg1iNZFjKBvQJBAL3t/vCJwRz0Ebs
5FaB/8UwhhsrbtXlGdnkOjIGsmV0vHSf6pohquiay/DV88pvhN11ZG8zHpeUhnAQccJ9ekzkCQDHHG9LYCQqTgsyYms//
cw4sv2nuoE1uezTjUFeqo1sgo+WN96b/M5gnv45/Z3xZxz4JHOCJ/NRWXN0tEukw+zY=
```

And receives a ciphertext message of:

```
Pob7AQZZSm1618nMwTpx3V74N45x/rTimUqeTl0yHq8F0dsekZg0T385J1s1HUZWCx6ZRFPFMJ1RNYR2Yh7AkQtFLVx9T
YDfb/Q+SkinBIBX59ER3/fDhrVKxIN4S6h2QmMSRb1h4kdVhyY6cOxu+g48Jh7TkQ2Ig93/nCpAnyQ=
```

Using the following code:

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

msg="Pob7AQZZSm1618nMwTpx3V74N45x/rTimUqeTl0yHq8F0dsekZg0T385J1s1HUZWCx6ZRFPFMJ1RNYR2Yh7AkQtFLVx9T
YDfb/Q+SkinBIBX59ER3/fDhrVKxIN4S6h2QmMSRb1h4kdVhyY6cOxu+g48Jh7TkQ2Ig93/nCpAnyQ="
privatekey =
'MIICXAIBAAKBgQCWgjkEoyCxm9v6VBnUi5ihQ2knkdxGDL3GXLIUU43/froeqk7q9mtxT4AnPAaDX3f2r4STZYYiqXGs
HCUBZci90dvzf6YiEM5OY2jgsmqBjf2xkp/8Hgn/XDw/wD2+zeBYGLLYtd2u3Gxx9edqJ8kQcU9LaMH+ficFQyfq9UwTj
QIDAQABAoGAD7L1a6Ess+9b6G70gTANWkKJpshVZDGB63mXKRepAJEX8SRJEQLQOYDNSC+pkK08IsfHreh4vrp9bsZuEC
rB1OHSjwDB0S/fm3KEWbsaaXDUAu0dQg/JBMXAKzeATreoIYJItYgwzrJ++fuquKabAZumvOnWjyBIs2z103kDz2ECQQD
nn3JpHirmgVdf81yBbAJaXBNIPzOCth1zwFas4Evre35n2HVUQuRhy3ahUKXSKX/bGvwzmC206kbLTfEygVAKEAwxxZ
nPkAAY2vuoUCN5NbLZgegrAtmU+U2woa5A0fx6uXmShqxo1iDxEC71FbNIgHBg5srsUyDj30s1oLmDVjmQJAIy7qLyOA+
sCc6BtMavBgLx+bxCwFmsoZHOSX3179smTRAJ/HY64RREIsLIQ1q/yw7IWBzxQ5WTHg1iNZFjKBvQJBAL3t/vCJwRz0Eb
s5FaB/8UwhhsrbtXlGdnkOjIGsmv0vHSf6poHquiy/DV88pvhN11ZG8zHpeUhnAqccJ9ekzkCQDHHG9LYCQgtGsyYms/
/cw4sv2nu0E1uezTjUFeqO1sg0+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?

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: How long did it take to generate a 1,024 bit key? Use the following command to view the keys: cat private.pem

B.2	Use following command to view the output file: <code>cat private.pem</code>	What can be observed at the start and end of the file:
B.3	Next we view the RSA key pair: <code>openssl rsa -in private.pem -text</code>	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: <code>openssl rsa -in private.pem -des3 -out key3des.pem</code>	Why should you have a password on the usage of your private key?
B.5	Next we will export the public key: <code>openssl rsa -in private.pem -out public.pem -outform PEM -pubout</code>	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: <code>openssl rsautl -encrypt -inkey public.pem -pubin -in myfile.txt -out file.bin</code>	
B.7	And then decrypt with your private key: <code>openssl rsautl -decrypt -inkey private.pem -in file.bin -out decrypted.txt</code>	What are the contents of decrypted.txt

Following the method here:

<https://medium.com/asecuritysite-when-bob-met-alice/rsa-cracking-claims-eebf8ef1a97e>

Can you crack the following:

RSA Encryption parameters. Public key: [e,N].
e: 65537
N: 911844725340031776516886332975892441

Cipher: 801127314512167104045686292190207406
 We are using 60 bit primes
 Can you find the value of the message?

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	<p>First we need to generate a private key with:</p> <pre>openssl ecparam -name secp256k1 -genkey -out priv.pem</pre> <p>The file will only contain the private key (and should have 256 bits).</p> <p>Now use “cat priv.pem” to view your key.</p>	Can you view your key?
