Assignment 8. Asymmetric encryption

Crypto basics 3

- Got n and public exponent

```
banana_and_bread@yourMummy:~$ openssl asn1parse -i -dump -in ~/Downloads/rsa/pubkey.pem
    0:d=0  hl=2 l= 100 cons: SEQUENCE
    2:d=1  hl=2 l=  13 cons:  SEQUENCE
    4:d=2  hl=2 l=   9 prim:   OBJECT            :rsaEncryption
   15:d=2  hl=2 l=   0 prim:   NULL
   17:d=1  hl=2 l=  83 prim:  BIT STRING
      0000 - 00 30 50 02 49 00 c2 cb-b2 4f db f9 23 b6 12 68   .0P.I....O..#..h
      0010 - e3 f1 1a 38 96 de 45 74-b3 ba 58 73 0c bd 65 29   ...8..Et..Xs..e)
      0020 - 38 86 4e 22 23 ee eb 70-4a 17 cf d0 8d 16 b4 68   8.N"#..pJ......h
      0030 - 91 a6 14 74 75 99 39 c6-e4 9a af e7 f2 59 55 48   ...tu.9......YUH
      0040 - c7 4c 1d 7f b8 d2 4c d1-5c b2 3b 4c d0 a3 02 03   .L....L.\.;L....
      0050 - 01 00 01                                          ...
banana_and_bread@yourMummy:~$ openssl asn1parse -i -dump -in ~/Downloads/rsa/pubkey.pem -strparse 17
    0:d=0  hl=2 l=  80 cons: SEQUENCE
    2:d=1  hl=2 l=  73 prim:  INTEGER           :C2CBB24FDBF923B61268E3F11A3896DE4574B3BA58730CBD652938864E2223EEEB704A17CFD08D16B46891A6147475
9939C6E49AAFE7F2595548C74C1D7FB8D24CD15CB23B4CD0A3
```

- Factorised n using http://factordb.com
- Found private key using this code.

- Converted cipher to binary file through:

  cat cipher | base64 -d > cipher.bin

- Decrypted file through:

openssl rsautl -decrypt -inkey private.pem -in cipher.bin -out text

Text:
up2l6DnaIhZgxA

Crypto basics 4

```
banana_and_bread@yourMummy:~/Downloads/rsa$ openssl rsa -pubin -inform PEM -text -noout < ~/Downloads/rsa_2mess/key1_pub.pem
RSA Public-Key: (1024 bit)
Modulus:
    00:ad:6d:d4:00:cd:d6:8e:ec:61:d7:c5:4b:15:67:
    e1:66:71:d7:40:1e:bb:a0:ab:e6:b3:91:57:5f:82:
    71:ee:ea:d7:8a:de:10:d0:96:4d:01:74:dc:fd:2e:
    54:13:dc:1a:07:5e:0e:7f:83:d1:43:bf:76:c1:c1:
    ab:a5:a5:01:10:3e:51:8c:51:71:14:9d:00:09:eb:
    d2:92:55:a2:f1:1d:be:56:99:bd:2f:a9:7f:ea:c9:
    22:9c:f0:7b:1e:aa:de:70:6d:79:25:3a:b9:d9:78:
    72:77:1e:6d:e6:51:e2:29:96:95:8f:7f:5f:42:ea:
    0a:0d:dd:b5:06:ae:b9:e2:c3
Exponent: 65537 (0x10001)
banana_and_bread@yourMummy:~/Downloads/rsa$ openssl rsa -pubin -inform PEM -text -noout < ~/Downloads/rsa_2mess/key2_pub.pem
RSA Public-Key: (1024 bit)
Modulus:
    00:ad:6d:d4:00:cd:d6:8e:ec:61:d7:c5:4b:15:67:
    e1:66:71:d7:40:1e:bb:a0:ab:e6:b3:91:57:5f:82:
    71:ee:ea:d7:8a:de:10:d0:96:4d:01:74:dc:fd:2e:
    54:13:dc:1a:07:5e:0e:7f:83:d1:43:bf:76:c1:c1:
    ab:a5:a5:01:10:3e:51:8c:51:71:14:9d:00:09:eb:
    d2:92:55:a2:f1:1d:be:56:99:bd:2f:a9:7f:ea:c9:
    22:9c:f0:7b:1e:aa:de:70:6d:79:25:3a:b9:d9:78:
    72:77:1e:6d:e6:51:e2:29:96:95:8f:7f:5f:42:ea:
    0a:0d:dd:b5:06:ae:b9:e2:c3
Exponent: 343223 (0x53cb7)
```

- Both keys have the same modulus,it looks like it is not OK, so probably there must be some attack exploiting thins.

- Following this tutorial this code was made. It decrypts ciphertexts.

Text:
Yeah man, you got the message. The flag is W311D0n3! and this is a padding to have a long text, else it will be easy to decrypt.
.