hgame 2016 WriteUp： Week2

written by SSGSGoKu

written on Jan.27.2017

- Pentest

我是最简单的渗透题

题目的 hint 提示万能密码，百度搜索后得知万能密码为用户提交登陆表单时利用语法中的 bug，使数据库认为登录用户的 username 和 password 合法。有几个万能密码如图所示：

网站后台万能密码/10大常用弱口令 (2011-12-28 10:29:50)

标签： 杂谈 分类： oop安全

01: "or "a"="a
02: ')or('a'='a
03: or 1=1—
04: 'or 1=1—
05: a'or' 1=1—
06: "or 1=1—
07: 'or'a'='a
08: "or"="a'='a
09: 'or''='
10: 'or'='or'
11: 1 or '1'='1'=1
12: 1 or '1'='1' or 1=1
13: 'OR 1=1
14: "or 1=1
15: 'xor
16: 用户名 ' UNION Select 1,1,1 FROM admin Where ''=' （替换表名admin） 密码 1

PHP万能密码
'or 1=1/*

jsp万能密码
1'or'1'='1

01: 123456
02: 12345
03: 123456789
04: Password

由于不知道哪个万能密码可以使用，只好一个个试 ==，结果试到第 12 个 1 or '1'='1' or 1=1 成功，跳出 flag.

- RE

re 从零开始的逆向之旅：Gold Miner

打黄金矿工到第六关，目标钱数的位置为 flag，用鼠标全选后复制粘贴。只要每关都尽量把值钱的抓上来感觉难度还是可以接受的……

- Crypto

密码学教室进阶（五）

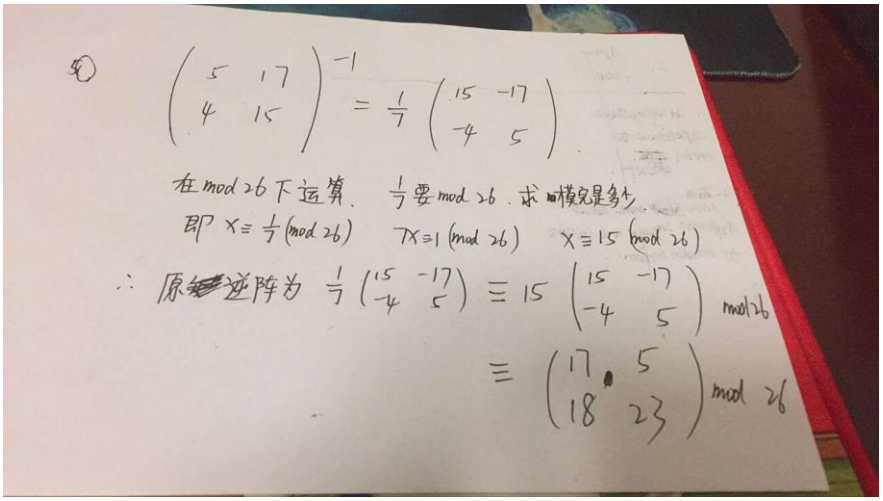
RSA 的题目，只不过这题没有给私钥需要自己算。用到的工具有 yafu（用于大数分解），BigNum（用于大数进制转换），Big Integer Calculator v1.14（仅支持 16 进制的大数计算，配合 BigNum 使用）。将 n 的 16 进制转换为 10 进制后再用 yafu 分解，得到两个素数 P8 和 PRP609 分别为 p 和 q，则 n 的欧拉函数值为（p-1）*（q-1），由此可算私钥 d

。d 算得后由 m≡c^d(mod N) 用 Big Integer Calculator 可算得 m，再用 hex to ascii 在线转换将其转换为 ascii 码值得 flag.

