Atitit 加密 模式 ECB CBC CTR OFB CFB。

# 分组密码工作模式

## 五种加密模式（CBC、ECB、CTR、OCF、CFB）

分组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.计算器模式（Counter (CTR)）；4.密码反馈模式（Cipher FeedBack (CFB)）；5.输出反馈模式（Output FeedBack (OFB)）。

以下逐一介绍一下：

**1.电码本模式（Electronic Codebook Book (ECB)**

**这种模式是将整个明文分成若干段相同的小段，然后对每一小段进行加密。**

**2.密码分组链接模式（Cipher Block Chaining (CBC)）**

**这种模式是先将明文切分成若干小段，然后每一小段与初始块或者上一段的密文段进行异或运算后，再与密钥进行加密**

**3.计算器模式（Counter (CTR)）**

        计算器模式不常见，在CTR模式中， 有一个自增的算子，这个算子用密钥加密之后的输出和明文异或的结果得到密文，相当于一次一密。这种加密方式简单快速，安全可靠，而且可以并行加密，但是在计算器不能维持很长的情况下，密钥只能使用一次。CTR的示意图如下所示：

4.密码反馈模式（Cipher FeedBack (CFB)）

这种模式较复杂。

5.输出反馈模式（Output FeedBack (OFB)）

这种模式较复杂。

## 初始化向量（IV）[[编辑](https://zh.wikipedia.org/w/index.php?title=%E5%88%86%E7%BB%84%E5%AF%86%E7%A0%81%E5%B7%A5%E4%BD%9C%E6%A8%A1%E5%BC%8F&action=edit&section=2" \o "编辑章节：初始化向量（IV）)]

主条目：[初始化向量](https://zh.wikipedia.org/wiki/%E5%88%9D%E5%A7%8B%E5%8C%96%E5%90%91%E9%87%8F" \o "初始化向量)

[初始化向量](https://zh.wikipedia.org/wiki/%E5%88%9D%E5%A7%8B%E5%8C%96%E5%90%91%E9%87%8F" \o "初始化向量)（IV，Initialization Vector）是许多任务作模式中用于将加密随机化的一个位块，由此即使同样的明文被多次加密也会产生不同的密文，避免了较慢的重新产生密钥的过程。

初始化向量与密钥相比有不同的安全性需求，因此IV通常无须保密，然而在大多数情况中，不应当在使用同一密钥的情况下两次使用同一个IV。对于CBC和CFB，重用IV会导致泄露明文首个块的某些信息，亦包括两个不同消息中相同的前缀。对于OFB和CTR而言，重用IV会导致完全失去安全性。另外，在CBC模式中，IV在加密时必须是无法预测的；特别的，在许多实现中使用的产生IV的方法，例如SSL2.0使用的，即采用上一个消息的最后一块密文作为下一个消息的IV，是不安全的[[12]](https://zh.wikipedia.org/wiki/%E5%88%86%E7%BB%84%E5%AF%86%E7%A0%81%E5%B7%A5%E4%BD%9C%E6%A8%A1%E5%BC%8F" \l "cite_note-12)。

## 填充[[编辑](https://zh.wikipedia.org/w/index.php?title=%E5%88%86%E7%BB%84%E5%AF%86%E7%A0%81%E5%B7%A5%E4%BD%9C%E6%A8%A1%E5%BC%8F&action=edit&section=3" \o "编辑章节：填充)]

主条目：[填充 (密码学)](https://zh.wikipedia.org/wiki/%E5%A1%AB%E5%85%85_(%E5%AF%86%E7%A0%81%E5%AD%A6)" \o "填充 (密码学))

[块密码](https://zh.wikipedia.org/wiki/%E5%A1%8A%E5%AF%86%E7%A2%BC" \o "块密码)只能对确定[长度](https://zh.wikipedia.org/w/index.php?title=%E5%9D%97%E9%95%BF%E5%BA%A6&action=edit&redlink=1" \o "块长度（页面不存在）)的数据块进行处理，而消息的长度通常是可变的。因此部分模式（即[ECB](https://zh.wikipedia.org/wiki/ECB" \o "ECB)和[CBC](https://zh.wikipedia.org/wiki/CBC" \o "CBC)）需要最后一块在加密前进行填充。有数种填充方法，其中最简单的一种是在[明文](https://zh.wikipedia.org/wiki/%E6%98%8E%E6%96%87" \o "明文)的最后填充空字符以使其长度为块长度的整数倍，但必须保证可以恢复明文的原始长度；例如，若明文是[C语言](https://zh.wikipedia.org/wiki/C%E8%AF%AD%E8%A8%80" \o "C语言)风格的[字符串](https://zh.wikipedia.org/wiki/%E5%AD%97%E7%AC%A6%E4%B8%B2" \o "字符串)，则只有串尾会有空字符。稍微复杂一点的方法则是原始的[DES](https://zh.wikipedia.org/wiki/DES" \o "DES)使用的方法，即在数据后添加一个1[位](https://zh.wikipedia.org/wiki/%E4%BD%8D" \o "位)，再添加足够的0位直到满足块长度的要求；若消息长度刚好符合块长度，则添加一个填充块。最复杂的则是针对CBC的方法，例如[密文窃取](https://zh.wikipedia.org/wiki/%E5%AF%86%E6%96%87%E7%AA%83%E5%8F%96" \o "密文窃取)，[残块终结](https://zh.wikipedia.org/w/index.php?title=%E6%AE%8B%E5%9D%97%E7%BB%88%E7%BB%93&action=edit&redlink=1" \o "残块终结（页面不存在）)等，不会产生额外的密文，但会增加一些复杂度。[布鲁斯·施奈尔](https://zh.wikipedia.org/wiki/%E5%B8%83%E9%AD%AF%E6%96%AF%C2%B7%E6%96%BD%E5%A5%88%E7%88%BE" \o "布鲁斯·施奈尔)和[尼尔斯·弗格森](https://zh.wikipedia.org/w/index.php?title=%E5%B0%BC%E5%B0%94%E6%96%AF%C2%B7%E5%BC%97%E6%A0%BC%E6%A3%AE&action=edit&redlink=1" \o "尼尔斯·弗格森（页面不存在）)提出了两种简单的可能性：添加一个值为128的字节（[十六进制](https://zh.wikipedia.org/wiki/%E5%8D%81%E5%85%AD%E8%BF%9B%E5%88%B6" \o "十六进制)的80），再以0字节填满最后一个块；或向最后一个块填充*n*个值均为*n*的字节[[13]](https://zh.wikipedia.org/wiki/%E5%88%86%E7%BB%84%E5%AF%86%E7%A0%81%E5%B7%A5%E4%BD%9C%E6%A8%A1%E5%BC%8F" \l "cite_note-13)。

CFB，OFB和CTR模式不需要对长度不为密码块大小整数倍的消息进行特别的处理。因为这些模式是通过对块密码的输出与明文进行[异或](https://zh.wikipedia.org/wiki/%E5%BC%82%E6%88%96" \o "异或)工作的。最后一个明文块（可能是不完整的）与[密钥流](https://zh.wikipedia.org/wiki/%E5%AF%86%E9%92%A5%E6%B5%81" \o "密钥流)块的前几个字节异或后，产生了与该明文块大小相同的密文块。流密码的这个特性使得它们可以应用在需要密文和明文数据长度严格相等的场合，也可以应用在以流形式传输数据而不便于进行填充的场合

# Rf

AES五种加密模式（CBC、ECB、CTR、OCF、CFB） - 月之星狼 - 博客园.html

分组密码工作模式 - 维基百科，自由的百科全书.html