加密：

1. 凯撒加密

凯撒加密是一种移位加密方式，将每一位字符的ascii码增加或减少固定的大小（超过字符的范围自动循环）。例如，aBcD向前移动3位变成xYzA。

Python代码有EncodeCaesar.py和DecodeCaesar.py可以使用。

EncodeCaesar用于凯撒加密，需要指定明文和加密时移动的步长，返回密文：

From EncodeCaesar import encoder

e=encoder()

e.func(明文，步长)

DecodeCaesar用于解密凯撒密码，输入密文，返回所有26种可能的凯撒明文及对应的步长：

From DecodeCaesar import decoder

d=decoder()

d.func(明文)

工具位置：D:\security\其他\工具汇总\8CTF\凯撒加密.exe

1. MD5和SHA1加密

MD5和SHA1是普通的hash加密，python代码有md5.py。

getMD5(明文)返回32位小写md5加密后的结果。

getSHA1(明文)范围32位小写sha1加密后的结果。

m = hashlib.md5()

m.update(s)

m.hexdigest() #return value

1. 摩斯密码

摩斯密码通过·和-的不同组合来表示不同的含义，具体加密方式可查看为知笔记。Python代码有morsecode.py（为了方便，用\*代替了·）。

* 1. 变种

摩斯编码只能由两种符号构成（一般为-和.），可以将这两种符号再进行一次加密，如ascii等。

这类变种情况的**特征就是密文只有两类**。

1. 素数分解

将一个大素数分解为两个素数因数，su.py算法很朴素，遍历3~大素数的平方根，寻找可能的素数因数并返回。

Input即为待分解的大素数，直接运行su.py即可。

1. Rsa加解密

Windows下可以用工具“\5破解工具\RSA文件解密.exe“

Kali下可以用openssl解密：

openssl rsautl -decrypt -in endata -inkey aaaa -out hello.de

1. 希尔密码

例：希尔密码：密文： 22,09,00,12,03,01,10,03,04,08,01,17 （明文：wjamdbkdeibr）

希尔密码是运用基本矩阵论原理的替换密码，由Lester S. Hill在1929年发明。

每个字母当作26进制数字：A=0, B=1, C=2... 一串字母当成n维向量，跟一个n×n的矩阵相乘，再将得出的结果模26。

注意用作加密的矩阵（即密匙）在必须是可逆的，否则就不可能解码。只有矩阵的行列式和26互质，才是可逆的。

* 1. 加解密过程

假设明文为ACT，因为A=0，C=2，T=19，则明文矩阵为

假设秘钥为

确认算法可逆，即秘钥的行列式和26互质

加密过程：

因此，对应的密文就是POH。

解密时，假设知道密文和秘钥，首先计算出秘钥的逆矩阵：

将逆矩阵和密文相乘：

得到原明文ACT

1. 栅栏密码

栅栏密码：把要加密的明文分成N个一组，然后把每组的第1个字连起来，形成一段无规律的话。

启明工具包中有解密工具。（5破解和8ctf中均有）

1. BrainFuck

一种特殊的编程语言，在Brainfuck官网和启明5.破解包中都能找到解密工具。形式如下：

++++++++++++[>++++>+++++>++++++>+++++++>++++++++>+++++++++>++++++++++<<<<<<<-]>>>>+++.<-----.>---.<+++.>>>>+++.<<<<----.>>>++++++.<<<<<+++.--.>>>>>----.<<<++++.<<+++.>>>>+++.>---.>++.

1. 培根密码

培根所用的密码是一种本质上用二进制数设计的。不过，他没有用通常的0和1来表示，而是采用a和b。

例如：a AAAAA g AABBA n ABBAA t BAABA

b AAAAB h AABBB o ABBAB u-v BAABB

c AAABA i-j ABAAA p ABBBA w BABAA

d AAABB k ABAAB q ABBBB x BABAB

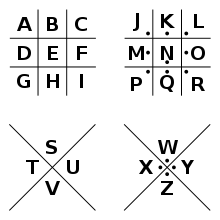
e AABAA l ABABA r BAAAA y BABBA

f AABAB m ABABB s BAAAB z BABBB

加密者需使用两种不同字体（一般是字体或大小写）。再准备一篇总字符数和明文AB编码后的字符数相等的假信息，使用两种字体分别代表A型和B型。因此假信息中的每个字母按字体来决定其代表“A”还是“B”。