密码学教室进阶（六）

Hill 密码。一开始卡了很久在于不知道怎么算分数模掉一个整数的值。后来查了很多资料才发现可转化为一次同余方程求解。如

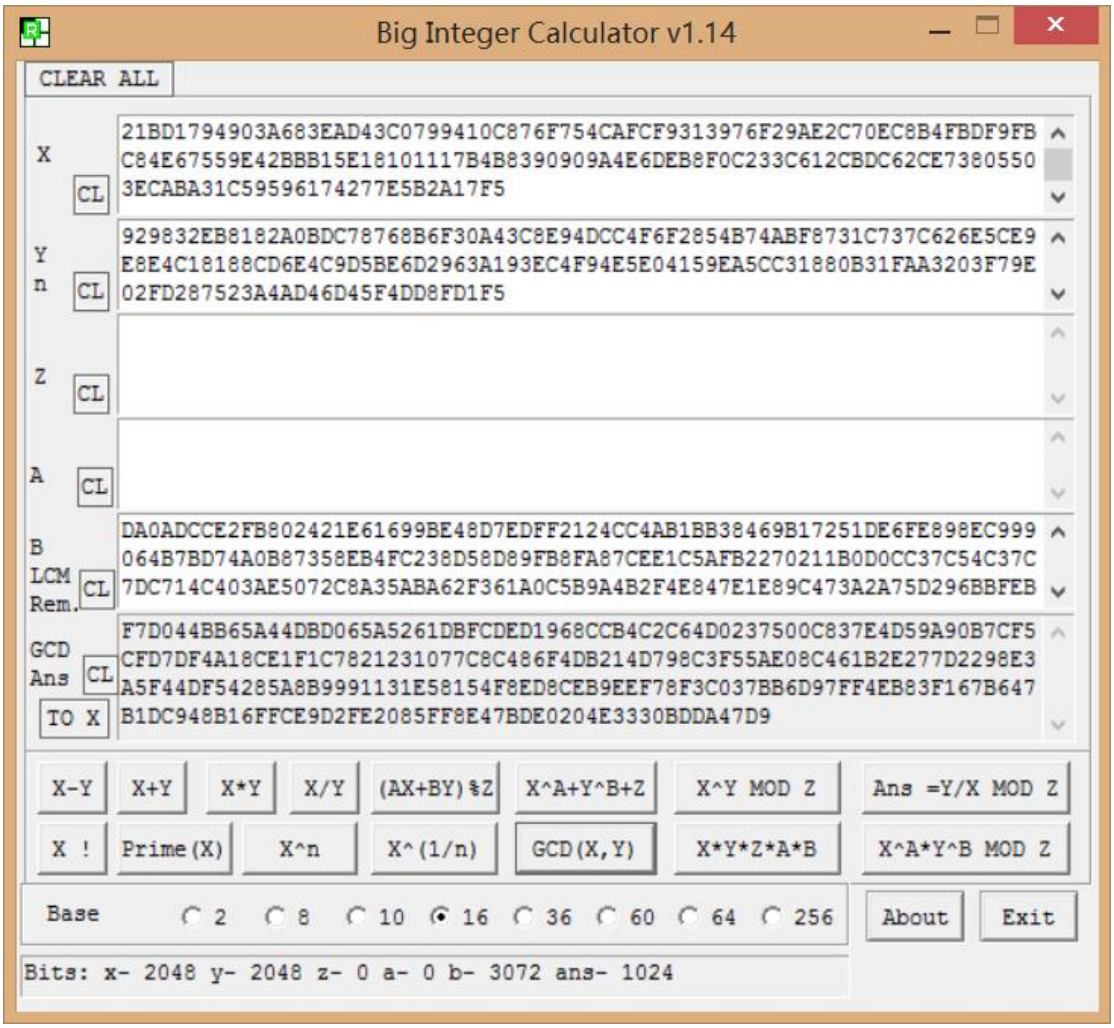
下图所示。



解密步骤:按照 wiki 上说的解密步骤,先将 key 写成 2x2 的矩阵,然后求其逆矩阵并将元素写成整数的形式（分数求模），将密文 2 个一组分组，写成列向量后分别用 key 去乘列向量，得到的序号即为 0-25 的整数，对应 a-z，再转化为英文字母加上 hgame{}即为 flag.

进击的 Crypto [0]

这题打开文档发现是若干组 n e c,感觉应该和密码学五的思路差不多，可是一开始理解错了题目方向，还以为是这么多组数据中只有一组是能解出 flag 的，加上用 yafu 分解这些 n 全都无法跑出结果，以为都是大素数,可是又没有一组能解出正确的 m,浪费了很长的时间。后来给了 hint 说 n 有共同点，尝试把这些 n 用 Big Integer Calculator 中求 gcd 的功能两两求了一下发现都相同，于是对于生成这些 n 的素数 p 或 q 中的一个必定是相同的，知道这点后很容易求出任一组数的 p 和 q，可解得 flag.（一开始可能由于计算问题，算到第 5 组数才算得明文得到正确的 flag，就立马认定一定是只有一组数能解出 m，询问出题的 dalao 后才知道所有的数都是可以解出的，自己一开始的计算肯定是出了问题…!）



（GCD Ans 显示的为这些 n 共同的素因数）

小小总结下，第二周时间比较紧，自己专攻密码学还是有了一定的进步，同时也意识到了课本知识和实际应用的巨大差距……继续努力！