C.2	<p>We can view the details of the ECC parameters used with:</p> <pre>openssl ecparam -in priv.pem -text -param_enc explicit -noout</pre>	<p>Outline these values:</p> <p>Prime (last two bytes):</p> <p>A:</p> <p>B:</p> <p>Generator (last two bytes):</p> <p>Order (last two bytes):</p>
C.3	<p>Now generate your public key based on your private key with:</p> <pre>openssl ec -in priv.pem -text -noout</pre>	<p>How many bits and bytes does your private key have:</p> <p>How many bit and bytes does your public key have (Note the 04 is not part of the elliptic curve point):</p> <p>What is the ECC method that you have used?</p>

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, 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, 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 details

E.1 In the RSA method, we have a value of e , and then determine d from $(d \cdot e) \pmod{\phi(n)} = 1$. 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.2 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:

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

xk0EXEOYvQECAIpLP8wFLxzgco1MpwgzCUZT1H0icggOIyuQKSHM4XNPugzu
X0NeaawrJhfi+f8hdRojJ5Fv8jBI0m/KwFMNTT8AEQEAAC0UYm1sbCA8Ym1s
bEBob21lLmNvbT7CdQQQAQgAHwUCXE0YvQYLCQCIawIEFQgKAgMWAgECGQEC
GwMCHgEAcgkQoNSXEDyt2ZjKTAH/b6+pDfQLi6zg/Y0tHS5PPrv1323cwoay
VMcPjnwq+VfiNyXzy+UJKR1PXskzDvHMLoyVpucj1e5ChyT5LOW/ZM5NBFxD
mLOBAGdY1Tst06vVQxu3jmfLzKMar4kLqqIuFFRCapRuHYLOjw1gJZS9p0bF
S0qS8ZMEGpN9QzxkG8YECH3GHx1rVALtABEBAAHCXwQYAQgACQUCE0YvQIb
DAAKCRCg2xcQNi3ZmMAGAf9w/XazfELDG1w3512zw12rKwM7rk97aFrTxz5W
XwA/5gqovP0iQxklb9qpX7Rvd6rLKu7zoX7F+sQod1sCwrMw
=CXT5
-----END PGP PUBLIC KEY BLOCK-----

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

xcBmBFxDmLOBAGCKSz/MHy8c4HKJTKcIM3FM05R9InIIDiMrkCrBzOFzT7oM
1F9DXmmskyYX4vn/IQ0aIyeRb/IwSNJvysBTDU0/ABEBAAH+CQMIBNTT/OPv
TJZgvF+fL0sLSNYP64QfNHav50744y0MLV/EZT3gsBwO9v4XF2Sszj6+EHbk
O9gwi31BAIDgSaDsJYf7xPOhp8iEwwrUkC+jlGpdTsGDJpeYmISVVv8Ycam
0g7MSRSL+dYQauIgtVb3dloLMPtuL59nVAYuIgd8Hxyah2vsEgSZSQn0kfVf
+dweqJxwFM/ux5PVKcuysroJFBE01zas4ERfxbbwnsQGNHpdIpueHx6/4EO
```

```

b1kmhOd6UT7BamubY7bcma1PBSv8PH31Jt8SzRRiawxsIDxiawxsQGhvbWUu
Y29tP5J1BBABCAAFBQJcQ5i9Bg5JBwgDagQVCAoCAXYCAQIZAQIbAwIeAQAK
CRCg2xcQNi3ZmORMAF9vr6kN9AuLrOD9j50dLk89G/XfbdzChrK8xw+odar5
V+I3JfNj5Qkphu9eyTMO8cws7JWlRyOV7kKHJPks7D9kx8BmBFxDmL0BAGDY
lTst06vVQxu3jmfLzKMar4kLqqIuFFRCapRuHYLOjw1gJZS9p0bFS0qs8zME
GpN9QZxkG8YECH3gHxlrvaLtABEBAAH+CQMI2Gyk+BqV0gzgZX3C80JRLBRM
T4sLCHOUGlwaspe+qatOVjeEuxA5DuSs0bVMrw7mJYQZLtjNkFAT92lSwfxY
gavS/biLlW3QGA0CT5mqijKr0nurKkekKBD5GjkjvbiOPLMYHfepPOju1322
Nw4V3JQ04LBh/sdgGbrNwW3LhHEK4Qe70cuiert8C+S5xfG+T5RWAD15HR8u
UTyH8x1h0ZrOF7K0Wq4UcNvrUm6c35H6lC1C4Zaar4JSN8fZPqVKLlHTVCL9
lpDzxxqxkjS05KXXZBh5w18EGAEIAAKFA1xDmL0CGwwACgkQoNsXEDYt2ZjA
BgH/cP12S3xCwxtvt+Zds8NdqysD06yve2ha7cc+Vl8AP+YKqFT9IkMZJW/a
qV+OVXeqyyru86F+xfrEKHdbA1qzMA==
=5NaF
-----END PGP PRIVATE KEY BLOCK-----

