CTF&密码学

单击此处添加副标题

seigo　　2023.3.19

what it is?

密码是一种用来混淆的技术，它希望将正常的、可识别的信息转变为无法识别的信息

密码学(Cryptology)　研究信息系统安全保密的科学。它以可靠的数学方法和理论为基础，对解决信息安全中的机密性、数据完整性、认证和身份识别，信息的可控性，以及不可抵赖性等提供系统的理论方法和技术。

密码可能受到的攻击类型

攻击类型	攻击者拥有的资源
唯密文攻击	•加密算法 •截获的部分密文
已知明文攻击	•加密算法， •截获的部分密文和相应的明文
选择明文攻击	•加密算法 •加密黑盒子，可加密任意明文得到相应的密文
选择密文攻击	•加密算法 •解密黑盒子，可解密任意密文得到相应的明文

CTF中的密码

在CTF中，密码学很多时候会和web与杂项结合考察，一般古典密码往往并不会给出加密算法，这就需要我们对常见的古典密码编码的特点有一定的了解。

而对于现代密码通常会给出或暗示提示所使用的加密算法，需要我们按照已经给出的算法思考加/解密并加以实现

古典密码

单击此处添加文本具体内容，简明扼要的阐述您的观点。

常见古典密码

- 单表代换:
- 埃特巴什密码
- 凯撒密码
- 多表代换:
- 维吉尼亚密码

单表置换密码の分析————字母频率分析

- 在单表置换之下，无论置换方式是什么，相同的字符在置换之后所得到的是一个固定的、相同的符号。
- 因此我们可以轻易从密文得到明文的统计规律。

- 那么，在文本样本量较为充足的条件下，我们可以根据密文和铭文不同符号的统计频率反推得到加密关系，从而从密文反推明文。

