极客时间-实用密码学-09为什么ECB模式不安全

原创

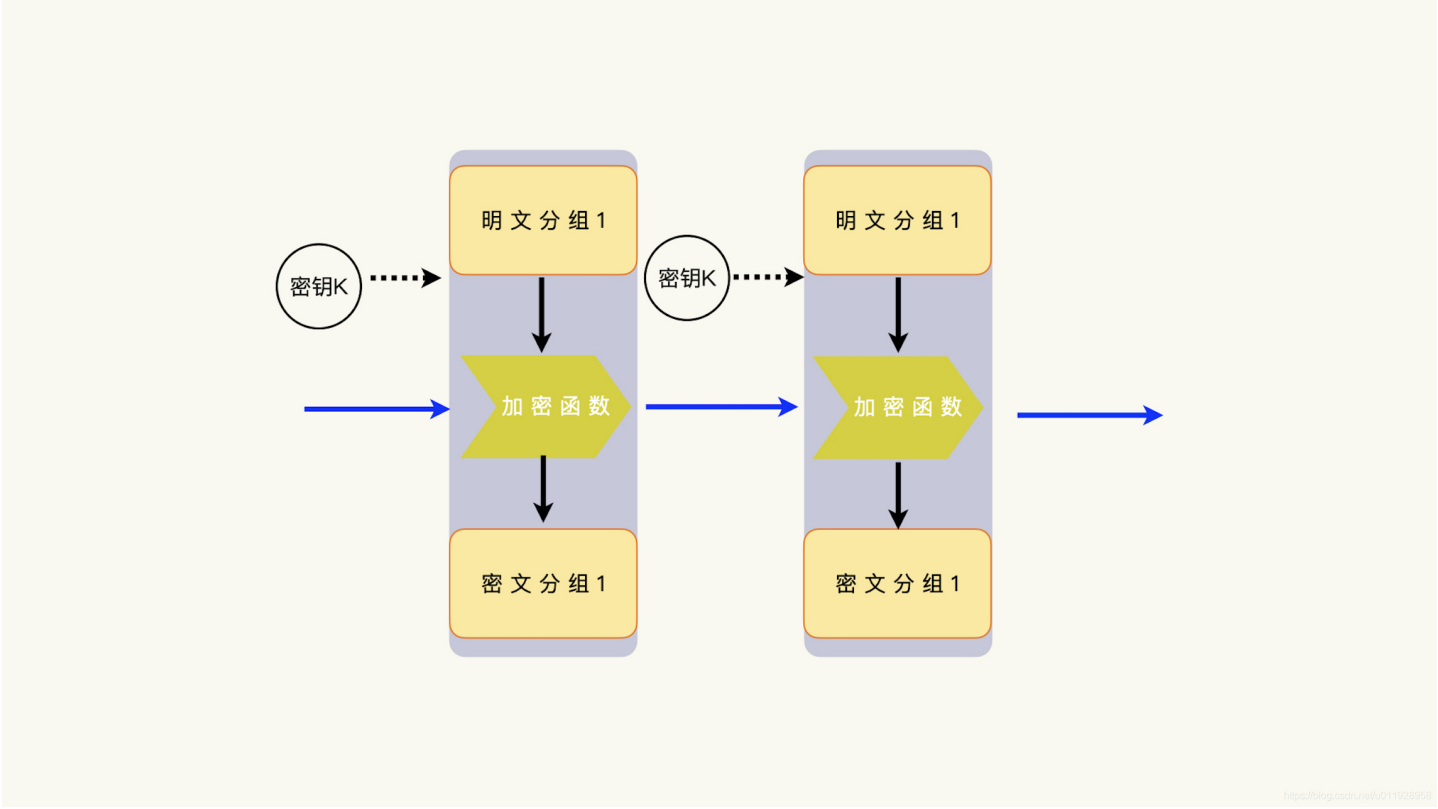
Tom哈哈 于 2020-12-16 09:22:37 发布 1738 收藏 4

