CTF-Crypto密码学

原创

彬彬有礼am_03 于 2021-08-23 13:31:47 发布 254 收藏 2

分类专栏： CTF基础

本文链接：https://blog.csdn.net/am_03/article/details/119867126

CTF基础 专栏收录该内容

9 篇文章 0 订阅

订阅专栏

密码学

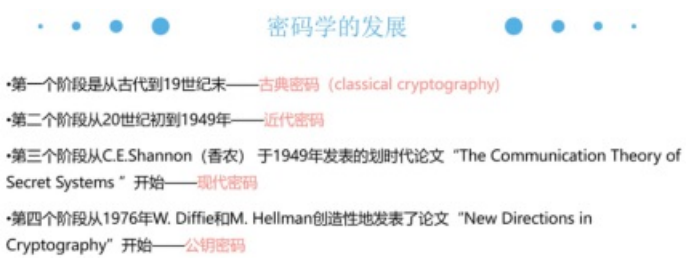
01密码学概述

一、密码学概述

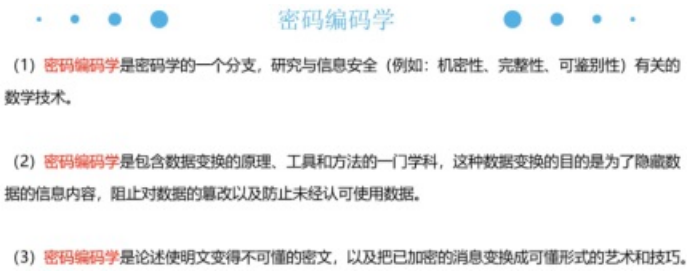
- 目的：为了保证数据传输的可靠性
- 核心：密码学；（用于数据动态传输和静态存储）

- 方法
  - 编码：相当于有一张映射表；红豆
  - 加密：需要算法和密钥，较为复杂
  - 摘要

密码学的发展

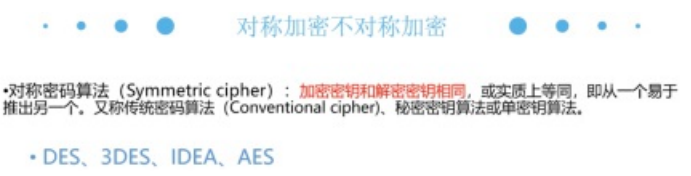


密码编码学



编码与加密？
编码为一类映射的关系(一一映射)
加密为一类算法(有算法(公开的)，密钥(不可泄漏))
明文 ------> 密文
plain text cipher text

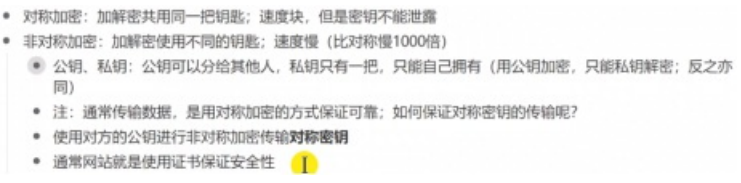
对称密码和不对称密码算法



对称密码算法优点：加密解密速度快
缺点：密钥不能泄漏(除了AES，因为密钥很长，目前无机器能够在短时间内破解)
对称密码算法常考DES

非对称密码算法(Asymetric cipher):
加密密钥和解密密钥不同，从一个很难退出另一个。又叫共要密码算法(Public-key cipher)。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。
如RSA,ECC,ElGamal

非对称密码算法优点：速度慢(比对称慢1000倍)
非对称密码算法常考RSA



摘要算法：

摘要算法

数据摘要算法为密码学算法里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，有时候会被用作敏感信息的加密。数据摘要算法也被称为哈希(Hash)算法，散列算法，常见的摘要算法有MD5和SHA。

在互联网上进行大文件传输时，都要得利用MD5算法产生一个与文件匹配的，存储MD5值的文本文件(后缀名为.md5或.md5sum)，这样接收者在接收到文件后，就可以利用与SFV类同的方法来检查文件完整性，绝大多数大型软件公司或者开源组织都以这类方式来校验数据完整性，而且部分操作系统也利用此算法来对用户密码进行加密，另外，它也是目前计算机犯罪里数据取证的最常用算法。