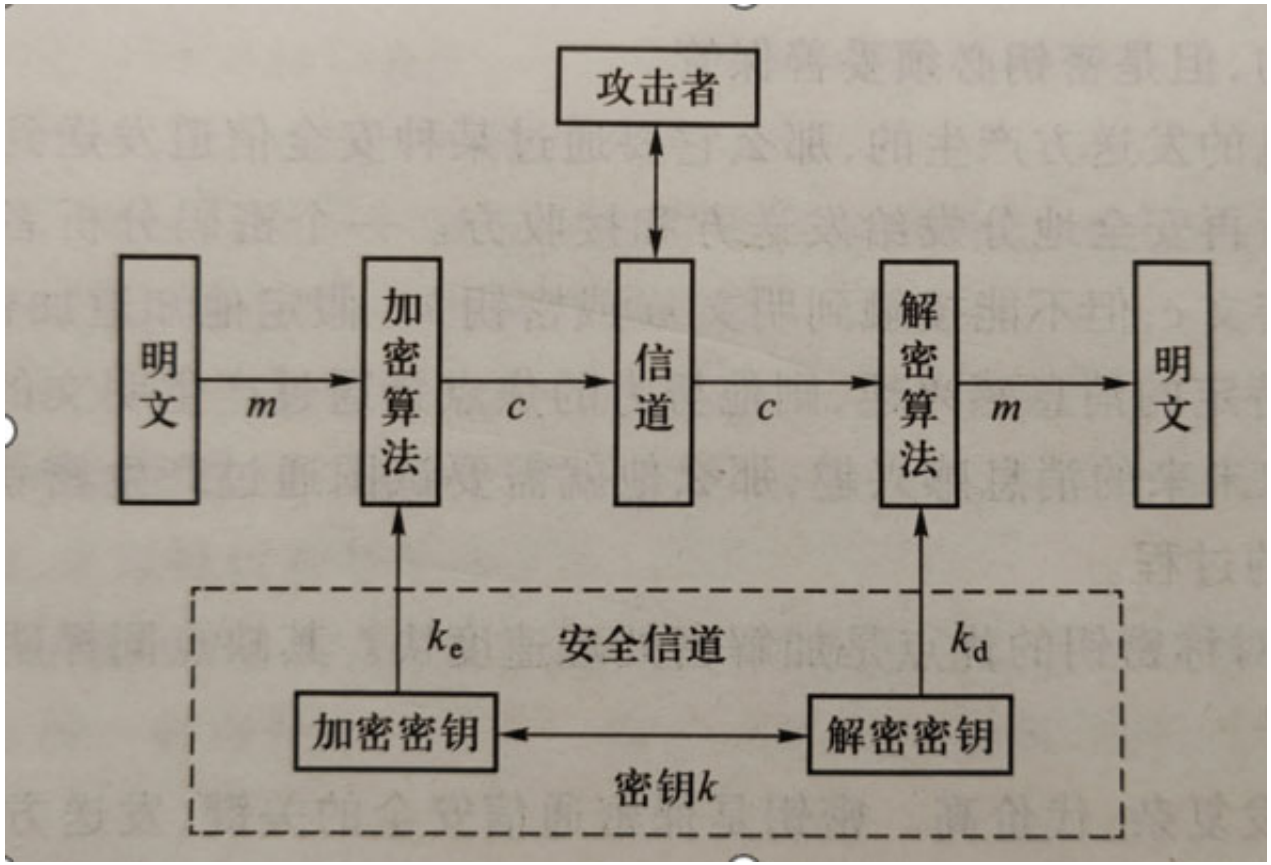
单表置换密码の分析————字母频率分析

- Besides 以英文为例
- 1、英语中出现频率最高的字母是e
- 2、 英语中出现最多的单词是The
- 3、 英语文章中9个最常用的字母是e，t，a，o，n，i，r，s, h
- 4、英语单词中有一半以上是以t，a，o，s或w开头的
- 5、 仅10个单词（the，of，and，to，a，in，that，it，is和I）就构成标准英语文章四分之一以上的篇幅

现代密码

现代密码

一般而言，加密密钥和解密密钥相同的算法成为对称密码，不同的称为非对称密码



对称密码设计特点——扩散&混淆

- 目的-破坏明文&密文之间的统计特性

- **扩散**：将每一位明文和密钥比特的影响扩散到尽可能多的密文比特中。在理想情况下，明文和密钥的每一位都影响密文的每一位。通过扩散，可以隐藏许多明文在统计上的特性。

- **混乱**（混淆） 是指明文与密钥、以及密文之间的统计关系尽可能复杂化，使破译者无法理出相互间的依赖关系，从而加强隐蔽性。采用复杂的非线性变换(比如S盒单元)就可达到比较好的混乱效果

常见对称密码-DES

- DES密码算法采用Feistel密码的S-P结构，其特点是：加密和解密使用同一算法、同一密钥、同一结构。区别是：16轮加密子密钥顺序为K1, K2,…,K16，解密子密钥顺序为K16, K15,…，K1。其中密钥长度为64位，在具体算法中，只使用56位(另外8位为奇偶校验位)的密钥输入对64位的明文进行加解密运算，获取64位密文。

