CTF 杂项 隐写术 密码学及编码 取证技术

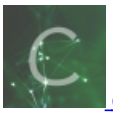
原创

SK Primin 于 2021-08-05 23:00:06 发布 304 收藏 5

分类专栏： ctf 笔记 文章标签： 密码学 加密解密

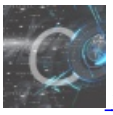
SKPrimn

本文链接：https://blog.csdn.net/m0_46530662/article/details/119429385


ctf 同时被 2 个专栏收录

2 篇文章 0 订阅

订阅专栏


笔记

116 篇文章 0 订阅

订阅专栏

隐写术

隐写术(steganography) : 将信息隐藏在其他载体中, 不让
计划的接收者之外的人获取到信息。

常见载体:图片、音频、视频、压缩包

图像隐写

图片:细微的颜色差别、GIF图多帧隐藏、Exif信息隐藏、图片修复

LSB(Least Significant Bit)最低有效位

1. 像素三原色(RGB)
2. 通过修改像素中最低位的1bit来达到隐藏的效果
3. 工具: stegsolve

将信息隐藏在动态图中,一闪而过,肉眼难以看到

1. 工具: stegsolve、Namo GIF、Photoshop

Exif (ExchangeableImage File)信息隐藏

1. 照片的Exif属性中可以保存大量信息

图片修复:

常见图片文件结构:

1. JPEG/JPG
   文件头标识(2 bytes) : FF D8
   一文件结束标识(2 bytes) : FF D9
2. PNG
   一文件头标识(8bytes):89 50 4E 47 0D 0A 1A 0A
3. GIF
   一文件头标识(6 bytes) : 47 49 46 38 39(37) 61
4. BMP
   文件头标识(2 bytes) : 42 4D

图片被损坏,缺少某部分数据如文件头等,需要对图片进行修复

工具: winhex

音频隐写

- 信息隐藏在声音里(逆序)
- 信息隐藏在数据里(分析音频数据)
- 工具: MP3stego、Audition、 Matlab

视频隐写

- 信息隐藏在视频的某个或多个帧里
- 工具: Premiere、会声会影等

文件隐写

- 文件拼接(copy /b 1.jpg+ 2.zip output.jpg)
- 工具: binwalk、dd、winhex

密码学及编码

古典密码学

凯撒密码（Caeser）

- 手动解密
- 在线工具凯撒密码在线加密解密 - 千千秀字 (qqxiuzi.cn)、凯撒密码在线计算-在线工具 (metools.info)、凯撒(Caesar)加密/解密 - Bugku CTF、凯撒密码加密/解密 - 一个工具箱 - 好用的在线工具都在这里！ (atoolbox.net)
- 使用python的pycipher模块

```
$pip install pycipher #安装pip工具
$python
>>> from pycipher import Caesar
>>> Caesar(key=5).encipher("HEL LOCAESAR")
>>> 'MJQQTHFJXFW'
>>> Caesar(key= 5).decipher("MJQQTHFJXFW")
>>> 'HELLOCAESAR'
```

ROT13(Rotate By 13 Places) :可以理解为一种特殊的凯撒密码。加密即解密，解密即加密。

栅栏密码

- 栅栏密码(Rail Fence Cipher)把要加密的信息分成N组，依次取各组的第1,2.3…位。

> 明文: HELLOWORLD
> 分组: HELLO WORLD
> 密文: HWEOLRLLOD (2栏)

> 栏数必须为密文长度的约数，明文长度与密文长度相同，通常偶数个
>
> 解密工具：栅栏密码在线加密解密 - 千千秀字 (qqxiuzi.cn)，栅栏密码_栅栏密码加密解密【基础型】-在线工具 (metools.info)、CTF在线工具-在线栅栏密码加密|在线栅栏密码解密|栅栏密码算法|Railfence Cipher (ssleye.com)

弗吉尼亚密码(Vigenere Cipher)

二维表单加密

> 明文: HELLOWORLD
> 密钥:GOOD
> 密文: NSZOUKCURR

- 解密工具：在线解密维吉尼亚密码在线加密解密 - 千千秀字 (qqxiuzi.cn)、维吉尼亚密码在线转换-在线工具 (metools.info)、维吉尼亚密码加密/解密 - 一个工具箱 - 好用的在线工具都在这里！ (atoolbox.net)、脚本