SHA里SHA1的应用较为广泛，主要应用于CA和数字证书里，另外在互联网里流行的BT软件里，也是利用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。

摘要：雪崩效应（哪怕只改变1bit）和不可逆（无法逆推）

编码

二、编码

- ASCII：7到8位，最多表示256个字符
- base系列：特征末尾有=
- URL：%两个十六进制数
- Unicode：\u
- JS系列

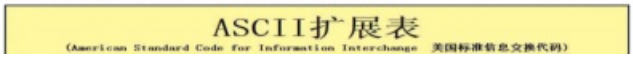
02 常见编码

ASCII编码

ASCII编码

ASCII码利用指定的7位或8位二进制组合来表示128或255类可能的字符。标准ASCII码也叫基础ASCII码，利用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，以及在英语里利用的特殊控制字符。

后128个称为扩展ASCII码。许多基于x86的系统都支持使用扩展（或“高”）ASCII。扩展ASCII 码允许将每个字符的第8 位用于确定附加的128 个特殊符号字符、外来语字母和图形符号。



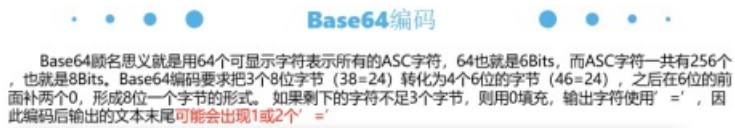
ASCII在线转换地址：http://www.mokuge.com/tool/asciito16/

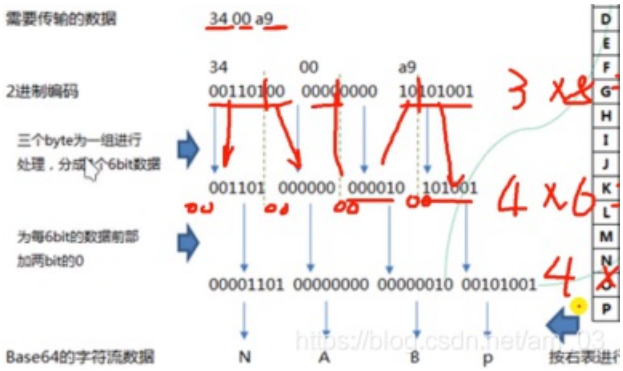
在python控制台里ord(‘a’)

CTF竞赛一个强功能的解密加密网站：http://ctf.ssleye.com

Base64编码：

Base64编码





第一行：3乘8=24

第二： 4乘6=24

第三： 4乘8=32

base64也有自己的base64表

base64解密可能会出错，可在后面加上一个或两个“=”

此题注意：base为base64,但base的表妹为base32

若以base64编码来解密，在密文后面去掉一个“=”，两个“=”，三个“=”甚至“=”都去掉会发现找不到flag，但以base32编码来解密可成。

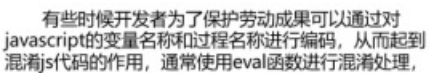
URL编码：

特点：密文里有多个%字符

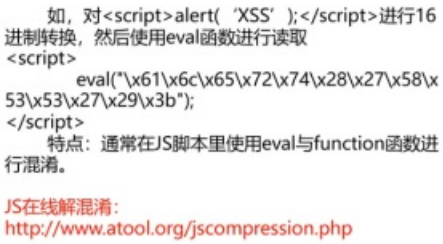
Unicode编码：

Unicode码扩展自ASCII字元集。在严格的ASCII里,以7位元表示一个字元,或电脑普遍采用的每字元有8位元宽；而Unicode采用全16位元字元集。这令Unicode能够表示所有语言里可能用于电脑通讯的字元和其他字符。
特点：密文里有多个\uxxx