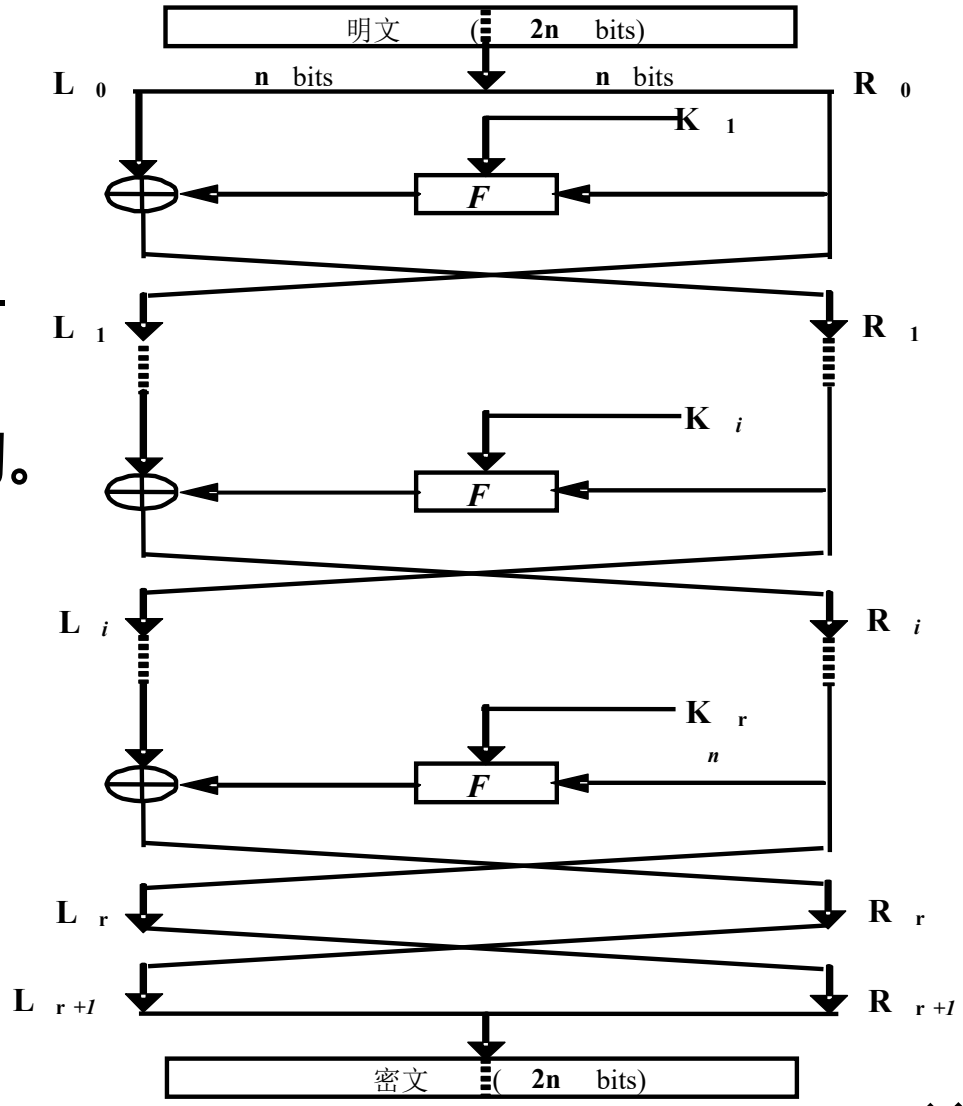


图 3 - 2 Feistel 密码结构

常见对称密码-DES

DES加密机制如图3-3所示，每轮结构完全一样。整个过程由三个阶段来完成：初始置换、乘积变换和逆初始置换。

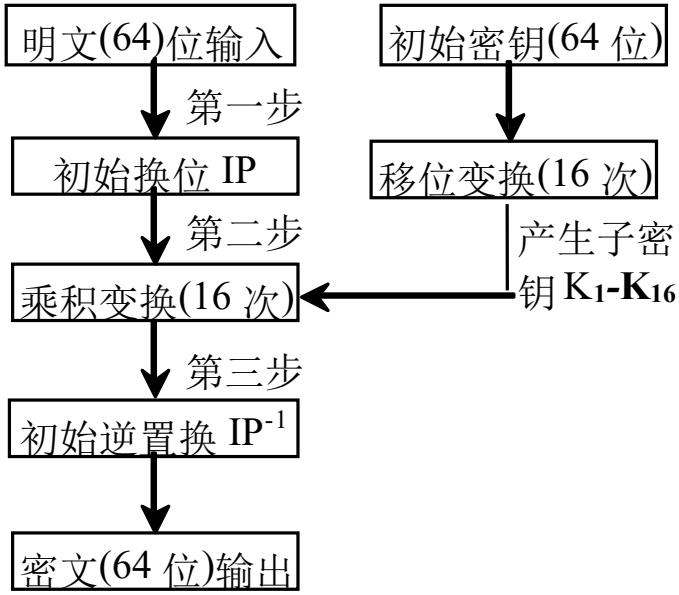
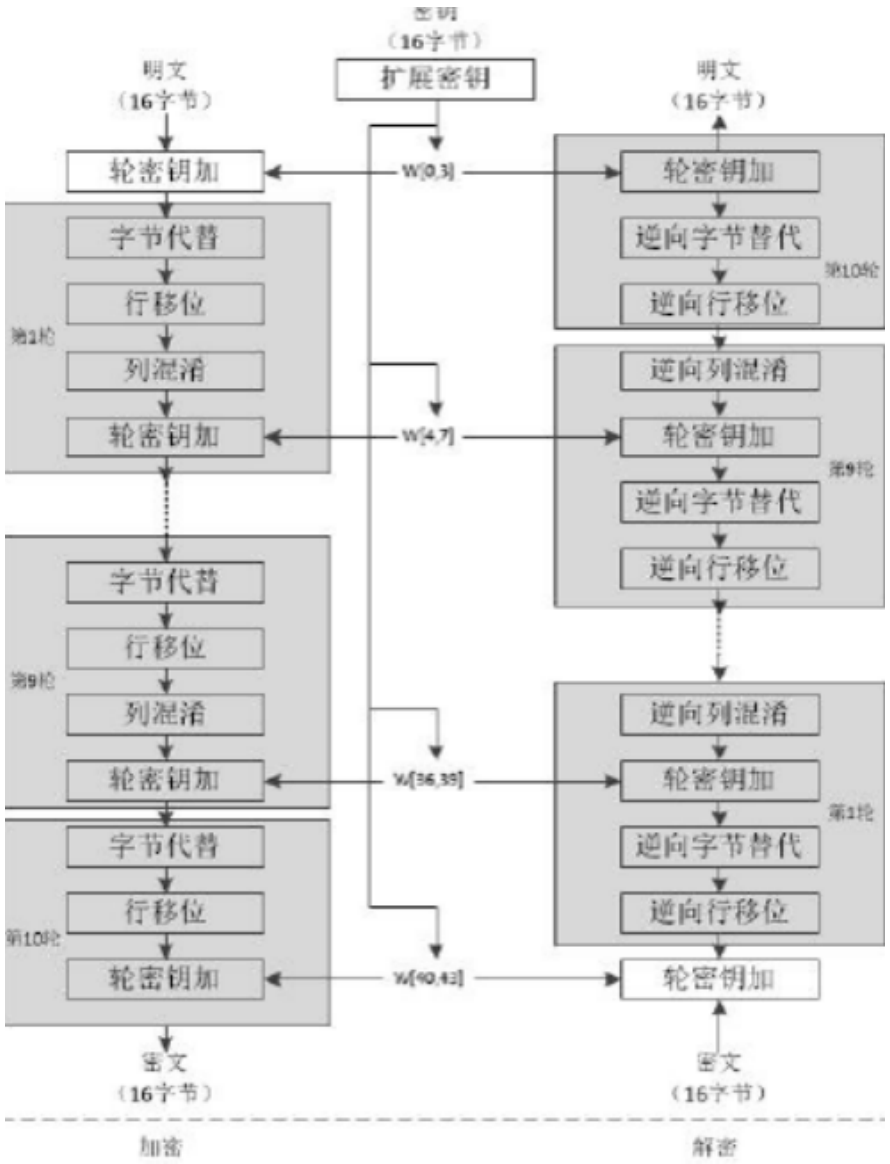


图 3-3 DES 简化示意图

常见对称密码-AES

- 分组长度固定为128位，密钥长度可以为128、192或256位



非对称密码密码——定义&特点

- 非对称密码（公钥密码）体制于1976年由W. Diffie和M. Hellman提出，同时，R. Merkle也独立提出了这一体制。

- 这种密码体制采用了一对密钥——加密密钥和解密密钥(且从解密密钥推出加密密钥是不可行的)，这一对密钥中，一个可以公开(称之为公钥)，另一个为用户专用(私钥)

