

密 码 学

分组密码运行模式
大数
据加密

一、计算机数据的特殊性

1、存在明显的数据模式：

- 许多数据都具有某种固有的模式。这主要是由数据冗余和数据结构引起的。
- 各种计算机语言的语句和指令都十分有限，因而在程序中便表现为少量的语句和指令的大量重复。
- 各种语言程序往往具有某种固定格式。
- 数据库的记录也往往具有某种固定结构。
- 操作系统和网络也有同样的问题。

一、计算机数据的特殊性

1、存在明显的数据模式：

- 根据明文相同、密钥相同，则密文相同的道理，这些固有的数据模式将在密文中表现出来。
- 掩盖明文数据模式的方法：
 预处理技术(随机掩盖)
 链接技术
- 如果不能掩盖数据模式，即使采用安全的密码算法也是徒劳的。

一、计算机数据的特殊性

数据的特殊性带来的需求：

- 分组固定而待加密的数据量是不定的。
- 即使有了安全的分组密码算法，也需要采用适当的工作模式来隐蔽明文的统计特性、数据的格式等，以提高整体的安全性，降低删除、重放、插入、和伪造成功的机会。
- 不仅要保持各分组的完整性，还有保持各分组的次序不变。

二、分组密码的工作模式

1977年DES颁布。1981年美国针对DES的应用制定了四种基本工作模式：

β 电码本模式 (ECB)

每个明文组独立地以同一密钥加密，单个数据加密。

β 密文反馈链接模式 (CBC)

将前一组密文与当前明文组逐步异或后再进行分组、加密，用途：加密、认证。

二、分组密码的工作模式

β 密码反馈模式 (CFB)

每次只处理k位数据，将上一次的密文反馈到输入端，从加密器的输出取k位，与当前的k位明文逐位异或，产生相应密文；用途：一般传送数据的流加密，认证

β 输出反馈模式 (OFB)

类似于CFB，以加密器输出的k位随机数字直接反馈到加密器的输入，用途：对有扰信道传送的数据流进行加密（如卫星数传）

二、分组密码的工作模式

2000年美国在征集AES的同时又公开征集AES的工作模式。共征集到15个候选工作模式。

- β 新的工作模式标准还在评审中。
- β 这些新的工作模式将为AES的应用作出贡献。

二、分组密码的工作模式

1、电码本模式 (ECB)

β 直接利用分组密码对明文的各分组进行加密。

β 设 明文 $M = (M_1, M_2, \dots, M_n)$,
密钥为 K ,

密文 $C = (C_1, C_2, \dots, C_n)$,

其中 $C_i = E(M_i, K)$, $i=1,2,\dots,n$

β 电码本方式是分组密码的基本工作模式。

β 缺点：可能出现短块，这时需要特殊处理。

β 缺点：暴露明文的数据模式。

β 应用：适合加密密钥等短数据

二、分组密码的工作模式

2、密文反馈链接模式 (CBC)

①明密文链接方式 (Plaintext and Ciphertext Block Chaining)

设 明文 $M = (M_1, M_2, \dots, M_n)$,

密钥为 K ,

密文 $C = (C_1, C_2, \dots, C_n)$,

其中 $C_i = \begin{cases} E(M_i \oplus Z, K), & i=1 \\ E(M_i \oplus M_{i-1} \oplus C_{i-1}, K), & i=2, \dots, n \end{cases}$

Z 为初始化向量。

二、分组密码的工作模式

2、密文反馈链接模式 (CBC)

①明密文链接方式

- β 即使 $M_i = M_j$ ，但因一般都有 $M_{i-1} \oplus C_{i-1} \neq M_{j-1} \oplus C_{j-1}$ ，从而使 $C_i \neq C_j$ ，从而掩盖了明文中的数据模式。
- β 加密时，当 M_i 或 C_i 中发生一位错误时，自此以后的密文全都发生错误。这种现象称为错误传播无界。
- β 解密时也是错误传播无界。