JS混淆(并不是一个编码方式)：



此函数可以计算字符串，并执行其里的JS代码



JS在线解混淆：
http://www.atool.org/jscompression.php

例题1：

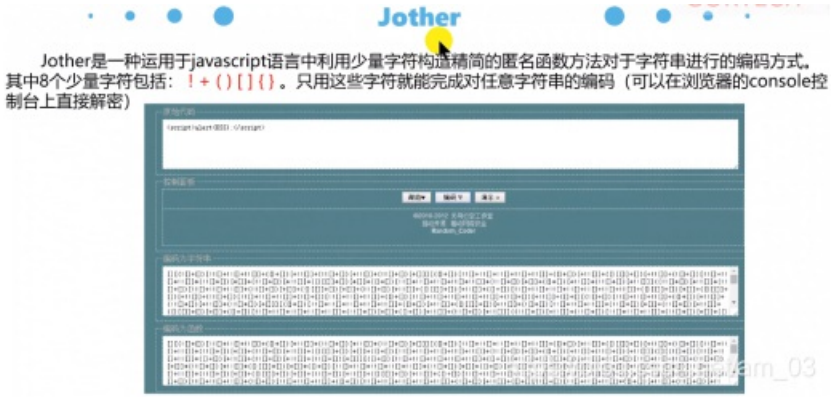
在浏览器按F12，点击控制台，在>>处输入密文，会车即可，得到“alert(“key”)”

例题2：

会车会弹出一个弹窗，

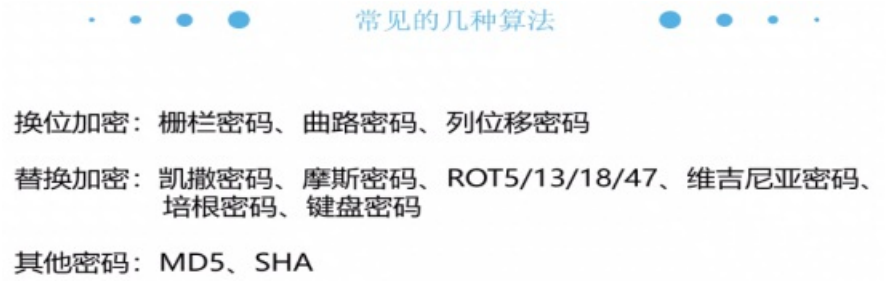
XSS并不是flag，flag即为alert('XSS')

JSfuck：



若出现没有[]，而有{}，就注意可能需要将{}改为[].

03 常见加密算法



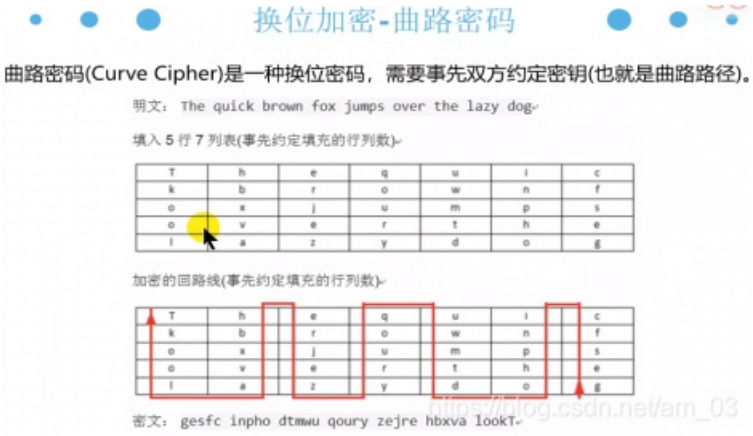
换位密码-栅栏密码

第一组：分组里的第一个字母
第二组：分组里的第二个字母

例题：

提示3组分别为yawce oreo@ uelm@
y a w c e
yo ar we co e@
you are wel com e@@
即为youarewelcome@@

