密码技术基本知识
2024

目录

本节简要介绍密码的概念和作用，指出密码需要合规、正确、有效地使用，并对密码技术的核心内容：密码算法、基于密码的认证、密钥管理、密码协议、密码功能进行介绍。[56]

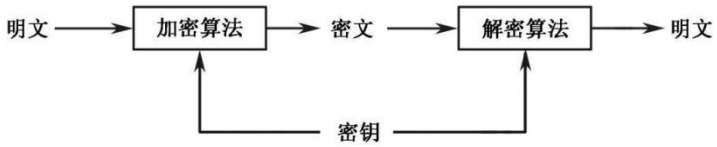
1.1. 密码算法

现代密码学理论中，算法是密码技术的核心，常见的密码算法包括：对称密码算法、公钥密码算法和摘要密码算法。

1.1.1. 对称密码算法

对称密码算法加密过程与解密过程使用相同的或容易相互推导得出的密钥，即加密和解密两方的密钥是“对称”的。早期的密码算法都是对称形式的密码算法。对称密码加密和解密基本流程如下图所示。用户通过加密算法将明文变换为密文。只有掌握了同一个密钥和对应解密算法的用户才可以将密文逆变换为有意义的明文。

图 109 对称密码加密和解密基本流程



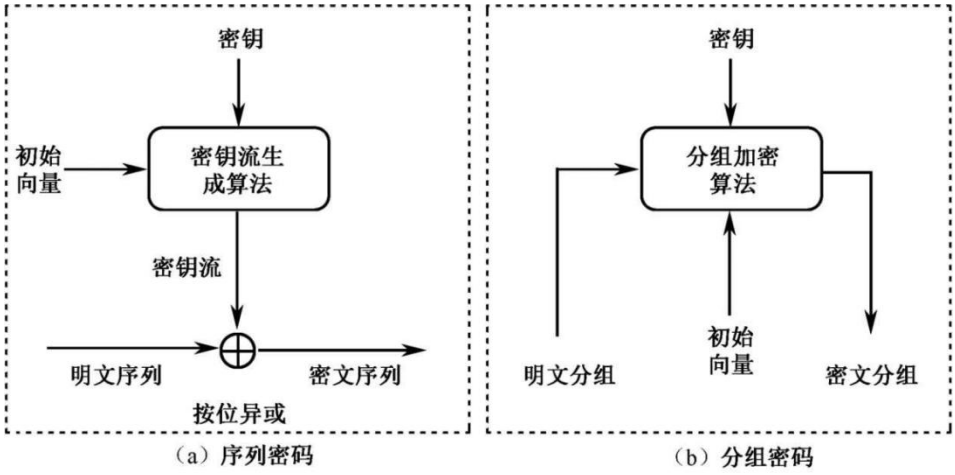
针对不同的数据类型和应用环境，对称密码有两种主要形式：一是序列密码，二是分组密码。

1．序列密码和分组密码

(1) 序列密码和分组密码的区别

序列密码和分组密码都属于对称密码，区别在于序列密码是将密钥和初始向量作为输入，通过密钥流生成算法输出密钥流，然后将明文序列和密钥流进行异或，得到密文序列。分组密码首先对明文消息根据分组大小进行分组，再将明文分组、密钥和初始向量一起作为输入，通过分组加密算法直接输出密文分组。

图 110 序列密码和分组密码的加密流程



(2) 初始向量

在对称密码的实际应用场景中，初始向量是一个在加密过程中起到引入随机性作用的随机数，即在加密一批明文数据之前，加密方先要随机生成一个初始向量，并将它和密钥一起输入到加密算法中。每次加密初始向量都必须重新生成，

初始向量的引入使得多次分别对同一明文数据使用相同的密钥进行加密，得到的密文是不同的。

2. 分组密码的工作模式

我国于 2008 年发布了规定分组密码算法工作模式的国家标准 GB/T 17964-2008《信息安全技术 分组密码算法的工作模式》。在分组密码算法中，根据分组数据块链接的组合模式不同，可以分为以下七种工作模式：电码本（ECB）模式、密文分组链接（CBC）模式、密文反馈（CFB）模式、输出反馈（OFB）模式、计数器（CTR）模式、分组链接（BC）模式、带非线性函数的输出反馈（OFBNLF）模式、GCM 模式。本节重点介绍常用的 ECB、CBC、CTR、GCM 模式。