1. 猪圈密码

猪圈密码又叫株高密码或者共济会密码,这是一种通过格子符号作为基础来代替的简单密码（如下图），这种密码规律性很强一般很容易破解。



1. CRC32

CRC为校验和的一种，是两个字节数据流采用二进制除法（没有进位，使用XOR来代替减法）相除所得到的余数。其中被除数是需要计算校验和的信息数据流的二进制表示；除数是一个长度为(n+1)的预定义（短）的二进制数，通常用多项式的系数来表示。在做除法之前，要在信息数据之后先加上n个0.

CRCa是基于有限域GF(2)（即除以2的同余）的多项式环。简单的来说，就是所有系数都为0或1（又叫做二进制）的多项式系数的集合，并且集合对于所有的代数操作都是封闭的。例如：

2会变成0，因为对系数的加法运算都会再取2的模数。乘法也是类似的：

我们同样可以对多项式作除法并且得到商和余数。例如，如果我们用除以。我们会得到：

也就是说，

等价于：

这里除法得到了商和余数-1，因为是奇数所以最后一位是1。

字符串中的每一位其实就对应了这样类型的多项式的系数。为了得到CRC，我们首先将其乘以，这里n是一个固定多项式的阶数，然后再将其除以这个固定的多项式，余数的系数就是CRC。

在上面的等式中，表示了本来的信息位是111, x+1是所谓的钥匙，而余数1（也就是）就是CRC. key的最高次为1,所以我们将原来的信息乘上来得到，也可视为原来的信息位补1个零成为1110。

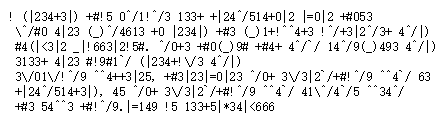
Python中自带的zlib.crc32()函数可以直接计算crc32。

1. rot

rot加密就是对字符进行置换加密，rot-N中的数字N就代表偏移的位数。rot-1就是偏移1位，rot-13就是偏移13位。rot加密只对字母进行置换，数字和特殊字符不发生变化，同时大小写属性保持不变。

1. leet speak

这其实相当于老外在网上使用的火星语，形式如下：



解密网站：<http://www.dcode.fr/leet-speak-1337>

图片隐写

(kali)工具收集：fcrackzip/fcrackzipinfo, imagemagick系列,identify,pcapinfo,pcapfix,gnuplot

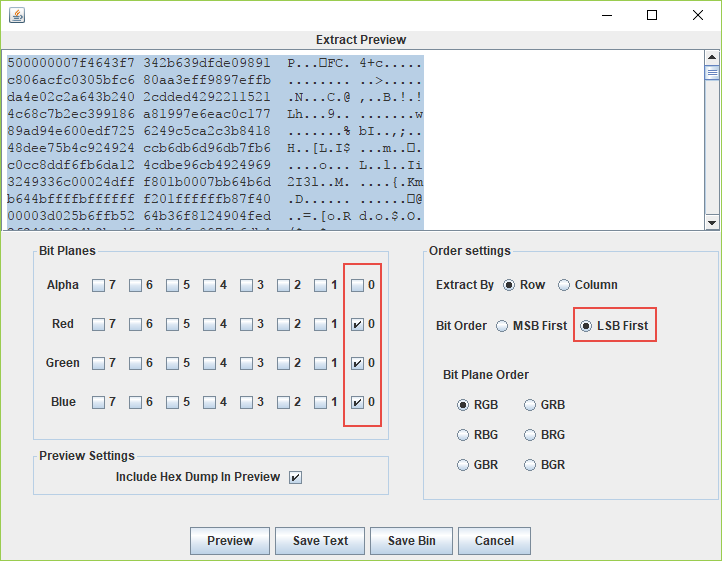
1. 图片通道隐写

在不同的图片通道中写入数据，使用工具：\5破解工具\Stegsolve-图片隐写解密.jar

* 1. LSB隐写

Least Significant Bit(LSB)隐写属于图片通道隐写的一种。在RGB图片中，每个像素点由RGB（不考虑A通道）由8bit构成，修改最低bit值人眼无法观察，因此可以用于信息隐写。

