现代密码学

第二十三讲 3DES

信息与软件工程学院

多重DES

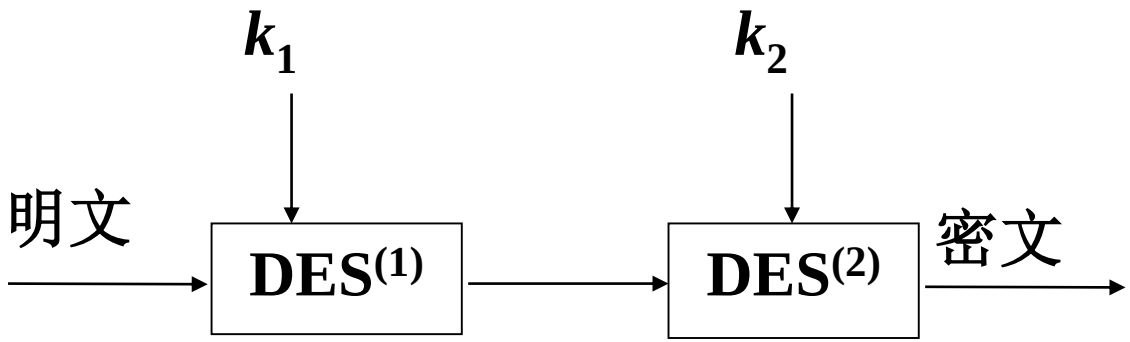
- 如果一个分组密码易受到穷举密钥搜索攻击，那么对同一消息加密多次就有可能增强安全性
- 多重DES就是使用多个密钥利用DES对明文进行多次加密。使用多重DES可以增加密钥量，从而大大提高抵抗穷举密钥搜索攻击的能力
- 多重加密类似于一个有着多个相同密码的级联，但各级密码无需独立，且每级密码既可以是一个分组密码加密函数，也可是相应的解密函数

第二十三讲 3DES

- 双重DES算法
- 三重DES算法

双重DES

- 简单的对消息x_i利用两个不同的密钥进行两次加密
- 目的是为了抵抗穷搜索攻击，期望密钥长度扩展为112比特



中间相遇攻击

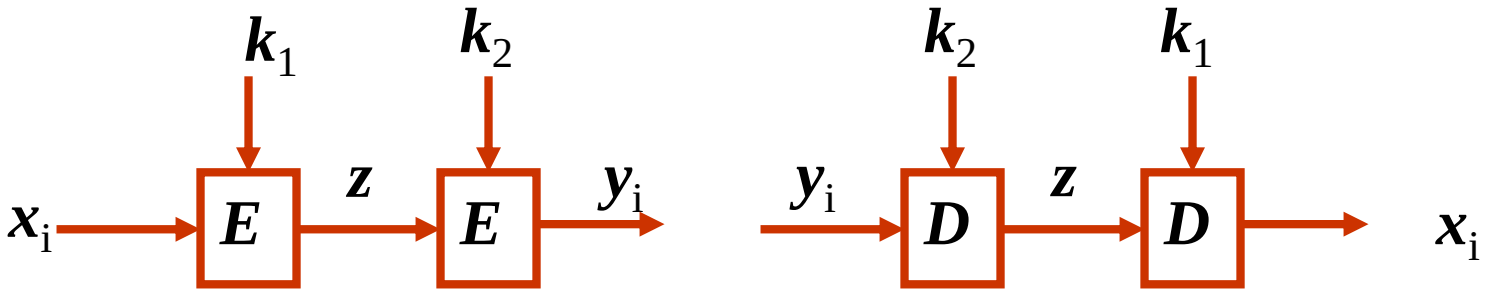
由Diffie和Hellman[1977]最早提出，可以降低搜索量，基本想法如下。

若有明文/密文对(x_i,y_i)满足

$$y_i=E_{k2}[E_{k1}[x_i]]$$

则可得

$$z=E_{k1}[x_i]=D_{k2}[y_i]$$



中间相遇攻击的步骤

给定一已知明密文对(x_1,y_1)，可按下述方法攻击。

- 以密钥k_1的所有2^{56}个可能的取值对此明文x_1加密，并将密文z存储在一个表中；
- 从所有可能的2^{56}个密钥k_2中依任意次序选出一个对给定的密文y_1解密，并将每次解密结果z在上述表中查找相匹配的值。一旦找到，则可确定出两个密钥k_1和k_2；
- 以此对密钥k_1和k_2对另一已知明文密文对$(x_2,\ y_2)$中的明文x_2进行加密，如果能得出相应的密文y_2就可确定k_1和k_2是所要找的密钥。