现代密码学

对称加密算法

- 特点:使用加密用过的密钥及相同算法的逆算法对密文进行解密,才能使其恢复成可读明文。即加密解密使用相同密钥。
- 常见对称加密算法: DES、3DES、 AES等。在线工具
- 使用在线工具进行加解密。

非对称加密算法

- 特点:加密和解密使用不同的密钥。公开密钥(Public Key)与私有密钥(Private Key)是一-对,如果用公开密钥对数据进行加密,只有用对应的私有密钥才能解密;如果用私有密钥对数据进行加密,那么只有用对应的公开密钥才能解密。
- 常见非对称加密算法: RSA、Elgamal、 背包算法、Rabin、 D-H、ECC

CTF中的密码

- 猪圈密码: 一种以格子为基础的简单替代密码。猪圈密码解密-在线工具 (metools.info)

培根密码: 一种由a和b构成的替换密码。培根密码 - Baconian Cipher - 在线工具网 (wtool.com.cn)

键盘密码:电脑键盘的位置模拟画出图案。

编码和摘要

- 加密(encipher/decipher) :加密传输信息,保证信息的安全性通过密钥和密文可以还原原始信息。
- 编码(encode/decode) :将数据转化成某种固定的格式的编码信息，方便不同系统间的传输,通过解码编码信息可以得到原始信息。
- 散列(hash) :也叫摘要或哈希,验证信息的完整性，不能通过哈希值还原原始信息。

编码

常见的编码: ASCII、 Base64、 UR编码、HTML 编码、Unicode、UTF-8、 摩斯电码、二维码

- Base64编码

Base64编码要求把3个8位字节(3*8=24)转化为4个6位的字节(4*6=24) ,之后在6位的前面补两个0 ,形成8位一个字节的形式。如果剩下的字符不足3个字节,则用0填充,输出字符使用'=',因此编码后输出的文本末尾可能会出现1或2个'='

- URL编码

为了解决URL中键值对规则的问题。http://xxx.com/?x=123&y= 456#test
将符号用ascii码的十六进制表示,并在数字前添加"%',如"<"的ascii码是60 ,转为十六进制是3C , URLencode后是%3C。

- JOTHER

匿名函数的原生形式，由[、]、(、)、{、}、+、!组成，可在浏览器的console直接还原

- JSFUCK

使用6个字符[、]、 (、)、!、+来编写JavaScript程序，可在浏览器的console直接还原

- 摩尔斯电码

摩尔斯电码(摩斯密码, Morse code)：用点、划、点和划之，间的停顿来表示字母和数字。

- 二维码

二维码(QR Code) : 用某种特定的几何图形按定规律在平面(二维方向上)分布的黑白相间的图形记录数据符号信息。

摘要

MD5 (Message Digest Algorithm 5) 特点:

- 压缩性:任意长度的数据,算出的MD5值长度都是固定的。
- 容易计算:从原数据计算出MD5值很容易。
- 抗修改性:对原数据进行任何改动，哪怕只修改1个字节， 所得到的MD5值都有很大区别。
- 强抗碰撞:已知原数据和其MD5值,想找到一个具有相同MD5值的数据(即伪造数据)是非常困难的。

SHA1 (Secure Hash Algorithm) :

主要适用于数字签名标准(Digital Signature Standard,DSS)里面定义的数字签名算法(Digital Signature Algorithm,DSA)。

隐写术、密码编码工具

隐写术常用工具：
Stegsolve.jar
010Editor / WinHex
Photoshop
Audition

密码编码工具：

在线加解密工具
Python脚本
CTF解密框架
(https://github.com/0Chencc/CTFCrackTools/releases)
Burpsuite的Decoder模块
(https://portswigger.net/burp/communitydownload/)

CTF取证技术

流量分析

Wireshark的基本使用方法:

- 筛选器的使用、追踪流、文件的导出
  - Wireshark筛选器
    协议筛选: http、ftp等
    IP地址筛选:ip.addr == 192.168.1.1

电子取证

日志分析:同过日志分析寻找隐藏在其中的信息。

SQL注入点的查找
WEBSHELL的查找
用户访问敏感路径的查找