在传统的对称密钥加密技术中，对小型的、不太重要的事务来说，40 位的密钥就足够安全了。但现在的高速工作站就可以将其破解，这些工作站每秒可以进行数十亿次计算。

相比之下，对于对称密钥加密技术，128 位的密钥被认为是非常强大的。实际上，长密钥对密码安全有着非常重要的影响，美国政府甚至对使用长密钥的加密软件实施了出口控制，以防止潜在的敌对组织创建出美国国家安全局（National Security Agency，NSA）自己都无法破解的秘密代码。

Bruce Schneier 编写的 *Applied Cryptography*（John Wiley & Sons 出版社）是一本很棒的书，书中有一张表，表中对使用 1995 年的技术和耗费，通过猜测所有的密钥来破解一个 DES 密码所需的时间进行了描述。[5] 表 14-1 摘录了这张表。

表14-1　较长的密钥要花费更多的精力去破解（来自*Applied Cryptography*一书，1995年的数据）

攻击耗费	40位密钥	56位密钥	64位密钥	80位密钥	128位密钥
100 000 美元	2 秒	35 小时	1 年	70 000 年	10^{19} 年
1 000 000 美元	200 毫秒	3.5 小时	37 天	7 000 年	10^{18} 年
10 000 000 美元	20 毫秒	21 分钟	4 天	700 年	10^{17} 年
100 000 000 美元	2 毫秒	2 分钟	9 小时	70 年	10^{16} 年
1 000 000 000 美元	200 微秒	13 秒	1 小时	7 年	10^{15} 年

根据 1995 年微处理器的速度，愿意花费 100 000 美元的攻击者可以在大约 2 秒内破解一个 40 位的 DES 代码。2002 年的计算机就已经比 1995 年的快 20 倍了。除非用户经常修改密钥，否则对于别有用心的攻击者来说，40 位的密钥是不安全的。

DES 的 56 位标准密钥长度就更安全一些。从 1995 年的经济水平来说，花费 100 万美元进行的攻击还是要几个小时才能破解密码。但可使用超级计算机的用户则只需 314
数秒钟即可通过暴力方法破解密码。与之相对的是，通常大家都认为长度与 Triple-DES 密钥相当的 128 位 DES 密钥实际上是任何人以任何代价都无法通过暴力攻击破解的。[6]

注 5：1995 年之后，计算速度得到了飞速的提高，费用也降低了。你越晚读到这本书，计算的速度就会越快！但即使所需的时间会成 5 倍、10 倍或更多倍的减少，这张表仍然是有参考价值的。

注 6：但是，长的密钥并不意味着可以高枕无忧了！加密算法或实现中可能会有不为人注意的缺陷，为攻击者提供了可攻击的弱点。攻击者也可能会有一些与密钥产生方式有关的信息，这样他就会知道使用某些密钥的可能性比另一些要大，从而有助于进行有目的的暴力攻击。或者用户可能将保密的密钥落在了什么地方，被攻击者偷走了。