分类专栏： 笔记 文章标签： 密码学

本文链接：https://blog.csdn.net/u011928958/article/details/111245179

链接模式怎么连？

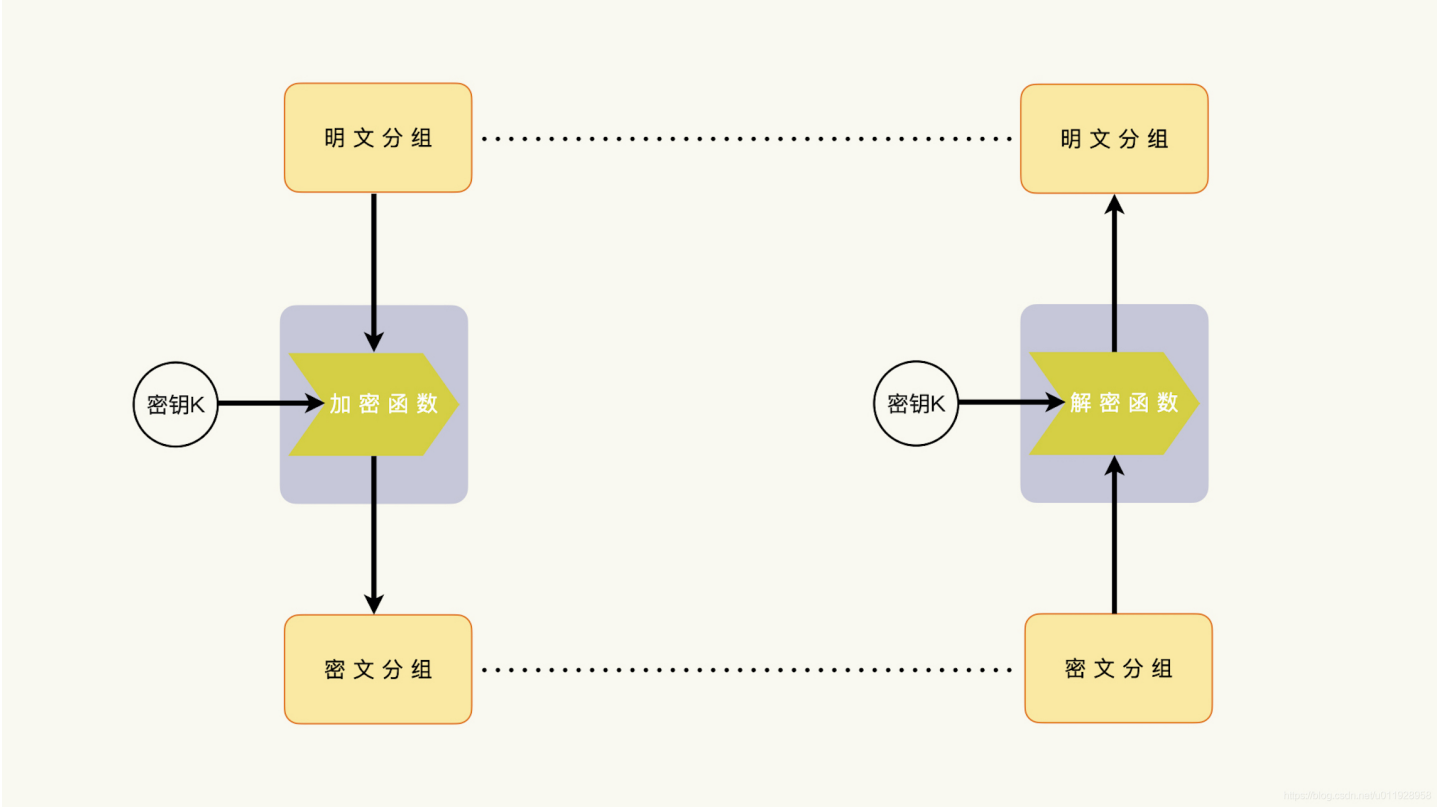
链接模式指的是如何把上一个分组运算和下一个分组运算联系起来，使得上一个分组运算可以影响下一个运算。但是，这个联系是怎么建立起来的，上一个运算到底又是怎么影响下一个运算的，这个描述是模糊的。



从道理上来说，上一个分组运算的所有要素，都有可能参与到下一个分组运算里；下一个分组运算的每一个要素，都有可能接收上一个运算的一个要素或者几个要素的组合。

而在这之间就会形成不同的分配组合，也就形成了不同的链接模式。

ECB模式



ECB模式不使用链接模式，也就不需要初始化向量。每一个分组的加密都是独立的。

分组的加密是独立的与其他分组不相关，可以带来并行计算的好处，也没用初始化向量管理的烦恼，也有好使用代码接口。比如java，默认采用的是ECB模式，这段代码看起来更简洁：

```
Cipher cipher = Cipher.getInstance("AES");
cipher.init(Cipher.DECRYPT_MODE, secretKey);
```

但你看，下面的代码就繁琐的多，还要在加密端和解密端传送初始化向量:

```
IvParameterSpec ivParameters = new IvParameterSpec(ivBytes);
Cipher cipher = Cipher.getInstance("AES/CBC/PKCS5Padding");
cipher.init(Cipher.DECRYPT_MODE, secretKey, ivParameters);
```

它的致命的安全缺陷却恰好来源于它令人振奋的特性：初始化向量的缺失和链接模式的缺失。

缺失带来了什么问题？

- 相同的明文加密出的密文一定相同
- 每一个数据分组单独加密与其他分组不相关，密文数据容易拼接形成伪造的密文数据，就是常说的“分组重放”攻击。

什么时候使用 ECB 模式？

大多数时候我们都不应该使用，那为什么安全应用程序接口还要提供 ECB 模式的编程接口呢？这主要是因为，ECB 模式是分组算法的基础。有密码学专业知识的算法工程师，可以通过合理地使用 ECB 模式，来构造更复杂、更安全的算法。