Dokin丶
码龄8年 企业员工
40
原创
1566
积分
私信 关注

搜博主文章

热门文章
FOC控制算法详解 34406
STM32 PVD的使用（掉电检测） 12363
FSEC大学生电动方程式赛车电气系统设计 12283
AES加密模式总结 7073
计算变量中有多少个bit位是1的方法 7044

最新评论
嵌入式消息订阅发布模式软件框架
房东的猫0618: 好的，非常感谢！如果有一些思想架构文档 辛苦一起可以发下，这 ...
嵌入式消息订阅发布模式软件框架
Dokin丶: 晚一点哈，这几天电脑坏掉了
FOC控制算法详解
LT_4399: 伺服系统中，如果想做foc需要哪些硬件设备，可不可直接买到
嵌入式消息订阅发布模式软件框架
房东的猫0618: 感谢楼主分享，方便拜读一下softbus源码嘛？1356579487@qq.com ...
嵌入式消息订阅发布模式软件框架
逸尘丶丿: 大神源码能否分享一下，最近在对工程进行重构，想借鉴一下13559783 ...

您愿意向朋友推荐“博客详情页”吗?
强烈不推荐 不推荐 一般般 推荐 强烈推荐

最新文章
SigmaStar空板烧录
蓝牙Inquiry与Inquiry Scan
BlueZ双模蓝牙音频卡顿问题优化

2023年 2篇
2022年 8篇
2021年 17篇
2020年 24篇

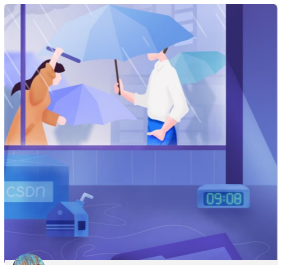
AES加密模式总结

原创 Dokin丶 已于 2022-04-16 19:54:14 修改 7088 收藏 20 版权

分类专栏： 算法 文章标签： AES AES加密模式 AES CBC AES ECB

算法 专栏收录该内容 1订阅 4篇文章 订阅专栏

目录



AES，即Advanced Encryption Standard，高级加密标准，又称Rijndael加密法，是对称为128位，密钥长度则可以是128，192或256位。

AES加密过程是在一个4×4的字节矩阵上运作，这个矩阵又称为“体（state）”，其初值就区块中的一个字节）。加密时，各轮AES加密循环（除最后一轮外）均包含4个步骤：AddRoundKey、SubBytes、ShiftRows、MixColumns。波士顿大学的Howard Stra

Dokin丶 关注

早在1981 年，DES 算法公布之后，NIST 在标准文献 FIPS 81中公布了 4 种工作模式：

电子密码本：Electronic Code Book Mode (ECB)

密码分组链接：Cipher Block Chaining Mode (CBC)

密文反馈：Cipher Feedback Mode (CFB)

输出反馈：Output Feedback Mode (OFB)

后面又新增了一些工作模式：

计数器模式：Counter Mode (CTR)

填充密码分组链接：Propagating Cipher Block Chaining Mode（PCBC）

ECB模式和**CBC**模式是最常用的两种模式，其他的模式稍作了解即可。

需要块对对齐（填充）的**AES**加密模式：**ECB**、**CBC**、**PCBC**，其余模式无需块对齐。

需要初始向量的**AES**加密模式：除**ECB**模式外，都需要初始向量。

1. ECB模式(Electric Code Book Mode)

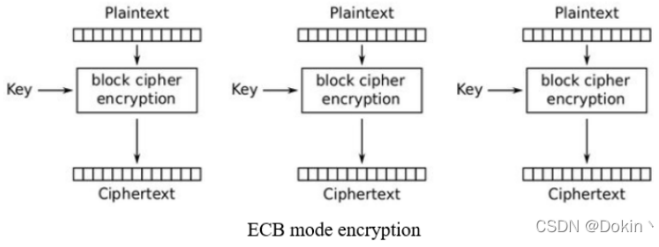
ECB模式是最早采用和最简单的模式，它将加密的数据分成若干组，每组的大小跟加密密钥长度相同，然后每组都用相同的密钥进行加密。

优点：有利于并行计算；误差不会累计(互不干扰）。

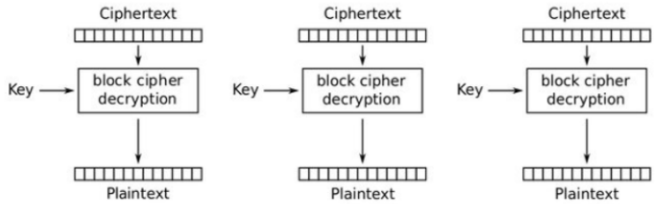
缺点：可能对明文进行主动攻击。

目录
1. ECB□□(Electric Code Book Mode)
2. CBC□□(Cipher Block Chaining Mode)
3. CFB□□(Cipher Feedback Mode)
4. OFB□□(Output Feedback Mode)
5. CTR□□(Counter Mode)
6. PCBC□□(Propagating Cipher Block ...

