

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](#)

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/am_03/article/details/119867126

版权



[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

02

常见编码

03

常见加密算法

04

摘要算法

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 **I**

密码学的发展

密码学的发展

- 第一个阶段是从古代到19世纪末——**古典密码 (classical cryptography)**
- 第二个阶段从20世纪初到1949年——**近代密码**
- 第三个阶段从C.E.Shannon (香农) 于1949年发表的划时代论文 "The Communication Theory of Secret Systems" 开始——**现代密码**
- 第四个阶段从1976年W. Diffie和M. Hellman创造性地发表了论文 "New Directions in Cryptography" 开始——**公钥密码**

密码编码学

密码编码学

- (1) **密码编码学**是密码学的一个分支, 研究与信息安全 (例如: 机密性、完整性、可鉴别性) 有关的数学技术。
- (2) **密码编码学**是包含数据变换的原理、工具和方法的一门学科, 这种数据变换的目的是为了隐藏数据的信息内容, 阻止对数据的篡改以及防止未经认可使用数据。
- (3) **密码编码学**是论述使明文变得不可懂的密文, 以及把已加密的消息变换成可懂形式的艺术和技巧。

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

对称加密不对称加密

• 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

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(Asymmetric cipher):

加密密钥和解密密钥不同, 从一个很难推出另一个。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,EIGamal

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

- 对称加密: 加解密共用同一把钥匙; 速度快, 但是密钥不能泄露
- 非对称加密: 加解密使用不同的钥匙; 速度慢 (比对称慢1000倍)
 - 公钥、私钥: 公钥可以分给其他人, 私钥只有一把, 只能自己拥有 (用公钥加密, 只能私钥解密; 反之亦然)
 - 注: 通常传输数据, 是用对称加密的方式保证可靠; 如何保证对称密钥的传输呢?
 - 使用对方的公钥进行非对称加密传输**对称密钥**
 - 通常网站就是使用证书保证安全性 **!**

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



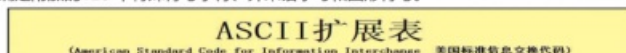
02 常见编码

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、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')

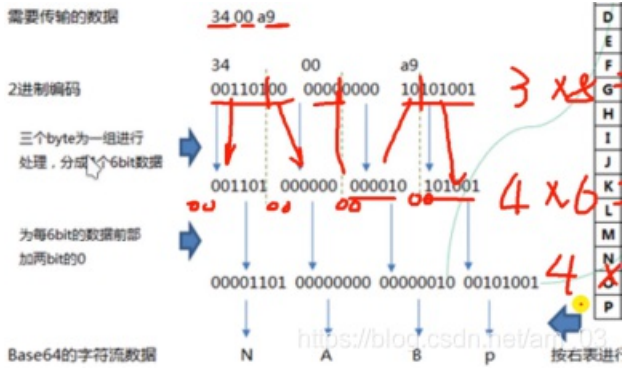
CTF竞赛一个强功能的解密加密网站：<http://ctf.ssleye.com>

Base64编码：

Base64编码

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（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“=”。



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“=”

“百度杯” CTF比赛 十月场

分值: 10分 类型: Misc 题目名称: 那能带我走过的贝壳 已解答

题目内容: 贝壳贝壳, 我爱你 (大声循环2的6次为ing)
ZmshZ3tpY3FZd+VIZ29nb2dwX2Jhc2U2NH0=

Flag: flag[icqedu_gogogo_base64]

提交

解题排名: 赵文轩 梁亚麟 Hello_Terry

提交Writeup获取金币

“百度杯” CTF比赛 十一月场

分值: 10分 类型: Misc 题目名称: 贝壳家族 已解答

题目内容: 我喜欢贝壳, 但是贝壳的表妹喜欢我
还给了我一封情诗
MZWGcZ33MvZGQZL5STQJtGRPWk45Vj56Q===

Flag: flag(erhei_e8934_erUO)

提交

回答正确

解题排名: icq18bdca80 poyoten Swings

提交Writeup获取金币

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:

url编码就是一个字符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：密文里有多多个%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：密文里有多多个\uxxxx

JS混淆(并不是一个编码方式)：

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。

此函数可以计算字符串，并执行其里的JS代码

如，对<script>alert('XSS');</script>进行16进制转换，然后使用eval函数进行读取

```
<script>
eval("\x61\x6c\x65\x72\x74\x28\x27\x58\x53\x53\x27\x29\x3b");
</script>
```

