crypto密码学知识大纲

原创

匡小萌 于 2020-07-17 20:18:19 发布

分类专栏： CTF

本文链接：https://blog.csdn.net/khy123khy/article/details/107416918

文章目录

概述

ctf-wiki https://ctf-wiki.github.io/ctf-wiki/crypto/introduction/

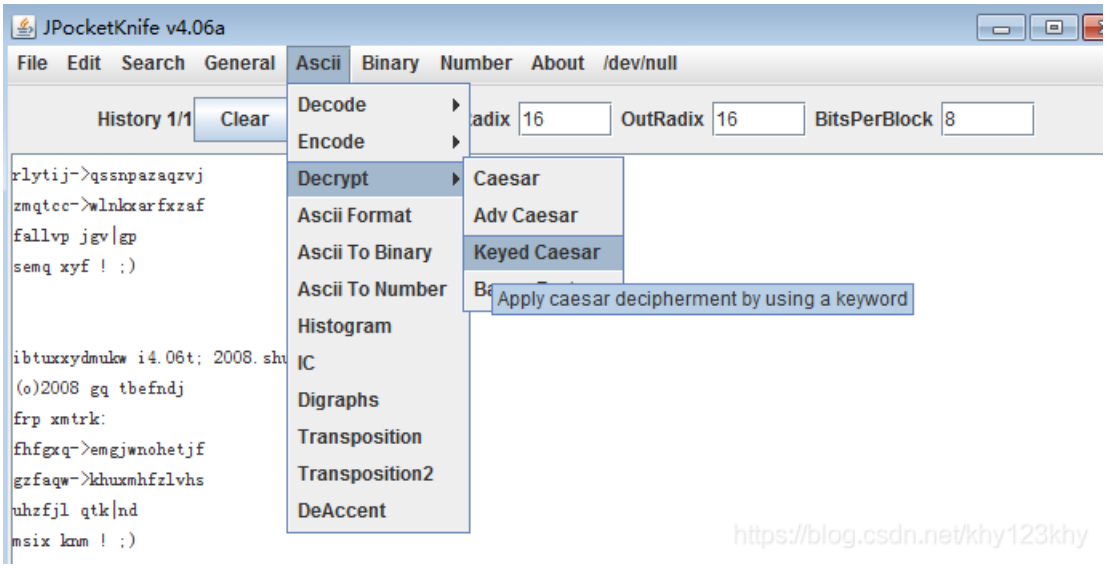
基本分类

古典密码

识别密码类型 加密方式，字符类型
##单表替换加密
特点：明文密文一一对应
破解：密钥空间小，暴力破解（2的64次方以内）；
密文长度长，词频分析(http://quipqiup.com/)
工具：CAP4
JPK
Cryptool

凯撒密码

明文中不同的偏移量，按照字母表中固定顺序
此外，还有还有一种基于密钥的凯撒密码 Keyed Caesar。其基本原理是 利用一个密钥，将密钥的每一位转换为数字（一般转化为字母表对应顺序的数字），分别以这一数字为密钥加密明文的每一位字母



JPK 解密凯撒
此图为解密知道密钥的凯撒，在空白框内键入密文，然后选择keyed Caesarsh输入密钥
还可以进行base64 等转换，功能挺强大

移位密码

字母和数字，特殊字符都能处理，ASCII表进行

atbash cipher(埃特巴什)

```
明文：A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
密文：Z Y X W V U T S R Q P O N M L K J I H G F E D C B A
```

词频分析

http://www.practicalcryptography.com/ciphers/classical-era/atbash-cipher/

简单替换密码

每个明文字母对应唯一的一个且不同的字母，完全混乱，26！数量太庞大

一般词频分析http://quipqiup.com/

仿射密码

加密函数

$$(ax+b)(mod m)$$

欧拉函数：

在数论中，对于正整数N,少于或等于N ([1,N]),且与N互质的正整数(包括1)的个数，记作φ(n)

