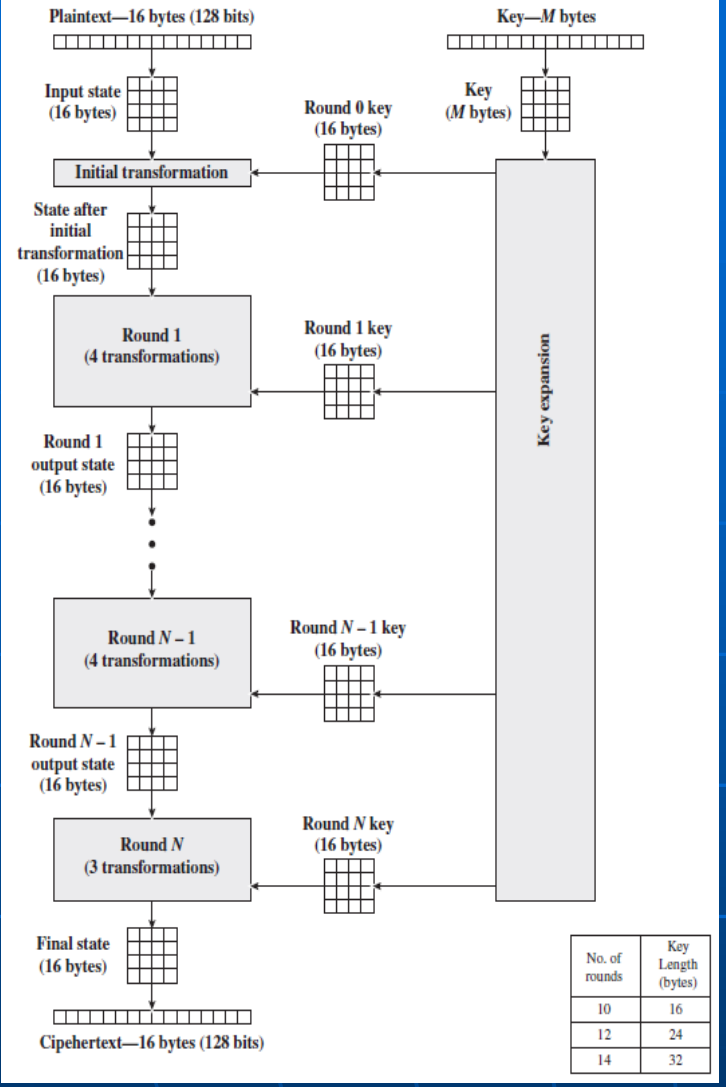


密码理论与技术

典型安全方案概览

课本阅读：Stallings 网络安全与密码学(第六版)

