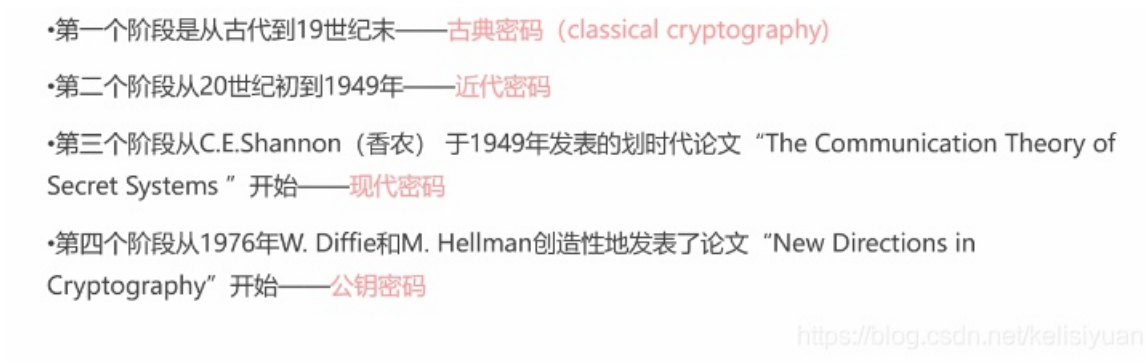
CTF crypto笔记（1）

原创

小源子先生 于 2019-12-19 17:50:37 发布

分类专栏： 网络攻防

本文链接：https://blog.csdn.net/kelisiyuan/article/details/103618140



现代密码大多不可逆

密码编码学

密码编码学是密码学的一个分支，研究与信息安全有关的数学技术。

对称加密与不对称加密

.对称密码算法(Symmetric cipher) :加密密钥和解密密钥相同，或实质上等同，即从-一个易于推出另一个。又称传统密码算法(Conventional cipher)、 秘密密钥算法或单密钥算法。

●DES、 3DES、 IDEA、 AES

非对称密码算法(Asymmetric cipher). : 加密密钥和解密密钥不同，从一个很难推出另-个。又叫公钥密码算法(Public-key cipher)。其中的加密密钥可以公开称为公开密钥(public key),简称公钥;解密密钥必须保密，称为私人密钥(private key),简称私钥。

●RSA（复杂）、 ECC、ElGamal

对称加密 相当于一把钥匙可以开门也可以锁门。

对称密钥的加密效率比非对称要高

AES世界上最长的密钥

摘要算法

数据摘要算法是密码学算法中非常重要的一个分支,它通过对所有数据提取指纹信息以实现数据签名、数据完整性校验等功能,由于其不可逆性,有时候会被用做敏感信息的加密。

也称为hash算法

常见算法：MD5 、SHA

MD5 校验数据完整性，也可看出是否添加有其他后门，病毒程序。

SHA中SHA1的应用较为广泛，主要应用于CA和数字证书中，另外在互联网中流行的BT软件中，也是使用SHA1来进行文件校验的，由于SHA系列算法的数据摘要长度较长，因此其运算速度与MD5相比，也相对较慢。

常见编码

ASCII编码

ASCII码使用指定的7位或8位二进制数组合来表示128或256种可能的字符。标准ASCII码也叫基础ASCII码，使用7位二进制数(剩下的1位二进制为0)来表示所有的大写和小写字母，数字0到9、标点符号，以及在美式英语中使用的特殊控制字符。

一开始只有7位 128

到扩充其他国家语言 256

Base64编码

Base64顾名思义就是用64个可显示字符表示所有的ASC字符，64也就是6Bits, 而ASC字符一共有256个也就是8Bits。Base64编码要求把3个8位字节(38=24) 转化为4个6位的字节(46=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

url编码就是-个字符ascii码的十六进制。不过稍微有些变动，需要在前面加上"%"。比如"\" ,它的ascii码是92, 92的十六进制是5c,所以"\" 的url编码就是%5c。特点:密文中有多个%号符

正常情况下不对字母做编码转换

Unicode编码

Unicode码扩展自ASCII字元集。在严格的ASCII中， 每个字元用7位元表示，或者电脑上普遍使用的每字元有8位元宽;而Unicode使用全16位元字元集。这使得Unicode能够表示世界上所有的书写语言中可能用於电脑通讯的字元、象形文字和其他符号。

特点:密文中有多个\uxxx

JS混淆

有些时候开发者为了保护劳动成果可以通过对javascript的变量名称和过程名称进行编码，从而起到混淆js代码的作用，通常使用eval函数进行混淆处理,该函数可以计算字符串，并执行其中的JS代码。

如，对进行16进制转换，然后使用eval函数进行读取

特点:通常在JS脚本里使用eval与function函数进行混淆。

凯撒密码

在密码学中，恺撒密码（英语：Caesar cipher），或称恺撒加密、恺撒变换、变换加密，是一种最简单且最广为人知的加密技术。它是一种替换加密的技术，明文中的所有字母都在字母表上向后（或向前）按照一个固定数目进行偏移后被替换成密文。

密码在明文中，只不过发生了偏移

凯撒密码也可做维吉尼亚密码的一部分

维吉尼亚密码（又译维热纳尔密码）是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。意味着，在一段密文中，每一部分都需要不同的凯撒密码解密偏移量 …

感觉凯撒密码没有什么特征，只能看是不是乱文，作为尝试解密的一个选项。

维

栅栏密码

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

提示：一只羊跳过了N个栅栏

Brainfuck/Ook!编码

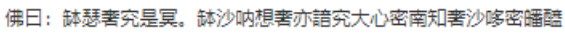
周日做的一道题，特征为出现类似+++++ +++++ [->++ +++++ +++<] 的字符

ROT13

之前博客提到的回转加密，可以进行连续加解密。

与佛论禅

emmm 很佛系的一道题，



特征　　乱文汉字

听说实质是AES加密（对称加密）和替换字符

解密地址

http://www.keyfc.net/bbs/tools/tudoucode.aspx

社会主义核心价值观

不得不说，创出这种加密方式的人简直是人才…

网址：http://z.duoluosb.com/?btwaf=62118251

Rabbit加密

特征

明文I Love You小可爱无密匙加密后密文为U2FsdGVkX1/ouFei55jKdzY1fWNS4jxHVNf/AfKWjnBrOGY=

明文I Love You 521无密匙加密后密文为U2FsdGVkX19DvuEo5PvBA8TuLrM2t+EZBvUkzlAa

明文I Love You 521密匙为666加密后密文为U2FsdGVkX18w6vxXxux/ivRVwo3xMzTxmUyk7cHz

解密网址：https://www.sojson.com/encrypt_rabbit.html

遇到再更 待续~