中间相遇攻击的复杂度

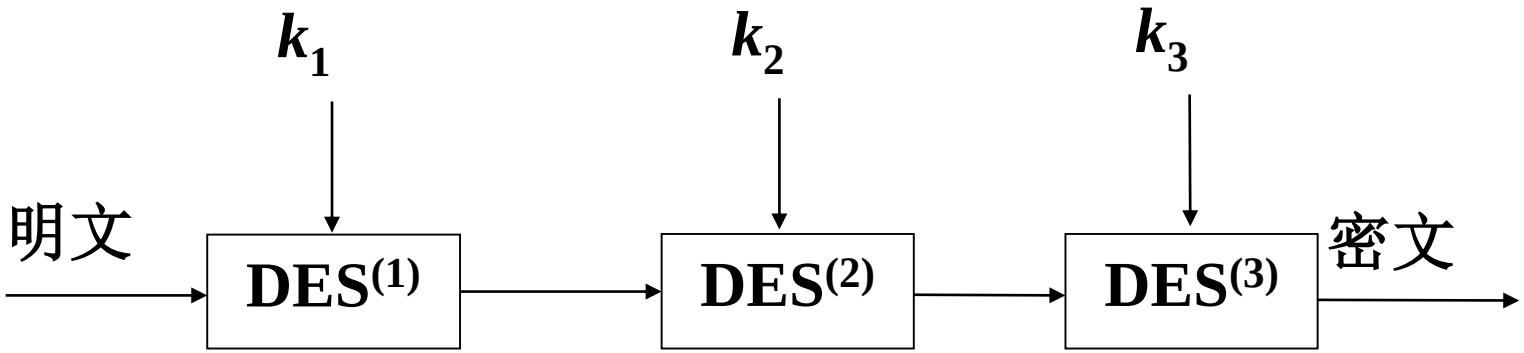
- 对于给定明文x，以两重DES加密将有2^{64}个可能的密文。
- 可能的密钥数为2^{112}个。所以，在给定明文下，将有$2^{112}/2^{64}=2^{48}$个密钥能产生给定的密文。
- 用另一对64比特明文/密文对进行检验，就使虚报率降为$2^{48-64}=2^{-16}$。
- 这一攻击法所需的存储量为$2^{56}\times 8$ Byte，最大试验的加密次数$2\times 2^{56}=2^{57}$。这说明破译双重DES的难度为2^{57}量级。

第二十三讲 3DES

- 双重DES算法
- 三重DES算法

三重DES算法

- 三重DES中三个密码组件既可以是一个加密函数，也可以是一个解密函数。
- 当$k_1=k_3$时，则称为双密钥三重DES

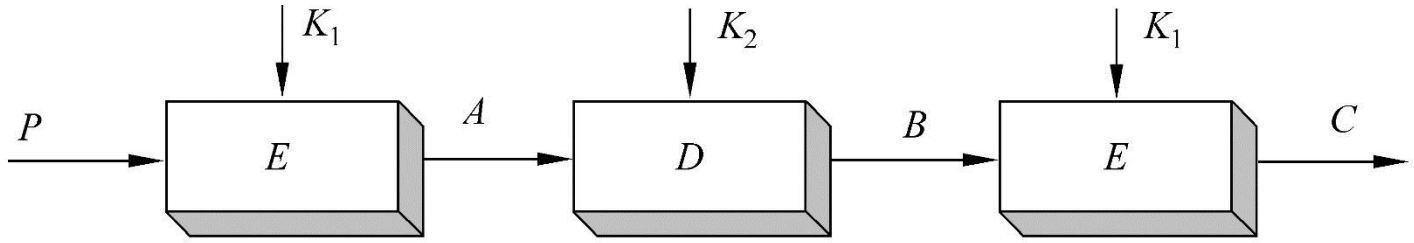


双密钥三重DES算法

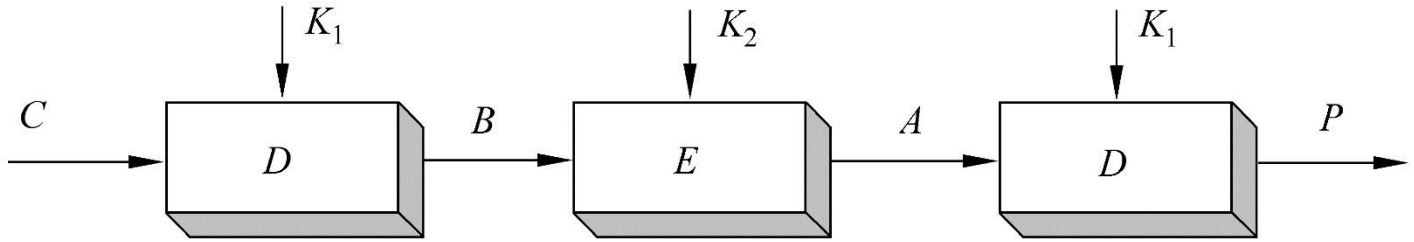
加密：$y=E_{k1}[D_{k2}[E_{k1}[x]]]$

解密：$x=D_{k1}[E_{k2}[D_{k1}[y]]]$

- 称其为加密-解密-加密方案，简记为EDE(encrypt-decrypt-encrypt)。
- 此方案已在ANSI X9.17和ISO 8732标准中采用，并在保密增强邮件(PEM)系统中得到利用。



(a) 加密



(b) 解密

双密钥三重DES算法的安全性

- 破译它的穷举密钥搜索量为$2^{112} \approx 5 \times 10^{35}$量级
- 差分分析破译也要超过10^{52}量级
- 此方案仍有足够的安全性

感 谢 聆 听!

xynie@uestc.edu.cn