HITCON 2016 BambooFox Challenge write up – Part 2

```
Public-Key: (220 bit)
Modulus:
    0c:4a:c5:82:2c:39:b7:62:33:9c:5f:9a:50:97:94:
    c2:bf:90:35:aa:ab:2d:57:19:4b:1d:05:6b
Exponent: 65537 (0x10001)
-----BEGIN PUBLIC KEY-----
MDcwDQYJKoZIhvcNAQEBBQADJgAwIwIcDErFgiw5t2IznF+aU
Sx0FawIDAQAB
-----END PUBLIC KEY-----
```

目標：解出被 RSA 加密的 AES key → 用該 key 解出被 AES 加密的檔案 Bomb

觀察 1：Modulus 是 RSA 中的 N (16 進位)

作法(步驟一)：將 Modulus 轉成十進位數字 N

```
f = open('pub.pem.info')
input = f.read()
input = input[input.find("Modulus:"):input.find("Exponent")]
input = input[input.find("\n"):]
input = input.replace("\n","")
input = input.replace(" ","")
input = input.replace(":","")
m = int(input,16)
print m
```

作法(步驟二)：用 yafu 分解 N=p*q

作法(步驟三)：用 rsatool 和已知的 p 和 q 算出 private key

作法(步驟四)：用 openssl 解出被 RSA 加密的 AES key

```
$ openssl rsautl -in aeskey.rsa.enc -decrypt -inkey key
```

作法(步驟五)：用 openssl 解出被 AES 加密的 Bomb

```
$ openssl aes-128-cbc -d -in Bomb! -out answer
```

```
$ cat answer
```

```
tH1$_1$_H0w_y0U_$4vE_tHe_w0Rld_B4Mb00f0X
```

成功拯救世界，也學到了資安技術 :)