换位加密-曲路密码

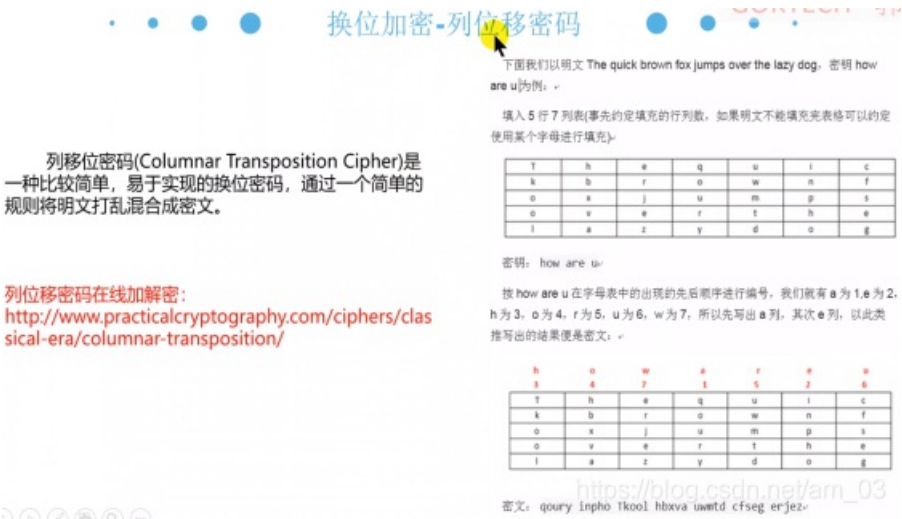


5行7列即为每5行就有一个空格

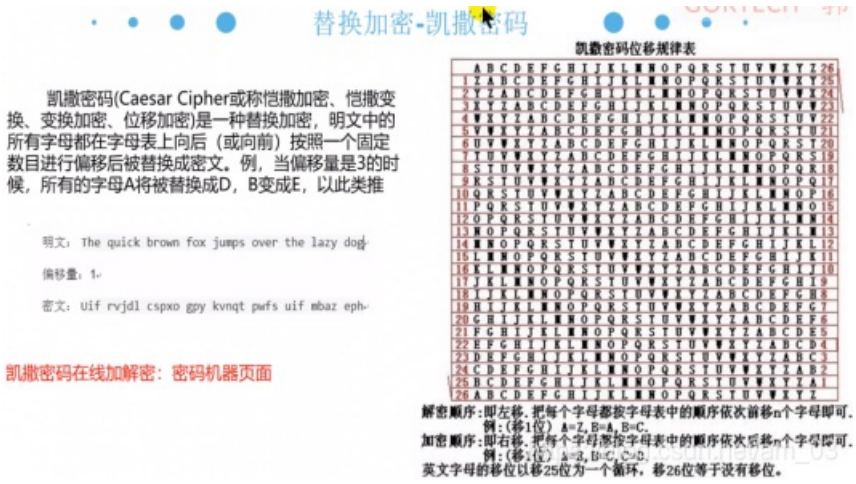
路径分为先上后下和先下后上
例题：

此题四个字母就有一个空格
首先先看先上后下：
c o n g r a t
u l a t i o n
t o y o u g e
t t h e k e y
从左向右看：congratulation to you get the key