通过steg-solve.jar->analyse->data extract可以提取指定通道中的值。勾选各通道0位，LSB First，导出即可。



在使用LSB隐写时，还可能对隐写payload进行加密。

可参考：https://github.com/livz/cloacked-pixel

1. 双图隐写

Kali中的工具：binwalk。该工具可以分解出拼合的文件，不单单是图片。

命令：

Binwalk –e file //extract隐含文件

Binwalk –B file //查看各个隐含文件的偏移量

Foremost –T file //extract 图片文件

比较两个图片的区别，Kali中有工具：

Compare 1.jpg 2.jpg output.jpg

Stegsolve.jar也可以xor比较两张图片。

1. Gif图片帧/图层提取
   1. 图层内容隐写

\5破解工具\UleadGIFAnimator-v5.05

D:\security\其他\工具汇总\5破解工具\Namo\_GIF\_gr

Stegsolve可以分解图层（貌似也能分解gif帧）。

* 1. 基于时间的隐写

就是gif图片每一帧的内容是一样的，但是每一帧的持续时间不同，持续时间就是隐写的内容。

可以在kali下用indentify –format “%s %T” image.gif提取出每一帧的时间，再根据结果分析转码（如ascii等）。

1. 图片修复

将图片和一个正常的图片进行对比。

1. 二维码信息读取

\5破解工具\二维码扫描软件(WinPC)V1.0.0.21 官方版.exe

1. 文件属性或备注

文件属性或备注中可能会包含flag信息。

1. zip隐写
   1. 伪加密

zip文件的central directory header的deFlags（通用标记位）用于标记压缩文件的特性，其中包括是否加密（1或9时表示加密？）。

将未加密的正常zip文件的deFlags置为加密，则形成伪加密zip文件。

* 1. 真加密

暴力破解。。

* 1. crc32爆破

当加密文件内容较少时，考虑采用暴力枚举所有可能，然后计算crc32值来还原文件内容。

1. Word文档隐藏部分文字

Word文档可以通过 右键->字体->勾选隐藏 隐藏部分文字。

或字体颜色为白色。

1. 音乐文件隐含文本文件

音乐文件中隐含文本文件使用工具： 工具汇总\8CTF\MP3Stego\_GUI

1. 音频文件查看波形

D:\security\其他\工具汇总\10未测试\Cool Edit Pro\_Setup.exe

文件头尾信息

启明星辰【渗透测试工具包AIO2015\_07】\5破解工具\各类文件头标志大全.mht

1. png

见收藏夹

1. Jpg

Jpg文件以0xffd8开头，以0xffd9结尾。

1. Gif

Gif文件以gif89（或gif87，较老版本）开头

1. zip

见收藏夹

信息收集

1. 切换dns服务器

>Nslookup //

>server ip //设定dns 服务器地址

>ls 域名 //在指定的dns服务器查找域名对应的地址

总结

1. 基本操作

binwalk,strings,grep,foremost

1. recon
2. 图片
   1. 通用

* 二进制转化思路
  + ascii
  + qrcode（二维码）
  + 图形
* RGB像素操作
  1. JPG
* 文件格式
* software
  1. PNG
* 文件格式
* LSB
* software
  1. GIF
* 文件格式
* 时间轴
* 空间域

1. 音频

* 频谱
* 波形
* software

1. 压缩包

* 文件格式
* 爆破
  + 多重爆破
  + CRC32爆破
  + 明文攻击
* 伪加密

1. 流量包

* 文件修复 ----> pcapfix -n
* 协议分析
* 数据提取

wireshar -> file ->export

tshark –r –Y filter –T fields –e target|tr –d “\n”|awk|grep

python pypcap scapy

1. Other

pdf,html,bin,固件分析,pro,ntfs数据流