攻防世界 CRYPTO

原创

yuedarkshadow 于 2022-01-02 18:40:16 发布 1731 收藏
文章标签： 安全

本文链接：https://blog.csdn.net/yueshangttt/article/details/122269446

2021年12月27-2

目录

morse

Railfence

培根密码

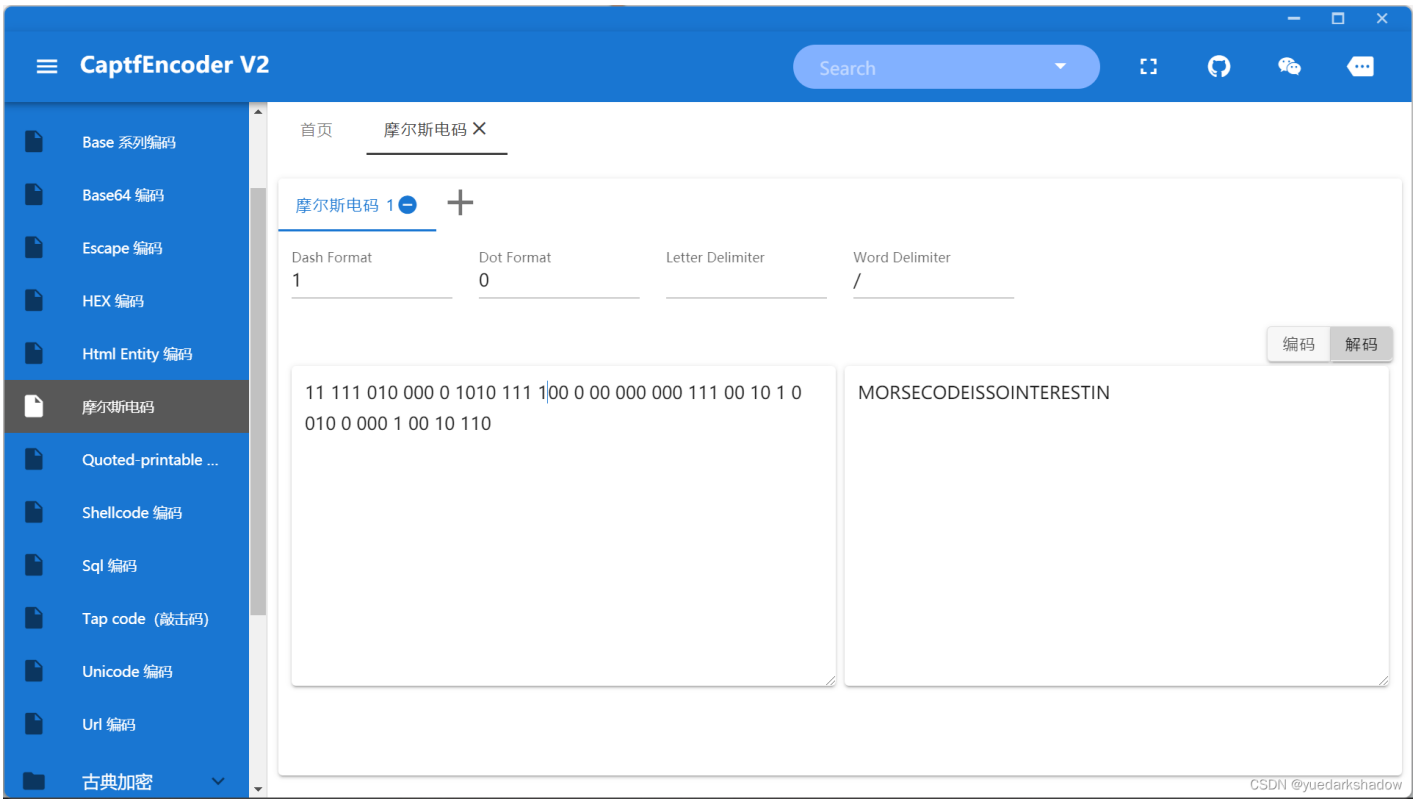
DES加密算法

新手练习区

morse

0表示(.)

1表示（-）#也可以反过来



Railfence

栅栏密码加密/解密【W型】 - 一个工具箱 - 好用的在线工具都在这里！http://www.atoolbox.net/Tool.php?Id=777解密时需适当改变栏数

培根密码

仅包含AB

加密者需使用两种不同字体，分别代表A和B。准备好一篇包含相同AB字数的假信息后，按照密文格式化假信息，即依密文中每个字母是A还是B分别套用两种字体

DES加密算法

例题：

假设DES 的某轮迭代的32位输入是1100 0011 0000 1100 1011 0101 1000 0010，经过E扩展之后的序列是什么？当该轮的密钥是1000 1011 1000 1000 1111 1101 1100 1010 1000 1000 1111 1101 ，进入S盒后，每一组的6比特数据经过S盒替换后的4比特输出分别是什么？

1100 0011 0000 1100 1011 0101 1000 0010

E扩展置换：先将32位扩展为48位

0 1100 0

0 0011 0

1 0000 1

0 1100 1

0 1011 0

1 0101 1

1 1000 0

0 0010 1

合并：0110 0000 0110 1000 0101 1001 0101 1010 1011 1100 0000 0101

密钥：1000 1011 1000 1000 1111 1101 1100 1010 1000 1000 1111 1101

进行异或运算 0异或0=1 1异或1=1 0异或1=0 1异或0=0（相等为1，不相等为0）

异或后：0001 0100 0001 1111 0101 1011 0110 1111 1100 1011 0000 0110

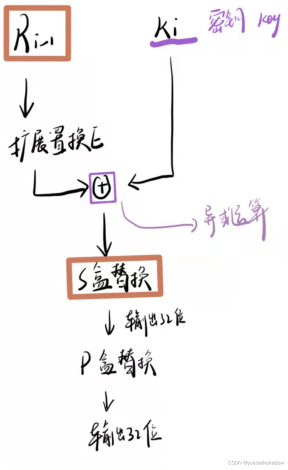
S盒替换

000101 000001 111101 011011 011011 111100 101100 000110

用4bit的列号代替原来6bit的数据

例：000101 首位作为行号 中间四位作为列号

则S盒替换后：0010 0000 1110 1101 1101 1110 0110 0011


Ri-1
Ki
密钥 key
扩展置换E
⊕
S盒替换
输出32位
P盒替换
输出32位