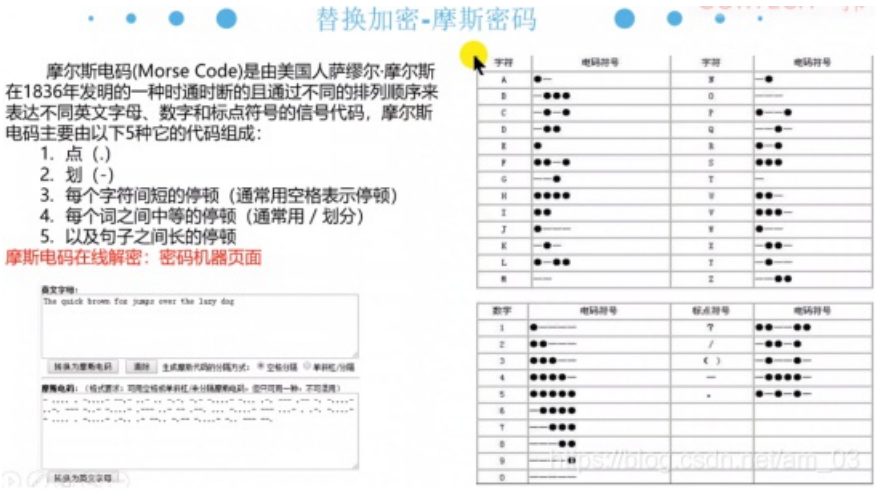
一般夺旗看key,flag,CTF,CTF{},flag{}等关键



替换加密-凯撒密码



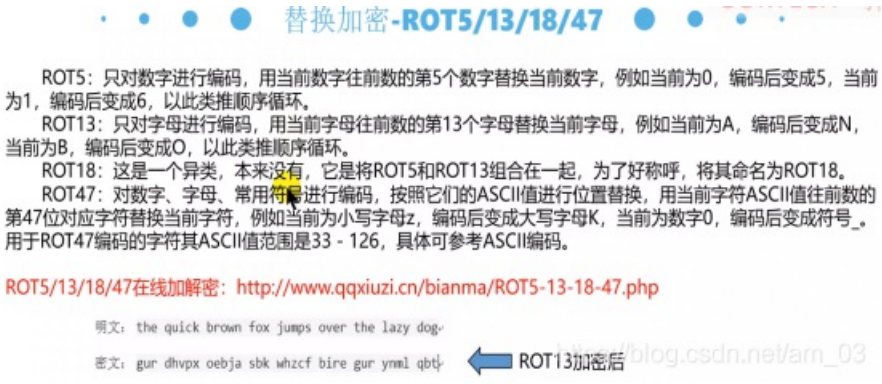
替换加密-摩斯电码



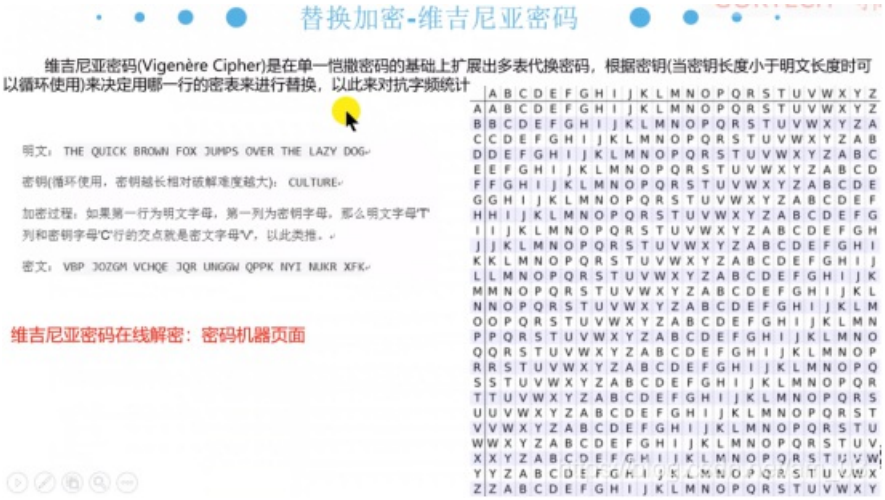
例题：

打开密码工具的离线工具，点击摩斯电码，在密文框里加入密文，在上方的“点”框加入*，右边加入-，字母间隔加入空格即可点击解密，得到give you the key

替换加密-ROT5/13/18/47

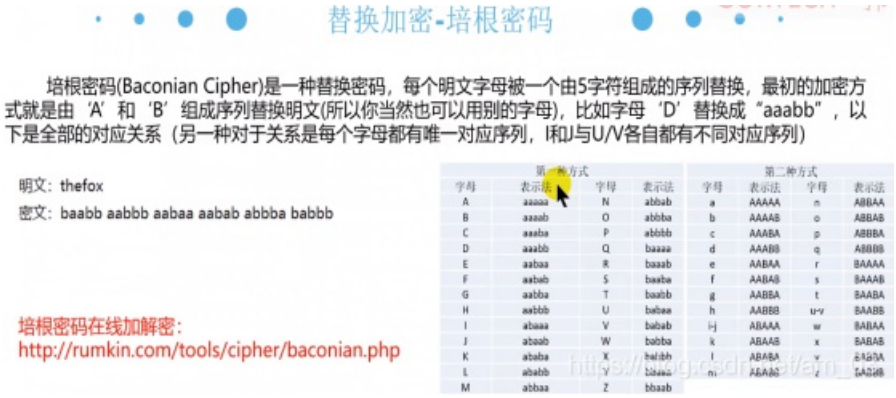


替换加密-维吉尼亚密码

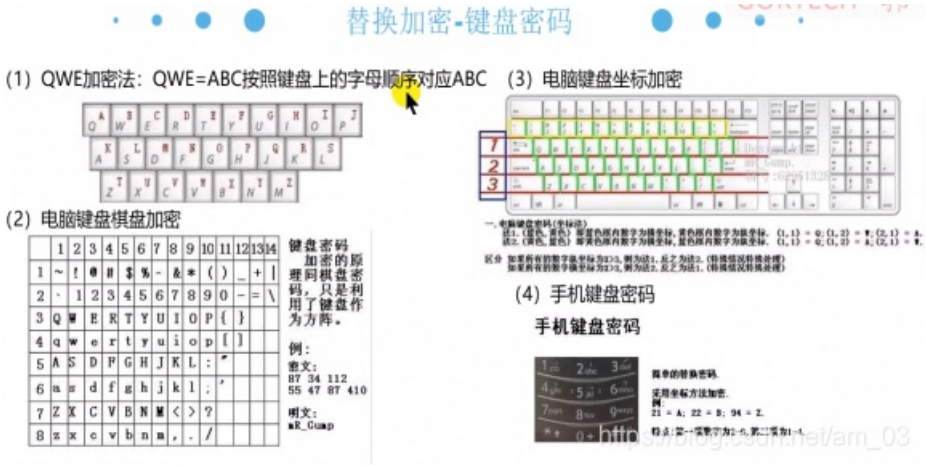


维吉尼亚解密网站：https://www.guballa.de/vigenere-solver

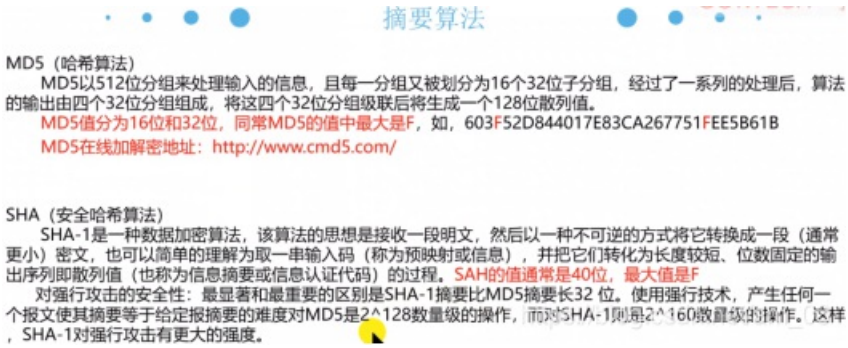
替换加密-培根密码



替换加密-键盘密码


替换加密-键盘密码
(1) QWE加密法：QWE=ABC按照键盘上的字母顺序对应ABC
(2) 电脑键盘棋盘加密
键盘密码
