ångstromCTF 2020

Crypto : Reasonably Strong Algorithm

Description : RSA strikes again!

Attachment : n = 126390312099294739294606157407778835887
e = 65537
c = 13612260682947644362892911986815626931

Solution :

For this challenge I used RsaCtfTool for crack the cipher (c).

Install it with the following commands.

```
root@kali:~# git clone https://github.com/Ganapati/RsaCtfTool.git
root@kali:~# cd RsaCtfTool
root@kali:/RsaCtfTool# apt-get install libmpc-dev
root@kali:/RsaCtfTool# pip2 install gmpy2
root@kali:/RsaCtfTool# pip2 install -r requirements.txt
root@kali:/RsaCtfTool# pip2 install -r optional-requirements.txt
root@kali:/RsaCtfTool# git clone https://github.com/hellman/libnum.git
root@kali:/RsaCtfTool# cd libnum
root@kali:/RsaCtfTool/libnum# python setup.py build
root@kali:/RsaCtfTool/libnum# python setup.py install
root@kali:/RsaCtfTool/libnum# apt-get install python3-crypto
```

Then uncipher it with RsaCtfTool.py and the parameter “-n Nvalue” “-e Evalue” “--uncipher Cvalue”.

```
root@kali:/RsaCtfTool# python RsaCtfTool.py -n 126390312099294739294606157407778835887 -e 65537 --
uncipher 13612260682947644362892911986815626931
[+] Clear text : actf{10minutes}
```

Alternatively you can use my tool (RsaCracker – rsa_part2.py), I’ve make it for the peaCTF2019 for the same challenge.

Source : https://github.com/V0lk3n/RsaCracker

Follow the readme on the github for install and use the tool.

Flag : actf{10minutes}