```

F.2 Using the 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.

No	Description	Result
1	<p>Create a key pair with (RSA and 2,048-bit keys):</p> <p>gpg --gen-key</p> <p>Now export your public key using the form of:</p> <p>gpg --export -a "Your name" > mypub.key</p> <p>Now export your private key using the form of:</p> <p>gpg --export-secret-key -a "Your name" > mypriv.key</p>	<p>How is the randomness generated?</p> <p>Outline the contents of your key file:</p>
2	<p>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):</p> <p>gpg --import theirpublickey.key</p> <p>Now list your keys with:</p> <p>gpg --list-keys</p>	<p>Which keys are stored on your key ring and what details do they have:</p>
3	<p>Create a text file, and save it. Next encrypt the file with their public key:</p> <p>gpg -e -a -u "Your Name" -r "Your Lab Partner Name" hello.txt</p>	<p>What does the -a option do:</p> <p>What does the -r option do:</p>

		<p>What does the –u option do:</p> <p>Which file does it produce and outline the format of its contents:</p>
4	<p>Send your encrypted file in an email to your lab partner, and get one back from them.</p> <p>Now create a file (such as myfile.asc) and decrypt the email using the public key received from them with:</p> <p>gpg -d myfile.asc > myfile.txt</p>	Can you decrypt the message:
5	<p>Next using this public key file, send Bill (w.buchanan@napier.ac.uk) a question (http://asecuritysite.com/public.txt):</p> <p>-----BEGIN PGP PUBLIC KEY BLOCK-----</p> <pre> mQENBFxEQEMBCACTgu58j4RuE340w3Xoy4PIXlLv/8P+FUUFs8Dk4w05zUJN2Nfn 45fIASdKCh8cv2wbCVwjKEP0h4p5IE+lrwQK7bwYx7Qt+qmr5eLMUM8IvXA18wf AOPS7XektZxa4/jwagJupmmYL+MuV9o5haqYp1OYCCVR135KAZfx743YuWCNqvc 3Em0+gh4F2TXsefjñiwuJRGY3Kbb/MAM2zc2f7FfCJvB1C300LB+KwCddZP/23l1 nOqmzaVF0qqrHQ5EZGK3j3S4fzHNq14TMS3c21YkP00/DV6BkgIHTG5NIIdVEdQh wV8c1pj0ZP7ShIE8cDhTy8k+xrIByPUVfPmpABEBAAG0J0JpbGwgQnVjaGFuYW4g PHcuYnVjaGFuYW5AbmFwawVyLmFjLnVrPokBVAQTAQgAPhYhBK9cqX/wECpQ6+5 TFPDJcQRPXoQBQJCREHjAhsDBQkDwmCABQsJCACBhUKCQgLAGQWAgMBAh4BAheA AAoJEFPDJcQRPXoQ2KIH/2sRASqbrqCMNMrsiBo9xtCFzQ052odbzubIScnwzrDF Y9z+qPSAwawGO+1R3LPDH5SMLQ2YOSnqg8vvtJBt0JR9YGNX9/bqqVFRKKSQ0HiD Sb2M7phBdk4WLkqLZ/AfgHaLkpfNX0bq7whqZ+Pez0nqjn08JkIog7LhaQZh/Chf