(1) ECB 模式

ECB 模式是一种最直接的消息加密方法，ECB 模式的加密和解密流程如下图所示。

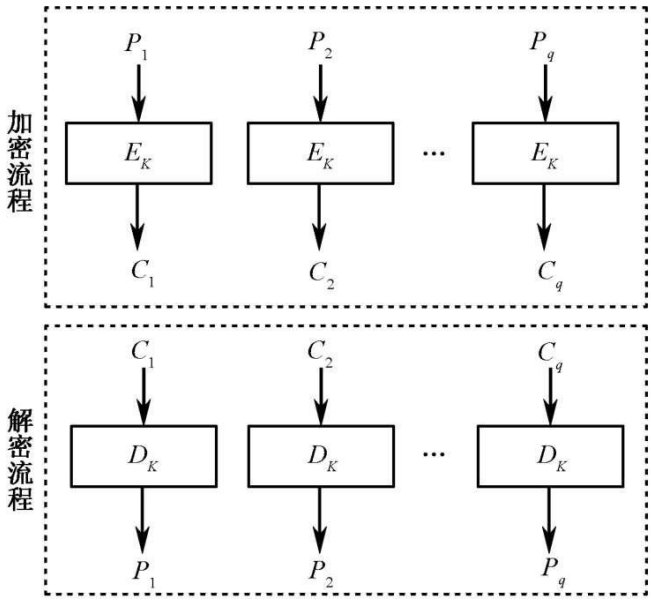


图 111 ECB 模式的加密和解密流程

可以看出 ECB 模式具有如下性质：

1） 对某一个分组的加密或解密可独立于其他分组进行；

2） 对密文分组的重排将导致明文分组的重排；

3） 不能隐蔽数据模式，即相同的明文分组会产生相同的密文分组；

4） 不能抵抗对分组的重放、嵌入和删除等攻击。因此，不推荐在应用中使用 ECB 模式。

(2) CBC 模式

在 CBC 模式下，每个明文分组在加密之前，先与反馈至输入端的前一组密文分组按位异或后，再送至加密模块进行加密。其中，IV 是一个初始向量，无须保密，但须随着消息的更换而更换，且收发双方必须选用同一个 IV。显然，计算的密文分组不仅与当前明文分组有关，而且通过反馈作用还与以前的明文分组有关。在解密过程中，初始值 IV 用于产生第一个明文输出；之后，前一个密文分组与当前密文分组解密运算后的结果进行异或，得到对应的明文分组。

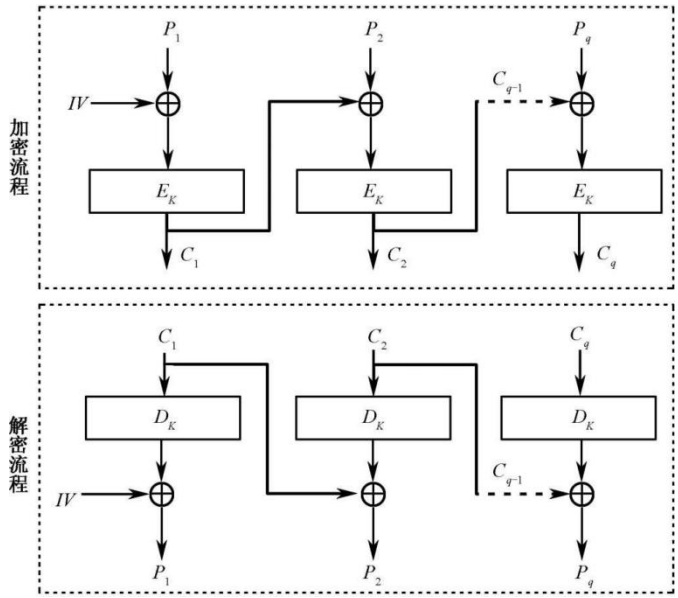


图 112 CBC 模式的加密和解密流程

CBC 模式具有如下性质：

1) 链接操作使得密文分组依赖于当前的和以前的明文分组，因此对密文分组的重新编排不会导致对相应明文分组的重新编排。

2) 加密过程使用 IV 进行了随机化，每次加密 IV 都必须重新生成，并且要保证 IV 的随机性。使用不同的 IV 可以避免 ECB 模式下每次对相同的明文使用相同的密钥加密生成相同的密文的弊端。

3) 加密过程是串行的，无法并行化；在解密过程中，通过两个相邻的密文分组执行解密操作可以获得明文分组，因此解密过程可以并行化。

4) 此外，CBC 模式还有一个重要用途：生成消息鉴别码（MAC），即使用最后一个分组的输出结果作为 MAC。MAC 可以用于检验消息的完整性、验证消息源的真实性等。