特点：通常在JS脚本里使用eval与function函数进行混淆。

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

例题1：



在

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

例题2:



```
eval('x61x6c\x65\x72\x74\x28\x27\x58\x53\x53\x27\x29\x3b');
undefined
eval('x61x6c\x65\x72\x74\x28\x27\x58\x53\x53\x27\x29\x3b');
```

会车会弹出一个弹窗,



XSS并不是flag, flag即为alert('XSS')

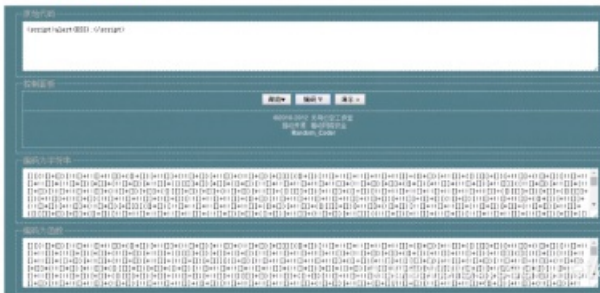
JSfuck:



JSfuck 是用6个字符 `!()+.[]` 来编写 JavaScript 程序, 如右图所示, `<script>alert(XSS);</script>` 经过加密后便使用了 `!()+.[]` 进行编写, 点击run this 可进行解密, 或将密文放在浏览器的console控制台上进行解密。

JSFuck在线加解密: <http://www.jsfuck.com/>

Jother是一种运用于javascript语言中利用少量字符构造精简的匿名函数方法对于字符串进行的编码方式, 其中8个少量字符包括: `!+(())[]`。只用这些字符就能完成对任意字符串的编码 (可以在浏览器的console控制台上直接解密)



若出现没有 `[]`, 而有 `{}`, 就注意可能需要将 `{}` 改为 `[]`.

aaencode使用的表情符号对js代码进编码，可以直接在命令行中继续解码，或者在以下的链接网站进行解码
加解密地址：<http://utf-8.jp/public/aaencode.html>



03 常见加密算法

常见的几种算法

换位加密：栅栏密码、曲路密码、列位移密码

替换加密：凯撒密码、摩斯密码、ROT5/13/18/47、维吉尼亚密码、培根密码、键盘密码

其他密码：MD5、SHA

换位密码-栅栏密码

换位密码-栅栏密码

栅栏密码(Rail-fence Cipher)就是把要加密的明文分成N个一组，然后把每组的第1个字符组合，每组第2个字符组合...每组的第N(最后一个分组可能不足N个)个字符组合，最后把他们全部连接起来就是密文

明文: The quick brown fox jumps over the lazy dog-

去空格: Thequickbrownfoxjumpsoverthelazydog-

分组: Th eq ui ck br ow nf ox ju mp so ve rt he la zy do g-

第一组: Teucbonojmsvrhlzdg-

第二组: hqikrwxupoeteayg-

密文: Teucbonojmsvrhlzdg hqikrwxupoeteayo-

栅栏密码在线加解密：<http://www.qqxiuzi.cn/bianma/zhalanmima.php>

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@

ya wce

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:

congrat

ulation

toyouge

tthekey

从左向右看: congratulation to you get the key

一般夺旗看key,flag,CTF,CTF{,flag}等关键

换位加密-列位移密码

列位移密码(Columnar Transposition Cipher)是一种比较简单,易于实现的换位密码,通过一个简单的规则将明文打乱混合成密文。

列位移密码在线加解密:

<http://www.practicalcryptography.com/ciphers/classical-era/columnar-transposition/>

下面我们以明文 The quick brown fox jumps over the lazy dog. 密钥 how are u为例:

填入 5 行 7 列表(事先约定填充的行列数,如果明文不能填充完整格可以约定使用某个字母进行填充)

T	h	e	q	u	i	c
k	b	r	o	w	n	f
o	x	j	u	m	p	s
o	x	e	r	t	h	e
i	a	z	y	d	o	g

密钥: how are u

按 how are u 在字母表中的出现的先后顺序进行编号,我们就有 a 为 1,e 为 2,h 为 3, o 为 4, r 为 5, u 为 6, w 为 7, 所以先写出 a 列, 其次 e 列, 以此类推写出的结果便是密文:

h	o	w	a	r	e	u
1	2	7	5	4	3	6
T	h	e	q	u	i	c
k	b	r	o	w	n	f
o	x	j	u	m	p	s
o	x	e	r	t	h	e
i	a	z	y	d	o	g