分类专栏
□□□□ 2□ Beta
RTOS 4□
STM32 11□
Linux□□ 1□
□□ 4□ Beta
Linux 5□
□□□ 2□
□□□□ 1□
Shell 1□
Makefile
Zigbee 9□
□□□□ 2□
□□□□ 1□
□□□□ 2□
C/C++ 4□
□□ 6□



ECB mode encryption



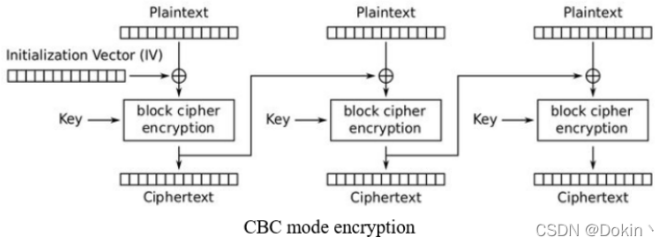
ECB mode decryption

2. CBC模式(Cipher Block Chaining Mode)

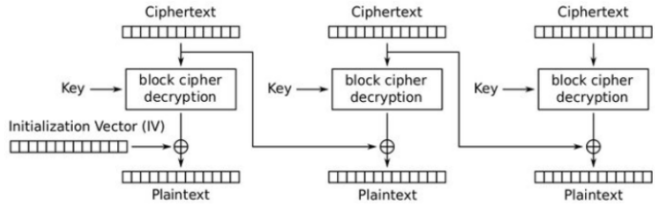
CBC模式对于每个待加密的密码块，在加密前会先与前一个密码块的密文异或然后再用加密器加密（图中的圆圈十字符号表示异或操作，下同）。第一个明文块与一个叫初始化向量的数据块异或。加、解密双方共同知晓密钥和初始化向量才能实现加解密。