3.1~3.2、3.3、3.4：DES加密方案

5.2、5.3、5.4：AES加密方案

6.2~6.7：分组密码的密文组合模式

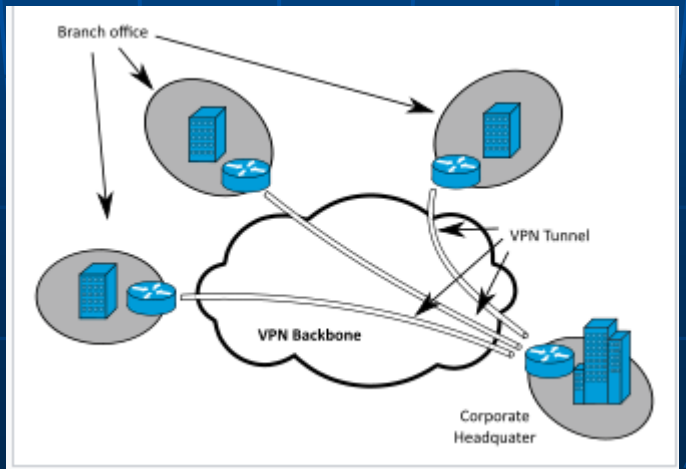
黄色：重点阅读；全部阅读以概念性的理解为主。

本组4节课的学习，以建立正确的概念为主。

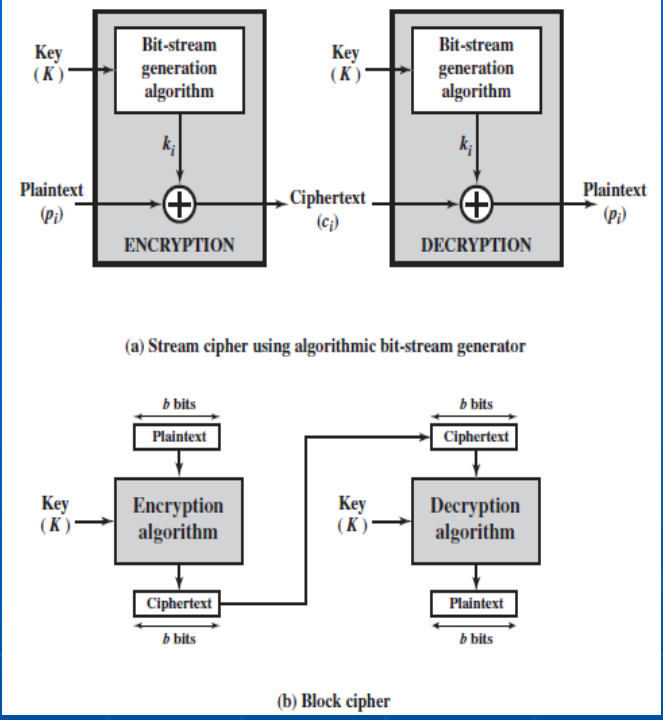
接下来的课程内容，将在此基础上发展对安全方案/协议更为定量的认知和理解。

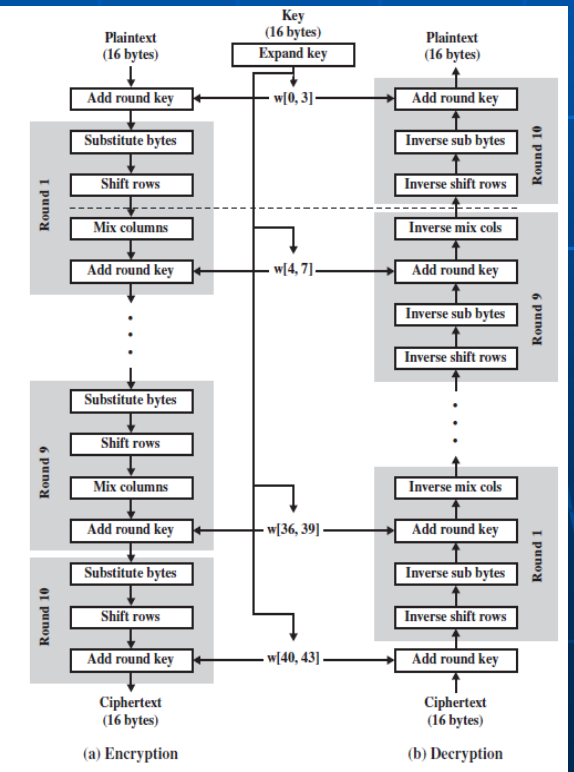
典型安全问题

- 保密性问题
- 保护通过不可信任的信道所传输的信息不被泄露。
- 认证性(完整性)问题
- 保护通过不可信任的信道所传输的信息不被篡改。
- 秘密交换问题
- A、B通过不可信任的信道交换一组消息，最终生成第三方未知的共享秘密。
- ……



基本加密方案





- 对称/分组加密
- 公钥加密
- 混合加密

对称加密方案(1)

- 问题：A如何通过不可信任的信道，
- 完全可靠地向B传递信息（保密）。

- 解决方案
- A(K) B(K)

明文M (plaintext) 2.传递密文y (cyphertext)

1.加密计算：

y=E(K,M)

3.解密计算：

M=D(K,y)

“这仿佛是说，我俩通过一个贼来传递珠宝...如果加密方案是安全的，就意味着他想偷也偷不着我们的东东...是这样吧”
“是这样的”
“哦...听上去真是心惊肉跳！”
“不，我觉得这才叫斗智斗勇、精彩绝伦！”

