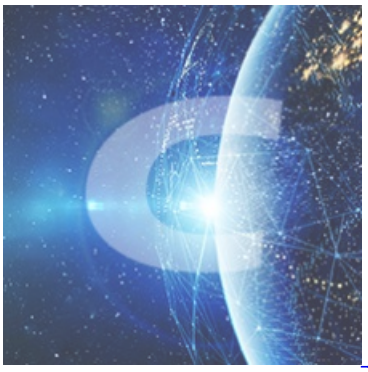
[Crypto/CTF]CTF Crypto 包函数和工具总结[2021/10/30更新]

原创

車鈇 于 2021-07-27 22:12:42 发布 358 收藏

分类专栏： # Crypto&MISC&BIN # 环境配置 文章标签： Crypto RSA Anaconda Ctf

本文链接：https://blog.csdn.net/DARKNOTES/article/details/119154603



Crypto&MISC&BIN 同时被 2 个专栏收录

2 篇文章 0 订阅

订阅专栏

环境配置

10 篇文章 0 订阅

订阅专栏

Crypto 函数和工具总结(持续学习...)

常用的库

采用Anaconda创建虚拟环境安装，然后设置环境变量或者在Pycharm当中导入。

Anaconda

以管理员权限运行anaconda prompt

(可解决 `UnsatisfiableError: The following specifications were found to be in conflict` 错误,即源未提供对应版本的依赖包，创建对应版本环境即可)

```
conda create -n python3.9 xxx # 创建虚拟环境，附带安装xxx包，可写多个)
activate python3.9   # 激活并进入环境
conda install xxx    # 安装xxx包
deactivate        # 退出环境
```

gmpy2

```
conda install gmpy2
```

pycryptodome

实际包名为`Crypto`，pycrypto、pycrytodome和crypto是相同的，但是第一个作为第三方库已经停止更新，需要3.7以上的python版本，

```
pip3 install pycryptodome
```

libnum

`libnum`库是一个关于数学运算函数库，

包含common maths、modular、modular squre roots、primes、factorization、ECC、converting、stuff

文档

```
pip3 install libnum
```

包函数基础使用方法

```
import gmpy2
gmpy2.mpz(n)   # 初始化一个大整数
n=invert(m,phi)   # 求mod phi的逆元
pow(m,e,n)     # 求c^d mod n
gmpy2.is_prime(n) # 素性检测
gmpy2.gcd(a,b)  # 欧几里得算法，最大公约数
gmpy2.gcdext(a,b)  # 扩展欧几里得算法
gmpy2.iroot(x,n) # x开n次根

import libnum
libnum.n2s(n)  # 数字转字符串，大端序
libnum.s2n(s)  # 字符串转数字，十六进制的位数奇偶都可，无需补零，大端序
libnum.b2s(b)  # 二进制转字符串，二进制的位数为8的倍数最佳
libnum.s2b(s)  # 字符串转二进制
s2b(n2s(n))   # 数字转二进制串，补零
libnum.generate_prime(1024) # 产生质数
libnum.factorize(1024) # 质数分解

from Crypto.Util.number import *
bytes_to_long(s)     # 把二进制串转化为长整型数字(大顶端)
long_to_bytes(n, blocksize=0)   # 把整型转化为二进制串
isPrime(N, false_positive_prob=1e-6, randfunc=None)   # 素数检验
```

常用工具安装

yafu

yafu 用于自动整数因式分解，原理是使用 Fermat 方法与 Pollard rho 方法等

RSA中可以快速分解的情况：1. p、q的取值差异过大；2. 取值相近

下载，https://sourceforge.net/projects/yafu/

```
.\yafu-x64.exe "factor(N)"    // 一般模式
.\yafu-x64.exe "factor(@)" -batchfile N.txt  // 待分解因数过长时，将其保存在yafu目录下文件N.txt(文件最后一行换行)中
```

rsa-wiener-attack

针对维纳攻击利用，当e很大的时候

https://github.com/pablocelayes/rsa-wiener-attack

下载手动导入可用

```
from RSAwienerHacker import hack_RSA
hack_RSA(e,n)
# 解得为d，在自行进行后续运算即可
```

RsaCtfTool

功能强大，详见文档，包括但不限于维纳攻击、小q等

下载，https://github.com/Ganapati/RsaCtfTool

我是初学者，详细用法请见大佬文章：RsaCtfTool的使用__Hydra的博客-CSDN博客__rsactftool

更新

UPDATE : 2021/10/30

问题解决1：gmpy2=>`fatal error: Python.h: 没有那个文件或目录`

详情

最近一次配置`gmpy2`库出现错误，记录一下,

```
src/gmpy2.c:404:10: fatal error: Python.h: 没有那个文件或目录
  404 | #include "Python.h"
      |          ^~~~~~~~~~
compilation terminated.
error: command 'x86_64-linux-gnu-gcc' failed with exit status 1
```

主要为:**fatal error:**

Python.h: 没有那个文件或目录

分析

这主要是由`python-dev`缺失导致的。

`linux`发行版通常会把类库的`头文件`和相关的`pkg-config`分拆成一个单独的dev包，

此库内含需要编译调用api的c/c++文件。

直接执行如下指令时，如果主机存在多版本的python可能导致不能正常安装到对应版本，

```
apt install python-dev
```

解决

需要执行以下指令，安装对应版本的`python-dev`，

```
apt install python2.7-dev
pip install gmpy2
```

或者，使用`aptitude`安装

测试

```
$ python
>>> import gmpy2
# 求逆元
>>> gmpy2.invert(17,379)
mpz(223)
```