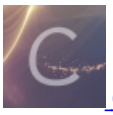
CTF Crypto 题目基础

原创

Daren_f0 于 2021-01-06 19:46:49 发布 382 收藏 4
分类专栏： CTF
版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。
本文链接：https://blog.csdn.net/qq_34423381/article/details/112294456
版权

CTF 专栏收录该内容
7 篇文章 1 订阅
订阅专栏
编码不同于加密，没有使用到密钥，只需要知道编码方式，就能得到原来的内容，因此了解常见的编码方式非常必要
如果本页面没有，请移步 Misc 项，或者直接谷歌（推荐）

常见编码方式

摩斯码 Jsfuck base家族 Uuencode等
古典密码：凯撒密码 栅栏密码 维基利亚密码等
分组密码：DES AES CBC比特反转
非对称密码学：RSA 模数安全性 指数安全性 复用安全性
哈希函数

常见编码解码

MD5

base家族：

- Base16：将二进制文件转换成由16个字符组成的文本
- Base32：由（A-Z、2-7）32个可见字符构成，“=”符号用作后缀填充
- Base64：由（A-Z、a-z、0-9、+、/）64个可见字符构成，“=”符号用作后缀填充

不常见编码解码

jsfuck：仅有 `[`、`]`、`(`、`)`、`!` 和 `+` 六种字符

uuencode

xxencode

jjencode：就是将正常的js代码转换成复杂的只有符号的字符串编码,进行加密
如：`[$._$_]+$._$+",\\"+$.$__+$.___+"\\"+$.__$+$.__$+$` 这样的组合

aaencode：将正常的js代码转为好玩的特殊网络表情符号，如: `ﾟωﾟﾉ= / ｀m´）ﾉ ~┻━┻ //*´∇｀*/ ['_']; o=(ﾟｰﾟ)` 这样的表情文字.

与佛论禅：佛经

brainfuck：仅有 `<>+-.,[]` 8 个字符

古典密码

凯撒密码：固定字母表偏移加密

栅栏密码

仿射密码

ROT13

维吉尼亚密码：使用一系列凯撒密码组成密码字母表的加密算法，属于多表密码的一种简单形式

猪圈密码：使用以格子为基础的简单替代式密码

键盘密码：一般来说是根据电脑键盘的位置进行加密获得密文

波利比奥斯棋盘密码

分组密码

DES

AES

CBC比特反转

非对称密码学

RSA

模数安全性

指数安全性

复用安全性

哈希函数

hash 一般使用hashlib进行程序编写

hash长度拓展攻击 https://github.com/bwall/HashPump

题目类型

唯密文攻击

已知明文攻击

选择明文攻击

选择密文攻击

题目形式：源码审计

学习方法

- WriteUp学习
- 学好数学
- 啃密码学书
- 论文

待更新。。。