ctf-crypto

原创

xiaohajunsky 于 2016-11-03 10:38:52 发布 2091 收藏

1.字母映射密码，每个字母对应随机的一个字母，所有的字母共有26！种排列方式，因此暴力破解是十分不可靠的。

由于英文中每个字母出现的频率是不同的，所以可以根据字母出现的频率进行分析，基于频率的替换字母

2.CRC32还原压缩（试用于小文件的解压缩，可能有碰撞）

文件在压缩之后会产生一个crc32校验值（文件夹除外）,打开压缩文件可见，如果文件长度很短，可以用枚举的方式进行破解，试用python自带的模块

引用模块 import binascii

试用函数 binascii.crc32(s)获得s的crc32校验值（十进制）,然后转换为16进制与0xFFFFFFFF相与然后与存在的crc32值相比较，如果相同则可能破解成功，但也可能是校验值相同的其他字符

3.分组加密

分组密码是一种对称加密算法，它将明文分成多个等长的分组，使用确定的算法和密钥对每个分组进行加密和解密操作，其中每个明文分组经过加密之后会产生一个等长的密文分组。

数据加密标准（DES，Data Encryption Standard）以及高级加密标准（AES，Advanced Encryption Standard）都属于分组密码。

分组密码有五种工作模式，包括：

1. 电码本模式（ECB, Electronic Code Book）；
2. 密文分组链接模式（CBC, Cipher Block Chaining）；
3. 密文反馈模式（CFB, Cipher Feedback）；
4. 输出反馈模式（OFB, Output FeedBack）；
5. 计数器模式（CTR, Counter）；