密文: qoury inpho tkool hbvxa uwtdt cfseg erjze-

替换加密-凯撒密码

替换加密-凯撒密码

凯撒密码(Caesar Cipher或称恺撒加密、恺撒变换、变换加密、位移加密)是一种替换加密,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。例,当偏移量是3的时候,所有的字母A将被替换成D, B变成E, 以此类推

明文: The quick brown fox jumps over the lazy dog

偏移量: 1-

密文: Uif rvjdl cspxo gpy kvnqt pafis uif mbaz eph

凯撒密码在线加解密: [密码机器页面](#)

凯撒密码位移规律表

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

解密顺序:即左移,把每个字母按字母表中的顺序依次前移n个字母即可。
例:(移1位) A=Z, B=A, C=B。
加密顺序:即右移,把每个字母按字母表中的顺序依次后移n个字母即可。
例:(移1位) A=B, B=C, C=D。
英文字母的移位以移25位为一个循环,移26位等于没有移位。

替换加密-摩斯电码

替换加密-摩斯电码

摩尔斯电码(Morse Code)是由美国人萨缪尔·摩尔斯在1836年发明的一种时通时断的且通过不同的排列顺序来表达不同英文字母、数字和标点符号的信号代码,摩尔斯电码主要由以下5种它的代码组成:

1. 点 (.)
2. 划 (-)
3. 每个字符短促的停顿 (通常用空格表示停顿)
4. 每个词之间中等的停顿 (通常用 / 划分)
5. 以及句子之间长的停顿

摩斯电码在线解密: [密码机器页面](#)



字符	电码符号	字符	电码符号
A	·-·-	X	·-·-·-
B	·-·-·-	Y	·-·-·-·-
C	·-·-·-·-	Z	·-·-·-·-·-
D	·-·-·-	[]	·-·-·-·-·-
E	·-·-·-	{ }	·-·-·-·-·-
F	·-·-·-·-	~	·-·-·-·-·-
G	·-·-·-	^	·-·-·-·-·-
H	·-·-·-·-	^	·-·-·-·-·-
I	·-·-·-	v	·-·-·-·-
J	·-·-·-	v	·-·-·-·-
K	·-·-·-	z	·-·-·-·-
L	·-·-·-	z	·-·-·-·-
M	·-·-·-	z	·-·-·-·-

数字	电码符号	标点符号	电码符号
1	·-·-·-	?	·-·-·-·-
2	·-·-·-·-	/	·-·-·-·-
3	·-·-·-·-·-	()	·-·-·-·-
4	·-·-·-·-·-	-	·-·-·-·-
5	·-·-·-·-·-	-	·-·-·-·-
6	·-·-·-·-·-	-	·-·-·-·-
7	·-·-·-·-·-	-	·-·-·-·-
8	·-·-·-·-·-	-	·-·-·-·-
9	·-·-·-·-·-	-	·-·-·-·-
0	·-·-·-·-·-	-	·-·-·-·-

例题:



txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

密文: `..* ** ***- * -*- --- **- - ** ** * -* - *-`

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-ROT5/13/18/47

ROT5: 只对数字进行编码，用当前数字往前数的第5个数字替换当前数字，例如当前为0，编码后变成5，当前为1，编码后变成6，以此类推顺序循环。

ROT13: 只对字母进行编码，用当前字母往前数的第13个字母替换当前字母，例如当前为A，编码后变成N，当前为B，编码后变成O，以此类推顺序循环。

ROT18: 这是一个异类，本来没有，它是将ROT5和ROT13组合在一起，为了好称呼，将其命名为ROT18。

ROT47: 对数字、字母、常用符号进行编码，按照它们的ASCII值进行位置替换，用当前字符ASCII值往前数的第47位对应字符替换当前字符，例如当前为小写字母z，编码后变成大写字母K，当前为数字0，编码后变成符号_。用于ROT47编码的字符其ASCII值范围是33 - 126，具体可参考ASCII编码。

ROT5/13/18/47在线解密: <http://www.qqxiuzi.cn/bianma/ROT5-13-18-47.php>

明文: the quick brown fox jumps over the lazy dog.