$$\varphi(x)= x(1-1/p(1))(1-1/p(2))(1-\cdots$$

的所有质因数;x是正整数; φ(1)=1(唯一和1互质的数，且小于等于1)。

注意：每种质因数只有一个。

$$\varphi(10)= 10\times(1-1/2)\cdots$$

```
1379
```

破解：

首先特点一般都是26个字母，这种密码由两种参数来控制，如果我们知道其中任意一个参数，那我们便可以很容易地快速枚举另外一个参数得到答案

$$y_1 = (ax_1 + b) \pmod{26}$$
$$y_2 = (ax_2 + b) \pmod{26}$$

$$y_1 - y_2 = a(x_1 - x_2) \pmod{26}$$

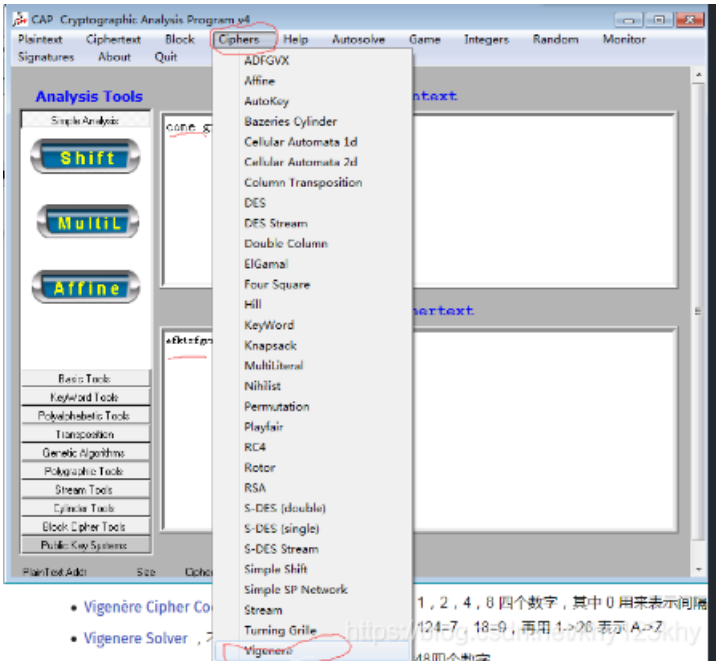
或者知道密文对应的两个不同的明文，则可以根据上式，求出a，然后可以枚举求出b

例子：TWCTF 2016 super_express ??

多表替换加密

维基利亚密码

已知密钥 可以直接用CAP4破解



未知密钥

https://www.mygeocachingprofile.com/codebreaker.vigenerecipher.aspx

https://www.guballa.de/vigenere-solver

hill密码

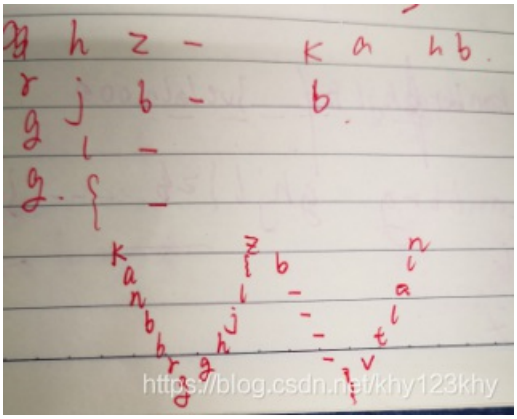
工具cap4

培根密码

只有两种字符，长度为5的倍数

栅栏密码

破解 可以Python暴力破解
这里发现了一个新大陆，国内和国外的栅栏竟然不一样，
http://www.practicalcryptography.com/ciphers/classical-era/rail-fence/
http://ctf.ssleye.com 这个解密工具也是根据国外的栅栏算法进行的
在线解的栅栏网站，国外的栅栏式“V”型进行解密，而国内一般是矩形的排列



7个作为一栏，然后在底部的是两栏共用，最后按照行从左至右的顺序进行加密
所以加密后的结果就是 kzna{blnl_abj_lbh_trg_vg}
变换成了类似 flag{} 的形式，然后想着凯撒解密
get。
PS：
此题的知识盲区就是对栅栏密码的了解只在矩形形式上，国外哪种V型不了解，而且是用其进行加密，以后遇到类似的可以试着不一定是解密，也可能是加密。

01248 云影密码

使用 0，1，2，4，8 四个数字，其中 0 用来表示间隔，其他数字以加法可以表示出 如：28=10，124=7，18=9，再用 1->26 表示 A->Z
只有01248四个数字

键盘密码

简单的替换密码.
采用坐标方法加密.
例:
21 = A; 22 = B; 94 = Z.
特点:第一项数字为2-9,第二项为1-4.

电脑键盘加密
例子：0ctf 2014 classic
2017 xman 选拔赛 一二三 木头人
阿里彩蛋，消失的三重密码（quip qiup）
2017 seccon vigenere3d

对称密码

加密和解密使用的密钥相同，需要传输密钥

流密码

流密码一般逐字节或者逐比特处理信息。一般来说

流密码的密钥长度会与明文的长度相同。
流密码的密钥派生自一个较短的密钥，派生算法通常为一个伪随机数生成算法。
伪随机数生成器（PRNG）
线性同余寄存器
例子：Google woodman
（比特位思想）
https://github.com/ctf-wiki/ctf-challenges/tree/master/crypto/streamcipher/prng/2016_google_ctf_woodman
线性反馈移位寄存器
例子：2018 强网杯streamgame1
https://ctf-wiki.github.io/ctf-wiki/crypto/streamcipher/fsr/lfsr/#2018-streamgame1
https://blog.csdn.net/qq_39153247/article/details/80144695
1.分析flag 的比特位 32，在范围内，可以暴力破解
2.矩阵变换，从a 0-a n-1 ,经过一次线性变换 a 1 -a n,输出an, 经过n次变换后，a n- a 2n-1,
矩阵中表示，a0*T^n=an ,从而乘以T^n的逆，得a0
非线性移位寄存器
例子：2018强网杯streamgame3
特殊流密码 RC4

