**AES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。**



**6.** **cipher block chaining message authentication code (CBC-MAC)**