优点：安全性比ECB模式高；是SSL的标准。

缺点：数据块之间的加密有依赖关系，因此不能并行计算。



CBC mode encryption



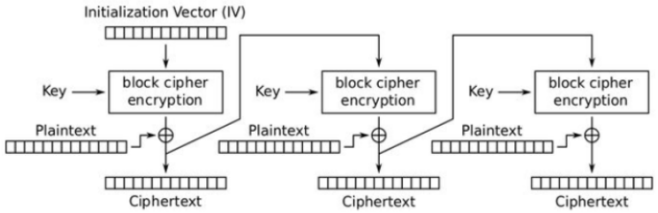
CBC mode decryption

3. CFB模式(Cipher Feedback Mode)

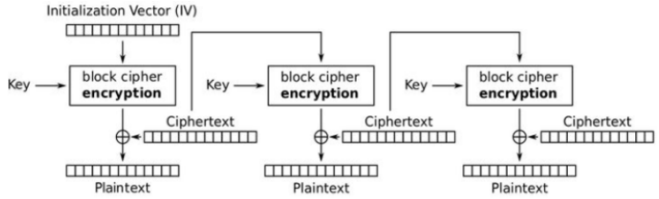
CFB 模式是用分组算法实现流算法，明文数据不需要按分组大小对齐。

优点：明文数据不需要按分组大小对其，即无需填充。

缺点：同CBC模式，无法并行计算。



CFB mode encryption



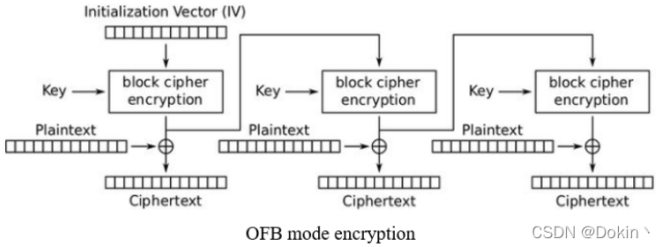
CFB mode decryption

4. OFB模式(Output Feedback Mode)

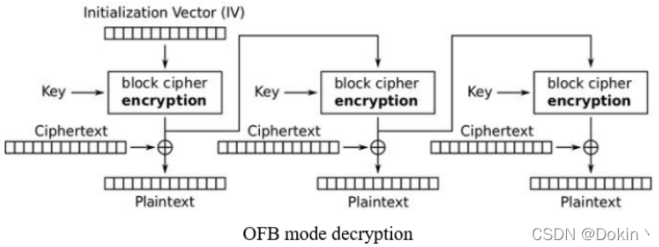
OFB 模式的过程和CBC模式有点像，但明文数据不需要按分组大小对齐。

优点：明文数据不需要按分组大小对其，即无需填充。

缺点：同CBC模式，无法并行计算。



OFB mode encryption



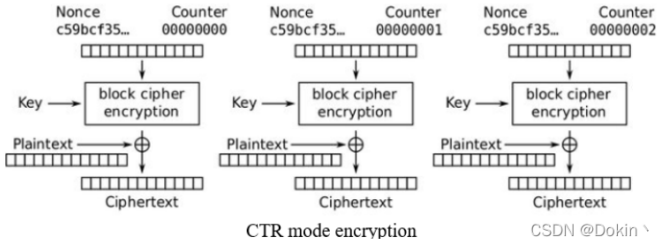
OFB mode decryption

5. CTR模式(Counter Mode)

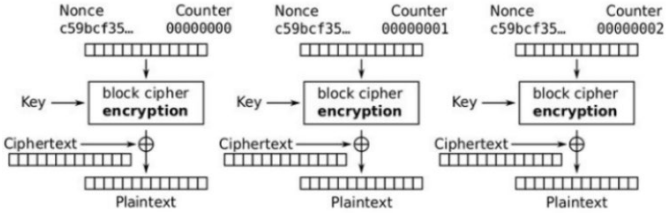
CTR模式是在ECB模式的基础上，引入了Nonce随机数和Counter计数器，Nounce随机数和Counter计数器整体可看作计数器，每加密一段明文，计数器向上加一，并且这个计数器都会和初始IV进行连接、加加、异或等运算，然后使用加密器进行加密，最后在和明文异或得到分段密文。

优点：明文数据不需要按分组大小对其，即无需填充。

缺点：加密方和解密方需要同时维护初始IV、Nonce、Counter。



CTR mode encryption



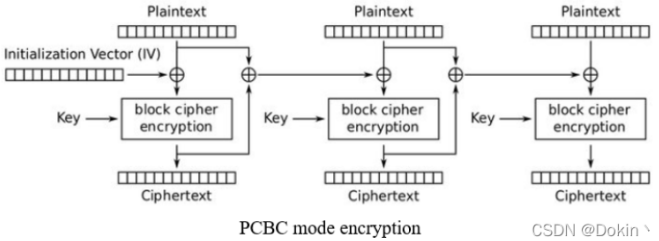
CTR mode decryption

6. PCBC模式(Propagating Cipher Block Chaining Mode)

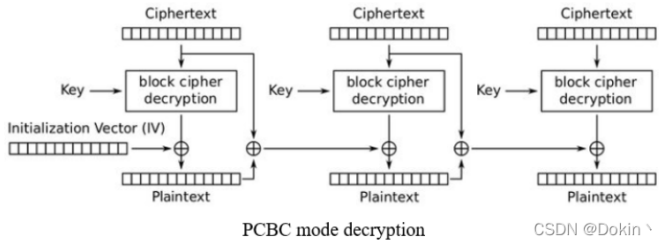
PCBC模式是CBC模式的改进版，与CBC模式的不同点在于，CBC模式后段明文加密的所需向量是前一段的密文，而PCBC模式后段明文加密所需的向量是前一段明文和密文的异或值。

优点：同CBC模式。

缺点：同CBC模式。



PCBC mode encryption



PCBC mode decryption

3 条评论 > Hulake_ 博主AES加密讲得真不错，支持博主继续更新，期待大佬的回访

【加解密】Java的AES默认加密模式_码农印象的博客 5-11

out.println("加密后的内容:" + new String(encrypt)); // 解密 String decrypt = AESUtil.decrypt(encrypt, password); System.out.println("解密后的内容:" + new…

加解密系列之一常用AES五种加密模式python呈现_aesdecode_武念的博客... 5-9
AES五种加密模式 密码有五种工作体制: 1.电码本模式(Electronic Codebook Book (ECB)); 2.密码分组链接模式(Cipher Block Chaining (CBC)); 3.计算器模…