对称加密方案(2)

- 特　点：
- 密钥生成算法KG，加密算法E，解密算法D均公开。
- 密钥K保密(仅通信双方知道且共享)。
- 安全性(保密性)：

若攻击者A未知共享的密钥K，则概率

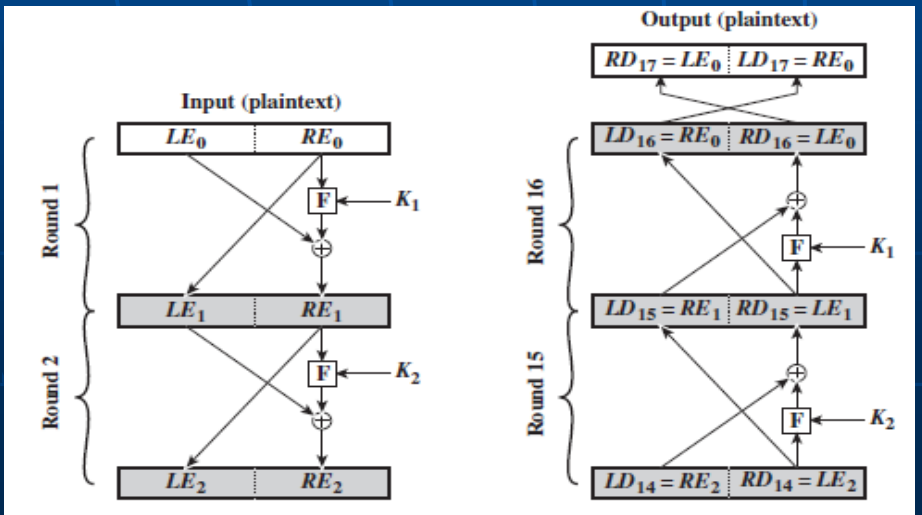
$P[M \leftarrow A(y, |M|, |K|, E, D, KG)]$很小。

“安全就是要使密文被成功破译的概率很小...听上去有道理，但多小才算是很小呀？”
“这个么...意味着把概率换算成取得接近100%的成功所需要的时间，将长的可怕。”
“所以.....”
“所以就没有哪个贼试图盗窃这种保护下的珠宝啦，得等他下下下...下辈子才能享受果实”
“哦...有点明白了...除非他运气好的出奇”
“但那只是运气而已，没法指望的东西！”
“我们来估算一下，如果每次破译成功的概率是2^{-100}，每秒破译1亿次，要用多少年才能接近100%的成功？”

对称加密方案(3)

对称加密方案实例/业界标准

- DES/64bit 定长密钥 参阅Stallings 第三章
- AES/128-256bit 变长密钥 参阅Stallings第五章
- IDEA/64bit 定长密钥(欧盟加密标准)
- Blowfish/64bit 定长密钥（适合软件实现的加密算法）



公钥加密方案(1)

- 问题：
- A如何通过不可信任的信道，保密地向B传递信息M。
- 解决方案
- A　　pk公开　　B(sk)

0. 生成公钥-私钥对(pk,sk)

明文M　　2.传递密文y

1.加密计算：y=E(pk,M)　　3. 解密计算：M=D(sk,y)

“加密算法E(pk,.)是一把公开可得到的锁，仅有接收方持有打开它的钥匙sk。”

“这样说来，公钥加密好像是...每个人有一个邮箱，任何其他人都可以投信进去，但只有邮箱的主人才能打开它。”

“二师兄，你...你一点也不傻呀！”

公钥加密方案(2)

- 特　点：
- 密钥生成算法KG, 加密算法E, 解密算法D均公开。
- KG生成一对密钥，其中一个公开(pk)、一个保密(sk)。
- sk完全由信息的接收方通过运行算法KG生成。
- 私钥sk仅为解密方持有(通信双方不共享任何秘密)。
- 安全性(保密性)：

若攻击者A未知私钥 sk，则

$P[M \leftarrow A(y, |M|, E, D, KG, pk)]$很小。

参阅：Stallings 9.1