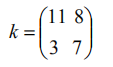
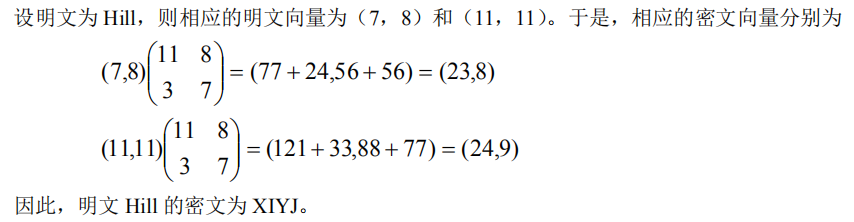
1. 用 Hill 密码加密消息”hill”，密钥为：



解：



1. Hill 密码不能抵抗已知明文攻击，如果有足够多的明文和密文对，就能破解 Hill 密码。

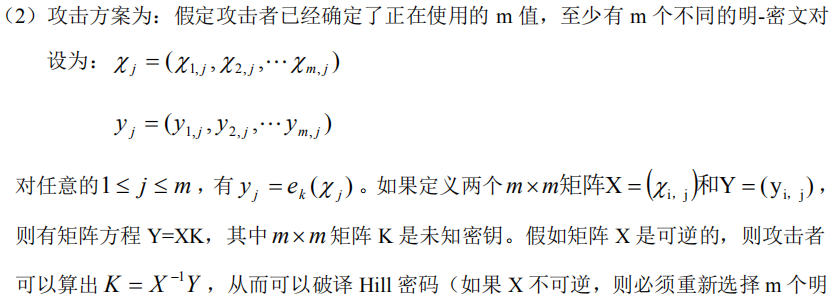
(1) 攻击者至少有多少个不同明文-密文对才能攻破该密码？

(2) 描述这种攻击方案。

解：

1. 设Hill 密码密钥K是m\*m矩阵，则破解一个 Hillm密码至少应该有 m 个不同的明文-密文对。

（2）



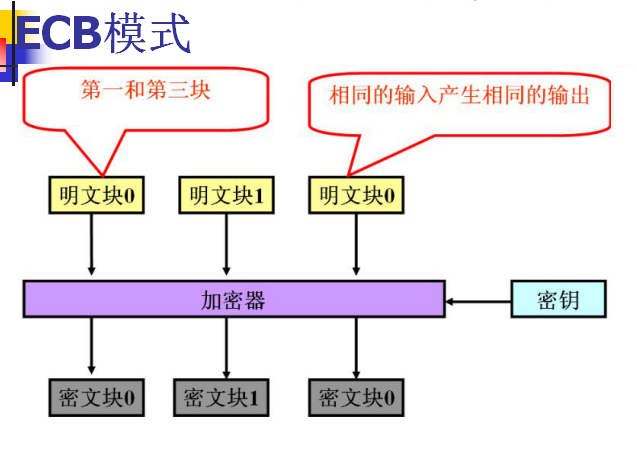
1. 试描述DES的4种工作模式。

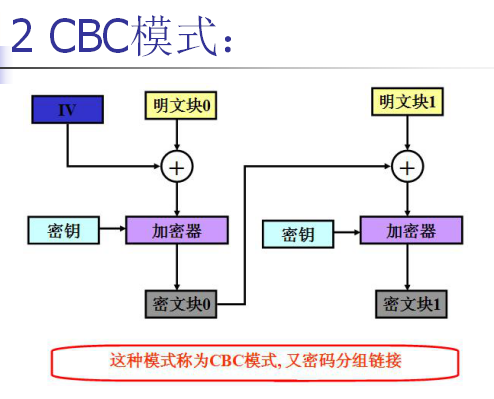
电子密码本ECB (electronic codebookmode)；

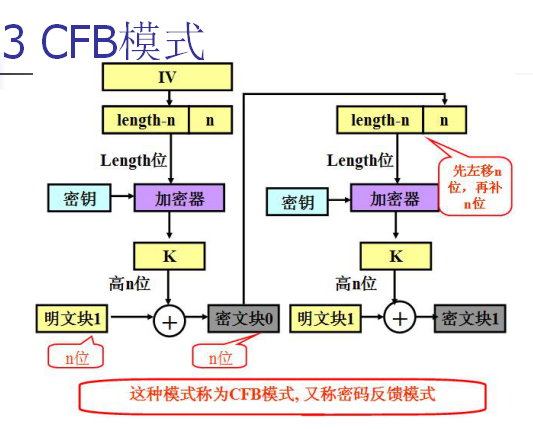
密码分组链接CBC (cipher blockchaining)；

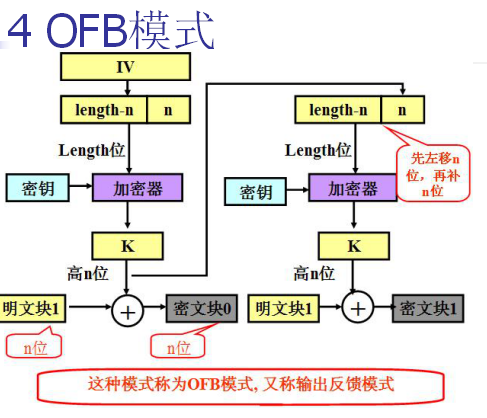
密码反馈CFB (cipher feedback)；

输出反馈OFB (output feedback)；









1. 在CBC模式中，有可能对多个明文分组进行并行加密吗？解密呢？

不能并行加密，

可以并行解密。