AES五种加密模式（CBC、ECB、CTR、OCF、CFB） feng271374203的博客 5159
分组密码有五种工作体制：1.电码本模式（ElectronicCodebookBook(ECB)）；2.密码分组链接模式（CipherBlockChaining(CBC)）；3.计算器模式（Cou…

AES加密算法的详细介绍与实现 热门推荐 qq_28205153的博客 67万+
AES简介高级加密标准(AES,Advanced Encryption Standard)为最常见的对称加密算法(微信小程序加密传输就是用这个加密算法的)。对称加密算法也就是…

AES加密方式简析_空的加密密钥_xy371661665的博客 5-8
最近了解AES加密相关,做一个总结,希望如有不对之处,请指教* AES加密是对称加密 128 192 256 分别表示密钥的长度* AES的加密方式会将明文拆分成不…

AES加密每种模式的优缺点 abc54250的博客 1008
需要注意的是，以上模式中，ECB模式安全性最差，CBC、CFB和OFB模式相对安全性更高，因此在选择加密模式时需要根据实际情况和安全需求进行选…

java | 使用Cipher类实现AES所有常用加密模式 橘生淮南 1149
java | 使用Cipher类实现AES所有常用加密模式

AES五种加密模式 whatday的专栏 1万+
分组密码在加密时明文分组的长度是固定的，而实用中待加密消息的数据量是不定的，数据格式可能是多种多样的。为了能在各种应用场合安全地使用分…

由浅入深AES-ECB模式加密、解密 五分之一世纪 1万+
学习密码学的同学可以看过来 ?????????????????? 文章目录【1】什么是AES加密【2】AES加密的过程1、明文的分组2、密钥的扩展3、加密的细节…

AES加密 — 详解 qq_39126560的博客 9602
java AES加密

【加密算法】AES mayue_web的博客 4245
本文介绍了AES加密算法供了五种不同的工作模式、明文填充模式、默认加密模式和填充模式。 哈希摘要算法：MD5,SHA，不可逆 对称加密算法：AES…

aes加密算法简单说明 tusong86的博客 3320
里面简要介绍了aes的补齐规则和ecb,cbc模式

什么是AES加密？详解AES加密算法原理流程 m0_69916115的博客 1万+
在密码学中，加密算法分为双向加密和单向加密。单向加密包括MD5、SHA等摘要算法，它们是不可逆的。双向加密包括对称加密和非对称加密，对称加…

AES加密过程详解 Tyler_Zx的博客 9万+
AES算法流程： AES加密过程涉及到4种操作，分别是字节替代、行移位、列混淆和轮密钥加。解密过程分别为对应的逆操作。由于每一步操作都是可逆…

C#开发中常用的加密解密方法汇总 12-16
相信很多人在开发过程中经常会遇到需要对一些重要的信息进行加密处理，今天给大家分享我个人总结的一些加密算法： 常见的加密方式分为可逆和不可…

两种JavaScript的AES加密方式（可与Java相互加解密） 01-19
由于JavaScript属于弱类型脚本语言，因此当其与强类型的后台语言进行数据交互时会产生各种问题，特别是加解密的操作。本人由于工作中遇到用js与Ja…

Android数据加密之Des加密 01-20
前言： 有个同事咨询我有关Android DES加密的相关实现，简单的实现了一下，今天来总结一下。 其他几种加密方式： •Android数据加密之Rsa加密 •A…

python实现加密的方式总结 01-20
加密算法分类 对称加密算法： 对称加密采用了对称密码编码技术，它的特点是文件加密和解密使用相同的密钥 发送方和接收方需要持有同一把密钥，发…

AES加密之五种模式 ncncff51131420的博客 2万+
AES加密AES加密之五种模式简介分析1.电码本模式（Electronic Codebook Book (ECB)2.密码分组链接模式（Cipher Block Chaining (CBC)）## copyFro…

对称加密算法(AES加密)以及对称算法与非对称算法的对比 qq_45475528的博客 1577
主要概括什么是对称加密算法，使用AES的ECB工作模式和CBC工作模式对数据进行加密与解密。以及对称加密算法与非对称加密算法的对比

hutool aes加密 最新发布 04-29
Hutool是一个优秀的Java工具包，其中提供了对AES（Advanced Encryption Standard，高级加密标准）加密的支持。AES是一种常用的对称加密算法，…