现代密码学

第二十二讲 DES的安全性

信息与软件工程学院

第二十二讲 DES的安全性

- DES的弱密钥
- DES的密钥长度的争论

关于DES密钥

- 互补性。**DES**算法具有下述性质。若明文组***x***逐位取补，密钥***k***逐位取补，即$y=DES_k(x)$, 则有 $\bar{y} = DES_{\bar{K}}(\bar{x})$

  这种互补性会使**DES**在选择明文破译下所需的工作量减半。

- 弱密钥和半弱密钥。
  - 弱密钥：$E_K \bullet E_K = I$，**DES**存在**4**个弱密钥

    $$DES_k(DES_k(x))=x$$

  - 半弱密钥: $E_{K1} = E_{K2}$，至少有**12**个半弱密钥

    $$y = E_{k1}(x) = E_{k2}(x)$$

DES的弱密钥

- **DES算法在每次迭代时都有一个子密钥供加密用。如果给定初始密钥k，各轮的子密钥都相同，即有$k_1=k_2=\ \ldots\ =k_{16}$，就称给定密钥$k$为弱密钥(Weak key)。**
- 原始密钥

$$(0,\ 0) \rightleftharpoons 01\ \ 01\ \ 01\ \ 01\ \ 01\ \ 01\ \ 01\ \ 01$$

$$(0,15) \rightleftharpoons 1F\ \ 1F\ \ 1F\ \ 1F\ \ 0E\ \ 0E\ \ 0E\ \ 0E$$

$$(0,15) \rightleftharpoons E0\ \ E0\ \ E0\ \ E0\ \ F1\ \ F1\ \ F1\ \ F1$$

$$(0,15) \rightleftharpoons FE\ \ FE\ \ FE\ \ FE\ \ FE\ \ FE\ \ FE\ \ FE$$

置换选择1后的密钥

$C\quad D$

$$(0,\ 0) \rightleftharpoons 00\ \ 00\ \ 00\ \ 00\ \ 00\ \ 00\ \ 00$$

$$(0,15) \rightleftharpoons 00\ \ 00\ \ 00\ \ 0F\ \ FF\ \ FF\ \ FF$$

$$(0,15) \rightleftharpoons FF\ \ FF\ \ FF\ \ F0\ \ 00\ \ 00\ \ 00$$

$$(0,15) \rightleftharpoons FF\ \ FF\ \ FF\ \ FF\ \ FF\ \ FF\ \ FF$$

第二十二讲 DES的安全性

- DES的弱密钥
- DES的密钥长度的争论

密钥长度的争论

- DES算法正式公开发表以后，引起了一场激烈的争论
- 对DES安全性批评意见中，较为一致的看法是DES的密钥短了些。IBM最初向NBS提交的建议方案采用112 bits密钥，但公布的DES标准采用64 bits密钥。有人认为NSA故意限制DES的密钥长度。
- 采用穷搜索已经对DES构成了威胁。
- 1977年Diffie和Hellman提出了制造一个每秒能测试106个密钥的大规模芯片，这种芯片的机器大约一天就可以搜索DES算法的整个密钥空间，制造这样的机器需要两千万美元。

密钥搜索

- 1993年，R.Session和M.Wiener给出了一个非常详细的密钥搜索机器的设计方案
- 基于并行的密钥搜索芯片，此芯片每秒测试5×107个密钥
- 当时这种芯片的造价是10.5美元，5760个这样的芯片组成的系统需要10万美元，这一系统平均1.5天即可找到密钥
- 如果利用10个这样的系统，费用是100万美元，但搜索时间可以降到2.5小时。

密钥搜索与超级计算

- DES的56位短密钥面临的另外一个严峻而现实的问题是：国际互联网Internet的超级计算能力。
- 1997年1月28日，美国的RSA数据安全公司在互联网上开展了一项名为“密钥挑战”的竞赛，悬赏一万美元，破解一段用56位密钥加密的DES密文。

密钥挑战

- 一位名叫Rocke Verser的程序员设计了一个可以通过互联网分段运行的密钥穷举搜索程序，组织实施了一个称为DESHALL的搜索行动，成千上万的志愿者加入到计划中
- 计划实施的第96天，即挑战赛计划公布的第140天，1997年6月17日晚上10点39分，美国盐湖城Inetz公司的职员Michael Sanders成功地找到了密钥
- 在计算机上显示了明文：“The unknown message is: Strong cryptography makes the world a safer place”

DES的破解

- 1998年7月电子前沿基金会（EFF）使用一台25万美圆的电脑在56小时内破译了56比特密钥的DES。
- 1999年1月RSA数据安全会议期间，电子前沿基金会用22小时15分钟就宣告破解了一个DES的密钥。

DES的安全性的其他方面

密文与明文、密文与密钥的相关性

Meyer[1978]详细研究了**DES**的输入明文与密文及密钥与密文之间的相关性。表明每个密文比特都是所有明文比特和所有密钥比特的复合函数，并且指出达到这一要求所需的迭代次数至少为**5**。**Konheim[1981]**用χ^2检验证明，迭代**8**次后输出和输入就可认为是不相关的了。

DES的其他攻击方法

目前攻击**DES**的主要方法有时间-空间权衡攻击、差分攻击、线性攻击和相关密钥攻击等方法，在这些攻击方法中，线性攻击方法是最有效的一种方法。

感 谢 聆 听!

xynie@uestc.edu.cn