ctf crypto工具篇

原创

STARSG0d 于 2019-11-06 14:46:00 发布 1458 收藏 9

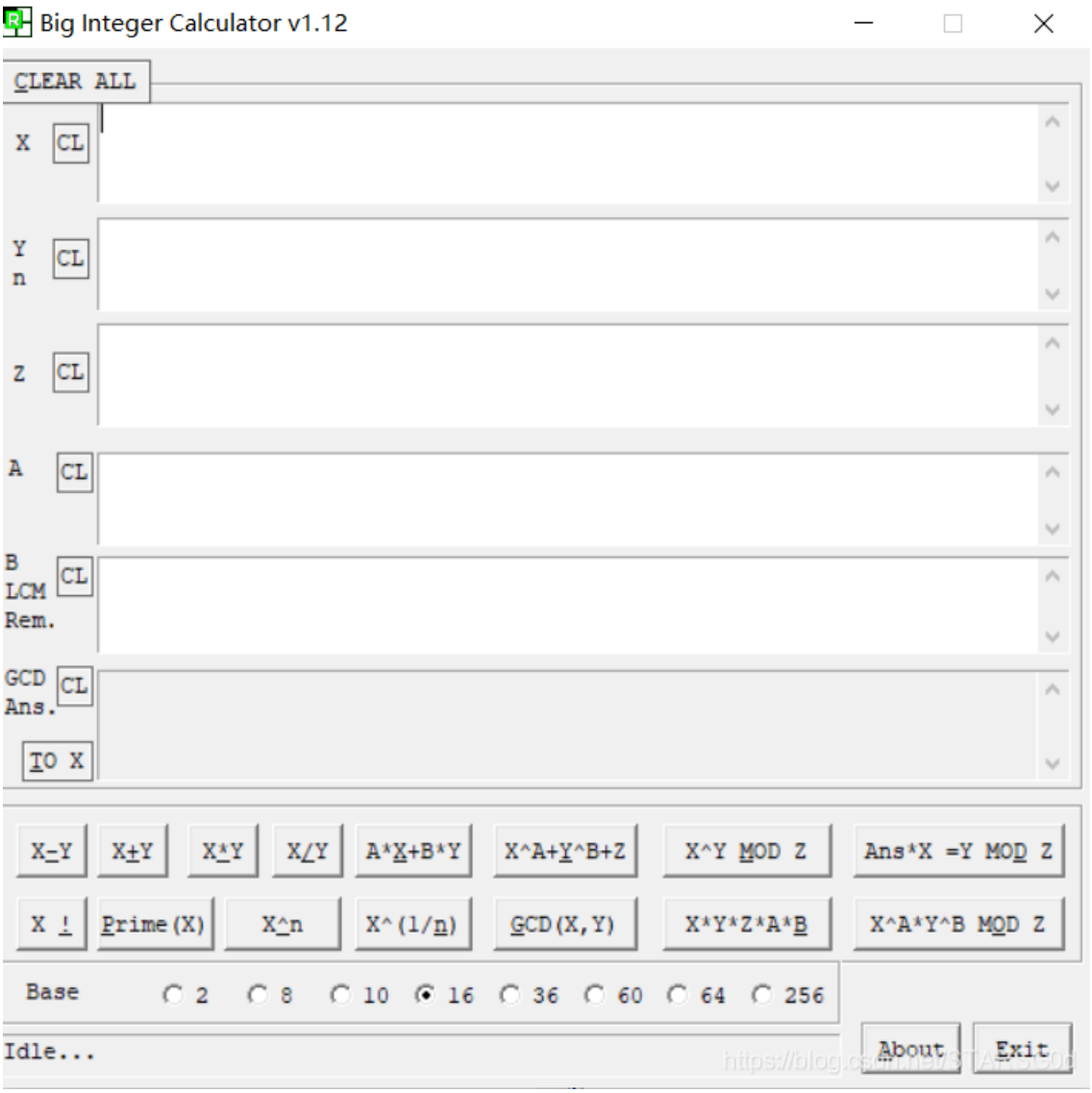
分类专栏： ctf 文章标签： ctf crypto 大整数 工具

本文链接：https://blog.csdn.net/STARSG0d/article/details/102934794

ctf大整数运算

在ctf比赛中crypto中经常会有一些大整数的运算，比较麻烦，这篇文章我将介绍一些工具，以及使用方法，十分方便。

Big Integer Calculator v1.12



1. 下面两排是计算公式，包括加法，减法，模运算等
2. 在Base中选择不同的进制运算
3. 没一个数值都有“CL”清除功能，“CLEAR ALL”清除全部

下载地址：https://bbs.pediy.com/thread-47934.htm

yafu

在cmd命令框下执行大整数的分解，有64和32位的应用程序可以执行

执行命令：factor(大整数)

你也可以在当前路径下打开cmd输入 “应用程序名称 factor()”，也可以完成

执行信息会保存在“factor log”文件里面

下载地址：https://sourceforge.net/projects/yafu/

（附：一个在线大整数的分解网站，不过位数有限http://factordb.com/index.php?query=100

RSATool

一款用于rsa算法解密的工具

1. 在进制选项选择需要的进制，加密指数也就是指“e”，key选择大小
2. 大素数选项中填写p,q,模式为n，私钥为“d”
3. 你也可以使用随机生成来获取大素数

下载地址：http://www.downcc.com/soft/142650.html

CTF-RSA-tool-master

也是rsa解密，它是基于python2的工具，里面还有一些经典例子可以学习

Ubuntu下安装教程：https://www.freebuf.com/sectool/185468.html

创作打卡挑战赛