密文: gur dhvpx oebja sbk whzcf bire gur ynml qbt.

← ROT13加密后 https://blog.csdn.net/am_03

替换加密-维吉尼亚密码

替换加密-维吉尼亚密码

维吉尼亚密码(Vigenère Cipher)是在单一恺撒密码的基础上扩展出多表代换密码,根据密钥(当密钥长度小于明文长度时可以循环使用)来决定用哪一行的密表来进行替换,以此来对抗字频统计

明文: THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG-

密钥(循环使用,密钥越长相对破解难度越大): CULTURE-

加密过程:如果第一行为明文字母,第一列为密钥字母,那么明文字母T和密钥字母C'行的交点就是密文字母V',以此类推。

密文: VBP JOZGM VCHQE JQR UNGGW QPPK NYI NUKR XFK-

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

维吉尼亚密码在线解密: [密码机器页面](#)

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

统计

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

替换加密-培根密码

替换加密-培根密码

培根密码(Baconian Cipher)是一种替换密码,每个明文字母被一个由5字符组成的序列替换,最初的加密方式就是由 'A' 和 'B' 组成序列替换明文(所以你当然也可以用别的字母),比如字母 'D' 替换成 "aaabb", 以下是全部的对应关系 (另一种对于关系是每个字母都有唯一对应序列, 但Q与U/V各自都有不同对应序列)

明文: thefox

密文: baabb aabbb aabaa aabab abbba babbb

培根密码在线解密:

<http://rumkin.com/tools/cipher/baconian.php>

字母	第一种方式		第二种方式				
	表示法	字母	表示法	字母			
A	aaaaa	N	abbbb	a	AAAAA	n	ABBAA
B	aaaab	O	abbbb	b	AAAAB	o	ABBAB
C	aaaba	P	abbbb	c	AAABA	p	ABBA
D	aaabb	Q	baaaa	d	AAAB	q	ABBB
E	aabaa	R	baaab	e	AABAA	r	BAAAA
F	aabab	S	baaba	f	AABAB	s	BAAAB
G	aabba	T	baabb	g	AABBA	t	BAABA
H	aabbb	U	baaaa	h	AABBB	u-v	BAABB
I	abaaa	V	baaab	i-j	ABAAA	w	BABAA
J	abaab	W	baaba	k	ABAA	x	BABAB
K	ababa	X	baabb	l	ABABA	y	BABBA
L	ababb	Y	baaaa	m	ABABB	z	BABBB
M	abbaa	Z	baabb				

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 (3) 电脑键盘坐标加密

Q	W	E	R	T	Y	U	G	H	I	P
A	S	D	F	G	H	J	K	L		
Z	X	C	V	B	N	M				



(2) 电脑键盘棋盘加密

1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	~	!	@	#	\$	%	-	&	*	()	_	+
2	`	1	2	3	4	5	6	7	8	9	0	-	= \
3	Q	W	E	R	T	Y	U	I	O	P	{	}	
4	q	w	e	r	t	y	u	i	o	p	[]	
5	A	S	D	F	G	H	J	K	L	:	"		
6	a	s	d	f	g	h	j	k	l	;	'		
7	Z	X	C	V	B	N	M	<	>	?			
8	z	x	c	v	b	n	m	,	/				

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:
明文: 87 34 112
55 47 87 410
明文: MR_Gump

一、电脑键盘坐标(坐标法)
注1: (蓝色、黄色) 背景色内数字为横坐标, 蓝色内数字为纵坐标。 0, 11 = 0; 0, 22 = 4; 02, 11 = 4。
注2: (蓝色、黄色) 背景色内数字为横坐标, 蓝色内数字为纵坐标。 0, 11 = 0; 0, 22 = 4; 02, 11 = 4。
解密: 如果所有的数字坐标为213, 则为注1, 反之则为注2。(特指横坐标纵坐标)
如果所有的数字坐标为213, 则为注2, 反之则为注1。(特指纵坐标横坐标)

(4) 手机键盘密码

手机键盘密码



简单的替换密码。

采用坐标方法加密。

例:
21 = A; 22 = B; 94 = Z。

特点: 第一数字为2-9, 第二数字为1-4。

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, 通常MD5的值中最大是F, 如, 603F52D844017E83CA267751FEE5B61B

MD5在线解密地址: <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。SHA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。