Op1+wHV0rEFuaDQn83yF5DWB1Dt4fbzfvUreJb92tSrReHALQQA3h5wkTA0qxhdD 9XyEwKnDrYCWioj0XwjivUre2fw3SKn8KHvJDeDYVKZyY18oA+da+xgs9b+n+Tq mM1fs1whw9wRyp0jbVLEs3yxLgE4elbCCmgiTNpnmMW5AQ0EXERB4WEIAKCPJqmM o8m6Xn163xtAZnx3t0EJSAV6u0yINIC8aEudNwg+/ptKKanUDm38dPn011mgOyc FEu4qfJHbMidkEEac5J01gvhRK7jv94KF3vxqkr/bYnxltghqcfXesga9jFAHV8J M6sx4exOoc+/52YskpvdUS/eTPnwoQnbgjP+wsZpNq0wS6yO5urDfD61vefgK5A TFB9lQUE01pb6IMKkcBZZvpZWochbWPWCb9JZMuirdSyksuTLdqgEsw7MyKBjCae E/THuTazumad/PyEb0RCbODdMb55L6CD2w2DUquvBLI9FN6KTYwk5L/JzNAIWBV9 TKfevup933j1m+sAEQEAAYkBPAAQYAAQAJhyhBK9cqX/wECpQ6+5TFPDJcQRPXoQ BQJCREHjAhsDBQkDwmCAAoJEFPDJcQRPXoQGRGh/3592g1F4+wRApBuCgFEmihd ma5gp1u2J7Njnbv9Icy8VZSGw7UAT7FmTPq1vwFM3w3gQDCXCKGztieUkZMTPqb LujBR4y55d5XDY6mP40zWRgdR1en2XsgHLPaJRQpAhZq8ZvOdGe/ANCyxvdfHbGy aFAMUfAhxkbITQKXH+EIKCHXDtDUHUXmAQvsZ8Z+Jm+ZwdhwkMsk43tw8UXLIynp Ae0oATdohke3EVK5+0Dc/jezcUwz2IKfw7LB3sQ4c6H8EY8PTHlNAIgwMCDp5WTB DmFoRWTU6CpKtwIg/lb1ncbs1h2xAfEUX6ASHXR8vBOnIXwss21FuAanmwe4lmyZ AQ0EXF1iYQEIALCmZgCvOira+YmtgQZuoos6veQ+uxysi9+wABtPEY5Bahe2BqtY /xrVE1bhekVfTpuvektTYQxe7wIyJj5xBnwNLzp/XedgIywgTWYnIHe+6lDoBqtX US7wfmC8CBcJAhp9ouTNP+/yI8TZJM0dTdGAgF4n4Tb6nXRawLEsn934ZfB88uG UvS6aoFDWd1cSDG0cNIGdOL+q+071J11/S13Pz+7E7ymPHJ1mFP6UxvFZFSHUUA6 Uk64uip1e61Lxbnfjdwd3cZAFfxj7K0B+Hdb9kIkZlH5MYxomaMybLZH9zi1h 9ARR9K/+nES/7//83Yzbyxrvn1HxwKIDJ1sAEQEAABQnQm1sbCBcdWNoYW5hbhiA8 dy5idwNoYW5hbkbBuYXBpZiUyWmudws+iQFUBBMBCAA+FiEEN/8zkuNo3g8ti6cX d5kNec0XwJMFALxdyMECGWMFCQPCZwAFcwkIBWIGFQoJCASCBYCAwECHgECF4AA cGkQd5KndXwJMKtggA13FA+td7f0sdo+KFntWH4QnQvEaRjJIXboFSx602wqME NZVPobw9ka4sYr9mejqm1vNzeAxlDahV1k5BPMUwA/NdHozPvmvmbku7vjJxz/f MqpP2Pa10/zBdkw80pbJel2SbqBtFon4wQY3hSEBDYHCBWGI/ZbLSLXLJH2e+frL Z3wi6uzrGPeRLNjhg1NADMDfU6mLTcsK8RaCJHjULogy4zstiZGGBQIyR209J0g tahUv/180s4Dcvs3kyuJqQFv7sBYfDRCMQfWSXdwWjK1AmUbpQpTzJAlYLeb5tNE LizcJwHPou1oiY8/ltpFvHKv6EnzAgyi2igj7F1S0rkBDQRCXWJhaQgAxUxraS8l Ccs2KFoyKeXN/nuFG132bEPPOquMA7949eNatbF/6g8Gw5+sVa93q5ueBnveQvn6 mywCF/62z8EL/vmypy47iaGJuLdotSmayHr1mrJDogOq7GUG8mfFmZKwmp/Jzt2i +R0uDRKqp73RRncczKgSeGLRxlNyY5+ol7F4Nphen4XE0J10fgzAghAcSzSYEQ9 xviFrHiCs4a72mf5TuqIyQ6X3AS8otZn0GXeZmIEoXxBz72jHURdJ15JS/Tt8qqq R69GvXgzX9+g7Vt0swCouj1jNskr5KPS4N0gFLKTFU17jlyfjPVN4yrs6lMWTZHE </pre>	Did you receive a reply:

