This repository   Search   Pull requests   Issues   Gist

📖 Beers4Flags / writeups

👁 Watch ▾ 6   ★ Star 8   ⑂ Fork 2

‹› Code   Issues 0   Pull requests 0   Projects 0   Wiki   Pulse   Graphs   ⓘ   ⑂   ▥   ▦

Branch: master ▾   Writeups / 2017 / yubitsec / crypto / rsa2 /   Create new file   Upload files   Find file   History

Ark1nar Yubitsec CTF - Write Up Crypto   Latest commit af115e3 2 days ago

..

📁 Src   Yubitsec CTF - Write Up Crypto   2 days ago

📄 Readme.md   Yubitsec CTF - Write Up Crypto   2 days ago

📖 Readme.md

```
RSA 2 - Crypto - 350

States :

  Can you decrypt these ciphertexts ?
```

Sources

Resolution:

The information contained in the public key is retrieved:

```
  Openssl rsa -in pubkey.pem -pubin -text -modulus


  Public-Key: (7470 bit)
  Modulus:
    3f:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:
    ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:
[...]
    00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
    00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
    00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
    00:00:00:01
  Exponent: 65537 (0x10001)
  Modulus=3FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
  -----BEGIN PUBLIC KEY-----
  MIIDxzANBgkqhkiG9w0BAQEFAAOCA7QAMIIDrwKCA6Y///////////////////
  /////////////////////////////////////////////////////////////
[...]
  AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
  AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
  AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
  AAAAAAABAgMBAAE=
  -----END PUBLIC KEY-----
```

We pass the modulo of hexa to int:

```
  sage : n=int("mon_modulo_en_hexa",16)
```

The length of the modulo is too high to be directly factorized

We will see if it has already been factorized on factordb

=> Full factorized: we have the two factors p & q

We recreate public keys with rsatool:

```
Python rsatool.py -p my_p -q my_q -f PEM -o privkey.pem
```

We decipher:

```
Openssl rsautl -decrypt -inkey privkey.pem -in cipher.txt
```

YUBITSEC {G00D_J0B_BRO_Y0U_MUST_KN0W_H0W_D03S_1T_W0RKS}

By team Beers4Flags

```
    _____
   |        |
   |  #BFF  |
   |_____|
    _··_,_|,_
   (    |   )
    ]~,"-.-~~[
  .=] Beers ([
  | ])  4  ([
  '=]) Flags [
    |:: '    |
      ~~----~~
```