块密码

DES
输入64位，输出64位，密钥64位
例子：2018 N1CTF N1ES
AES
攻击攻击 积分攻击、碰撞攻击、不可能攻击
例子：2018国赛 Crackmec
simoon block cipher
例子：
ECB
不同明文分组的加密
例子：2016 ABCTF aes-mess
https://github.com/ctfs/write-ups-2016/tree/master/abctf-2016/crypto/aes-mess-75
e220eb994c8fc16388dbd60a969d4953f042fc0bce25dbef573cf522636a1ba3fafa1a7c21ff824a5824c5dc4a376e75
对这个判断明文之间的长度，可以分为三段
CBC
padding Oracle attack
例子：2017 HITON Secret Server
https://github.com/p4-team/ctf/tree/master/2017-11-04-hitcon/secret_server
2017 SECCON Simon and Speck Block Ciphers

非对称密码

RSA

公钥与私钥的产生 ¶

1. 随机选择两个不同大质数 p 和 q，计算 $N = p \times q$
2. 根据欧拉函数，求得 $r = \varphi(N) = \varphi(p)\varphi(q) = (p-1)(q-1)$
3. 选择一个小于 r 的整数 e，使 e 和 r 互质。并求得 e 关于 r 的模反元素，命名为 d，有
   $ed \equiv 1 \pmod{r}$

4. 将 p 和 q 的记录销毁

此时，(N,e) 是公钥，(N,d) 是私钥。

然后 公钥为N+e，私钥为N+d，的拼接，

$$n^e \equiv c \pmod{N}$$

进行加密，其中n为消息经过某种编码转换成的数字，

$$c^d \equiv n \pmod{N}$$

进行解密，所以知道N,e,d就能解出

RSA的证明，可以看ctf-wiki

工具：RSAtool 生成私钥

```
python rsatool.py -f PEM -o private.pem -p 1234567 -q 7654321
```

RSA Converter

根据给定密钥对，生成pen.m文件（存储证书和密钥，实质上是base64编码的二进制内容）

根据n e d 得出p q

openssl

查看公钥文件

```
openssl rsa -pubin -in pubkey.pem -text -modulus
```

factor.db网站分解整数，yafu工具分解

Python 库 ：primefac（整数分解库）

gmpy2

pycrypto

例子：

Jarvis OJ - Basic - veryeasyRSA

https://github.com/ctf-wiki/ctf-challenges/tree/master/crypto/asymmetric/rsa/rsa-theory/JarvisOJ-Basic-veryeasyRSA

这道题直接给出了p , q ,e ,让求d，直接可以在Python中运用gmpy2库

gmpy2.invert(e,r)，此命令可以求e关于r的逆元即d

2018 CodeGate CTF Rsababy

https://github.com/ctf-wiki/ctf-challenges/tree/master/crypto/asymmetric/rsa/rsa-theory/2018-codegate-rsababy

对于这种根据RSA的原理来解题要分利用充分利用RSA中的已知条件e和d的逆元关系，即

$$ed \equiv 1 \pmod{r}$$

，然后试着分解N，或找出N与其他某数的公约数，求出p

所以呢，此题中变量g中包含d，不妨

$$eg = ed * (p - const)$$

这样ed就能发挥作用，

$$2^{eg} = 2^{ed*(p-const)} = 2^{p-const} \pmod{n}$$

$$2^{p-const} * 2^{const-1} = 2^{p-1} \pmod{n}$$

根据RSA解密的原理，消去e d

根据RSA解密的原理，消去ed，

$$2^{p-1} = 2^{eg} * 2^{const-1} + kn$$

把上面的第2个算式带入第3个，并把模展开，

$$2^{p-1}$$

然后看见 ，可能想到费马小定理（费马小定理(Fermat's little theorem)是数论中的一个重要定理，在1636年提出，其内容为： 假如p是质数，且
$gcd(a,p)=1$ ，

所以

$$p|gcd(2^{eg+const-1}-1,n)$$

gmpy2.powmod(a,b,c)求 a^b mod c
因此根据这个能求出来。

模数分解
例子：模数分解-光滑
smooth:Google一哈 光滑数是可以因式分解为质数相乘的正整数
primefac模块

哈希函数

MD5

```
0x67452301, 0xEFCDAB89, 0x98BADCFE, 0x10325476
```

MD5函数的初始IV，可以012345这样的顺序记忆
http://www.cmd5.com/ 破解

SHA1

```
0x67452301
0xEFCDAB89
0x98BADCFE
0x10325476
0xC3D2E1F0
```

初始IV
https://alf.nu/SHA1 破解
hashcat https://hashcat.net/hashcat/