	BDWOfdrQ/DTEuWARAQABtQE8BBgBCAAMFiEEN/8zkuNo3g8ti6cXd5kNec0XwJMF AlxdYmECGwwFCQPCZwAACgkQd5kNec0XwJ089Af/Rl1nf4Ty4MjgdbRVo43crcn+ Z17LPt+IBpPXoyv/a//5CDZCWSEcJ7ijPmAx5Zgyw8SGt10EW2kOcEhDwPCds32r 6iEIwaoMT7NXKOGZxYfAjT0iYE1cR6zxZVcPkC5561TB5yZt51+H6GshQ5eUIH+ fs6DMRGrWTEZENJ2Evof08DUJanaTi4ImIJF6Gidwmt+YoL1d5THZEWBXyNvRIeZ K+FWAZm7a5gBTCgeafvUDbw3Drecm6y7YTuoFHF32laHNK8/9Lu0T5JTX9jhYvTr 1BrwqYij2gvKYwAk5gkJdguUodNVLCn1RaeliGetiL3BEVZsfE3bHANFS107Bw== =DvMI -----END PGP PUBLIC KEY BLOCK-----	
6	Next send your public key to Bill (w.buchanan@napier.ac.uk), and ask for an encrypted message from him.	

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/rvWdyUarew14g9pneIbkvMaeu1qSjk55M1vkiEscrRDLq2fee8g2oGrwx2j6KH+VafnLfn+QFByIKDQKy+GoJQ3
B5bD8QsZPpoumJhdsILCOdHNSZtseuMAM1CSBawbddL2Kmpw2zmeiNTrYeA+T6xE9JdgOfrZ0UrtKw=

The private key is:

```
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQCqRucTX4+UBgKxGUV5TB3A1hZnUwazkL1sUdBbm4hXo0+n307v
jklUfhItDrvgkl3Mla7CmpyIad1ohSzn8jcvGdNY/Xc+rv7BLfR8Feat0IXGqv+G
d3vDXQtsxCDRnjXGNHfWZCypHn1vqVdu1B2q/xTywCKgC61Vj8mMiHXcAQIDAQAB
AoGAA7ZYA1jqAG6N6hG3xtU2ynJG1F0MoFpfY7hegotQTAV6+mXoSUC8K6nNkgq0
2Zrw5vm8cNXTPwyEi4Z+9bxbjU8B3P2s8w+3t7NN0vDM18hiQL21oS0s7HL1Gzb
IgbC1J56b+B8qF2YtOoLaPrwke2uV0TPZGRVLBGAKCw4YECQDFhZNqwwTFgpzn
/qrvYvw6dtn92cmUBT+8pxgaEUEBF41jAoyR4y97pvM85zeJ1Kcj7Vhw0CnyBzEN
ItCnme1dAKEA3LBoaCjJnEXwhAJ8OJ0S52RT7T+3LI+rdPKNomZW0vZZ+F/SvY7A
+voIGQauenvK1PRhbeFjraBvVN+d009a9QJBAJWWLxGPgYD1BPgD1W81PrUH0Rha
```

svHMMItFjkxi+wJa2PlIf//nTdrFoNxs1XgMwkXF3wacnSNTM+cilS5akrkCQCa
o102BsZl4rfJt/gurzMMwcbw6YFPDwhDtKU7ktvpjEa0e2gt/HYKIVROvMatIGSa
XPZbzVskdu0rm1h7NRJlAkeAttA2r5H88nqH/9akde9Gi7o05Yvd8CM2Nqp5Am9g
CoZf01NZQS/X2avLEiwtNtEvUbLGpBDgbvnNotoYspjqpg==
-----END RSA PRIVATE KEY-----