加密的原理同棋盘密码，只是利用了键盘作为方阵。
例：
密文：
87 34 112
55 47 87 410
明文：
aK_Cuap
(3) 电脑键盘坐标加密
(4) 手机键盘密码
手机键盘密码

04 摘要算法


摘要算法
MD5（哈希算法）
MD5以512位分组来处理输入的信息，且每一分组又被划分为16个32位子分组，经过了一系列的处理后，算法的输出由四个32位分组组成，将这四个32位分组级联后将生成一个128位散列值。
MD5值分为16位和32位，同常MD5的值中最大是F，如，603F52D844017E83CA267751FEE5B61B
MD5在线加解密地址：http://www.cmd5.com/
SHA（安全哈希算法）
SHA-1是一种数据加密算法，该算法的思想是接收一段明文，然后以一种不可逆的方式将它转换成一段（通常更小）密文，也可以简单的理解为取一串输入码（称为预映射或信息），并把它们转化为长度较短、位数固定的输出序列即散列值（也称为信息摘要或信息认证代码）的过程。SAH的值通常是40位，最大值是F
对强行攻击的安全性：最显著和最重要的区别是SHA-1摘要比MD5摘要长32 位。使用强行技术，产生任何一个报文使其摘要等于给定报摘要的难度对MD5是2^128数量级的操作，而对SHA-1则是2^160数量级的操作。这样，SHA-1对强行攻击有更大的强度。