(3) CTR 模式

CTR 模式通过将逐次累加的计数器值进行加密来生成密钥流。CTR 模式的加密和解密流程如下图所示。

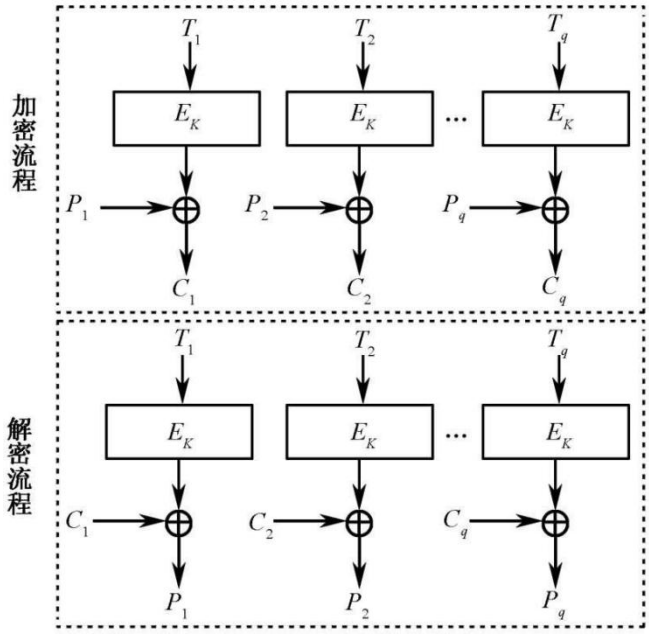


图 113 CTR 模式的加密和解密流程

此外，还有一种用法是将一个单独的 IV 与计数器值拼接在一起作为生成密钥流的输入分组，此时计数器值一般从 0 或 1 开始。需要注意的是，将 IV 与计数器值直接相加或异或后作为输入是不安全的，这样会导致选择明文攻击。

CTR 模式具有如下性质：

1) 支持加密和解密并行计算，可事先生成密钥流，进行加密和解密准备。

2) 用到了分组密码算法的分组加密操作。

3) 错误密文中的对应比特会影响解密后明文中的对应比特，即错误不会传播。

(4) GCM 模式

GCM 是认证加密模式中的一种，是遵循 EtM 方式（先加密后认证 Encrypte-then-MAC，EtM）在一个算法内部同时完成消息加密和 MAC 码计算的可认证加密模式，内部组合了 CTR 模式和 GMAC 算法。在实际应用场景中，有些信息是不需要保密，但信息的接收者需要确认它的真实性，例如源 IP，源端口， 目的 IP 等。因此，可以将这一部分作为附加消息加入到 MAC 值的计算当中。下图的 Ek 表示用对称密钥 k 对输入做 SM4 加密。

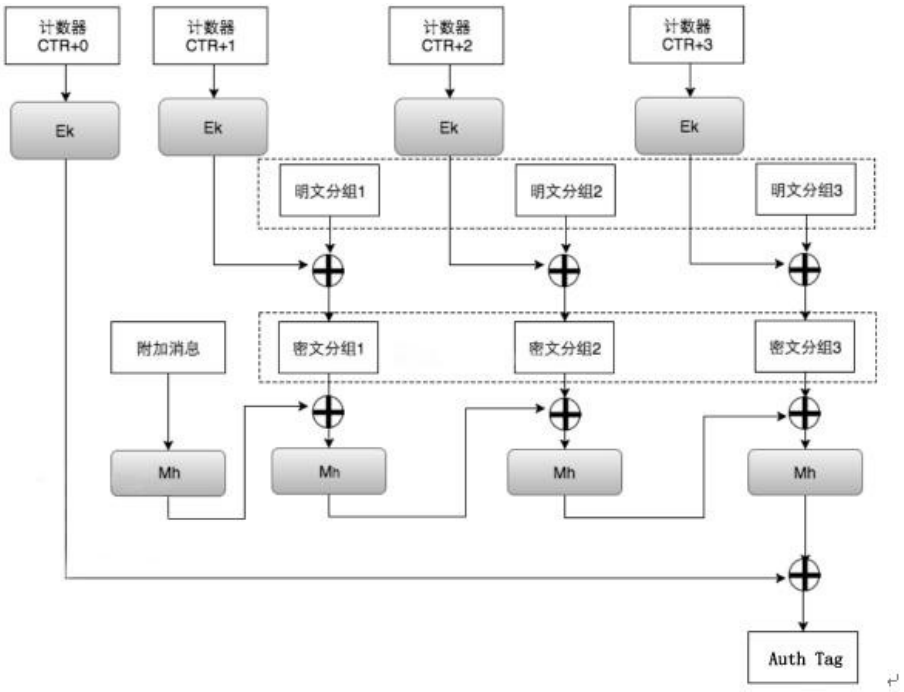


图 114 GCM 模式的加密流程

GCM 模式具有如下性质：

1) 能同时确保数据的保密性、完整性及真实性。

2) 可以提供附加消息的完整性校验。

3. ZUC 序列密码算法