ASIS 2015 Finals: Bodu (crypto175)

OCTOBER 14, 2015

Reading time ~1 minute

We got an RSA public key (pub.key) encoded in PEM format and the encrypted flag (flag.enc).

These are the converted parameters:

```
e = 23853301193316890834552115911829342614399993766164636485651785447041142855405233812146305031098886
N = 25622560187989822754955955895181634323720175022436018646585382747055379144839478071207837337661185
c = 16247689659782441222183849154402599497736230526191092653849605242040992414055093342982170120735742
```

The public exponent is too large thus we can suspect that the private exponent is possible too small.

I tried to attack it with Wiener's attack: https://en.wikipedia.org/wiki/Wiener%27s_attack with the following implementation, but it did not worked: https://github.com/pablocelayes/rsa-wiener-attack

So I remembered other RSA attacks from previous CTFs and how much time this page helped me: https://github.com/mimoo/RSA-and-LLL-attacks

The last attack is the Boneh Durfee attack, which is you know BO-neh DU-rfee => BODU just like the challenge's name, so I instantly know this will solve the challenge (also a lot of other teams are already solved it, so it should be not too hard challenge either).

Running budo.sage will give us the private exponent (d):

```
d = 895081866306385645134943864158654071476097023929492508646426254010599357513675 07
```

The executing pow(c,d,N) in python give us the following plaintext:

```
710585780145769608309866918037112518243090882527429586946226119699323233390484618208868245984590915 99
```

Converting this to ASCII (for example with my javascript based conversion tools, hosted on https://kt.pe/tools.html) will give us the flag (it is padded with PKCS v1.5 padding, but contrary to OAEP padding the flag is readable instantly):

```
ASIS{b472266d4dd916a23a7b0deb5bc5e63f}
```

ASIS ASIS2015FINALS CRYPTO

UPDATED ON OCTOBER 14, 2015 BY TAMÁS KOCZKA

ALSO ON KT.PE BLOG

ASIS 2015 Finals: Calm down – /var/log/security/kt.log

1 comment • 2 years ago•

Windu Putra Setiawan — flag invalid bro, why it can be?

ASIS 2015 Finals: Impossible – /var/log/security/kt.log

1 comment • 2 years ago•

abiusx — The point is that == comparison in PHP compares numbers, specially in case of 0e123457... which is scientific …

ASIS 2015 Finals: Giloph – /var/log/security/kt.log

1 comment • 2 years ago•

Epic Orange — > not with a safe primeNot that it was just not safe, moreover, it was smooth. There are many non-safe …

ASIS 2015 Finals: Myblog – /var/log/security/kt.log

1 comment • 2 years ago•

LamoniFinlayson — The "real" way to exploit this was to use the annotation tag in mPDF. You can find this in mPDF's …