公钥密码——定义&特点

- 公钥密码系统是基于陷门单向函数的概念。
- 单向函数是易于计算但求逆困难的函数，而陷门单向函数是在不知道陷门信息情况下求逆困难，而在知道陷门信息时易于求逆的函数。
- 如目前主流的非对称密码：
- RSA：基于大合数因式分解困难问题
- ElGamal:基于离散对数求解困难问题
- ECC：基于椭圆曲线离散对数求解困难问题

公钥密码——常见公钥密码RSA

- RSA是1977年由罗纳德·李维斯特（Ron Rivest）、阿迪·萨莫尔（Adi Shamir）和伦纳德·阿德曼（Leonard Adleman）一起提出的。

- 安全性基于大数分解的困难性。我们知道，求一对大素数的乘积很容易，但要对这个乘积进行因式分解则非常困难，因此，可以把一对大素数的乘积公开作为公钥，而把素数作为私钥，从而从一个公开密钥和密文中恢复出明文的难度等价于分解两个大素数之积。

公钥密码——常见公钥密码RSA

- 欧拉函数：

- Φ(m)表示1~m-1中与m互素的整数个数
- 特别的，若m是素数，则φ(m) = m – 1

- 欧拉定理：
- 若m>1，gcd(a,m) = 1
- $a^{\varphi(m)} = 1 (\mathrm{mod}\ m)$

公钥密码——常见公钥密码RSA

选择两个不同的大素数p和q(一般都为100位左右的十进制数字)，计算乘积：

$$n=pq$$

和欧拉函数值：

$$\varphi(n)=(p-1)(q-1)$$

随机取一整数e，$1 < e < \varphi(n)$，且e和$\varphi(n)$互素。此时可求得d以满足：

$$de \equiv 1 \bmod \varphi(n)$$

则

$$d = e^{-1} \bmod \varphi(n)$$

公钥密码——常见公钥密码RSA

- 这样可以把e和n作为公开密钥，d作为私人密钥。其中，p、q、φ (n)和d就是秘密的陷门(四项并不是相互独立的)，这些信息不可以泄露。

RSA加密消息m时(这里假设m是以十进制表示的)，首先将消息分成大小合适的数据分组，然后对分组分别进行加密。每个分组的大小应该比n小。
设c_i为明文分组m_i加密后的密文，则加密公式为

$$c_i=m_i^e \pmod n$$

解密时，对每一个密文分组进行如下运算：

$$m_i=c_i^d \pmod n=m_i^{de} \pmod n$$

公钥密码——RSA常见攻击方式

- **穷举攻击**：试图穷举所有可能的私钥
- **数学攻击**：数学攻击方法——试图分解两个素数的的乘积
- **计时攻击**：依赖于解密算法的运行时间
- **选择密文攻击**：利用RSA算法的性质
- **基于硬件故障攻击**

RSA常见攻击方式——低指数攻击

当加密指数 e 很小，c可能不比n大很多

这样就存在一个较小的可枚举的 k满足：

$$m^e=c+k*n$$

尝试枚举 k并开根，能刚好开根的就是解

RSA常见攻击方式——共模攻击

如果在 RSA 的使用中使用了相同的模 n 对相同的明文 m 进行了加密，那么就可以在不分解 n 的情况下还原出明文 m 的值。

不同的模数e1、e2，且e1、e2互素，对同一组明文加密得到密文c_1、c_2

- $c_1 = m^{e1} \bmod n$
- $c_2 = m^{e2} \bmod n$

存在整数x和y，使得xe1 + ye2 = 1

- $c_1^x \times c_2^y \bmod n = m^{xe1} \times m^{ye2} \bmod n = m1 \bmod n = m$

RSA常见数学攻击方式——广播攻击

对于相同的明文m，使用相同的指数e和不同的模数n1、n2…ni，加密得到i组密文时，可以用中国剩余定理解出明文：

- $c_1=m^e \bmod n_1$，
  $c_2=m^e \bmod n_2$
  $c_i=m^e \bmod n_i$

联立：

- 可以求得一个c_x满足 $c_i = m^e \bmod \Pi_1^j n_j$

小试牛刀

谢谢观看

汇报日期