第3章 密 码 学

本章主要内容

学习目标

在学完本章之后，应该能：

- 解释密码学的概念
- 描述对称密钥加密和密钥长度的重要性
- 解释协商阶段
- 说明初始认证，包括 MS-CHAP
- 描述密钥，包括公钥加密
- 解释电子签名的工作原理，包括数字签名、数字证书和密钥消息认证码（HMAC）
- 描述用于认证的公钥加密
- 描述量子安全
- 解释加密系统，包括 VPN、SSL 和 IPSec

注意：本章要学习的内容难度较大。每个单独的主题都需要密切关注，慢慢学习。此外，本章还包含许多彼此相似的概念。在学习时，要小心区分这些类似的概念。

3.1 什么是密码学

大多数人认为信息安全是最近才出现问题。实际上，安全地发送信息的需求已存在了数千年。早期的军事指挥官需要安全地发出命令，文艺复兴时期的商业王子需要保护商业机密。目前，企业和政府有同样的保密需求。为此，企业和政府转向密码学。密码学是使

用数学运算保护各方之间传输的消息或存储在计算机上的数据。

密码学是使用数学运算保护各方之间传输的消息或存储在计算机上的数据。

在 20 世纪 60 年代，许多人认为密码学将是应对攻击的主要对策。虽然后来证明这个观点略带局限性，但密码学仍是非常重要的安全对策。此外，密码学也是其他许多对策的组成部分。因此，本章和下一章将详细讨论密码学的技术对策。

新闻

巴西当局从一名涉嫌金融犯罪的巴西银行家 Daniel Dantas 那里缴获了 5 个硬盘。巴西国家犯罪学研究所（NIC）历时 5 个月，试图破解硬盘密码但未能成功。NIC 请求联邦调查局（FBI）提供帮助。历时 12 个月，FBI 穷尽了各种基于字典的攻击，也没能破解硬盘的密码。FBI 破解硬盘宣告失败。

Dantas 使用 256 位 AES 加密算法来加密硬盘驱动器[1]。算法使用流行的第三方加密软件 TrueCrypt 实现加密。如果 Dantas 使用较弱的密码，即来自于字典的常用字，那么硬盘数据早就被解密了。

3.1.1　为保密性而进行加密

常见的安全目标是保密性[2]，这意味着拦截消息的人无法读取消息。图 3-1 表明，保密需要使用某类密码系统进行加密，也就是说，是为了保密性而进行加密。密码学的最初目标是为保密性而进行加密[3]。

保密意味着拦截消息的人无法读取消息。

3.1.2　术语

明文

如图 3-1 所示，原始消息称为明文。顾名思义，只对文本消息进行加密。实际上，当创造明文这一术语时，情况真是如此。然而目前，明文消息可以是图像、音频、视频或几种数据格式的组合。虽然原有的命名不能改动，但目前明文是指任何的原始消息。

加密与密文

加密是指将明文变成伪随机比特流的过程。这个变换过程称为加密。密文是指所生成的伪随机比特流。发送方将密文发送给接收方。即使窃听者确实拦截了密文，他也不能理解密文。但接收方能解密密文，将密文还原成原始的明文。

1　John Leyden, “Brazilian Banker’s Crypto Baffles FBI,” TheRegister.com, June 28,2010. http://www.theregister.co.uk/2010/06/28/brazil_banker_crypto_lock_out.

2　在历史上，保密性也称为隐私。然而在过去几年中，隐私已经只意味着个人隐私了。

3　事实上，“密码学”源于希腊语 kryptos（隐藏）和 graphos（写入）。除了预期的接收方之外，对每个人都隐藏了写入消息的含义。

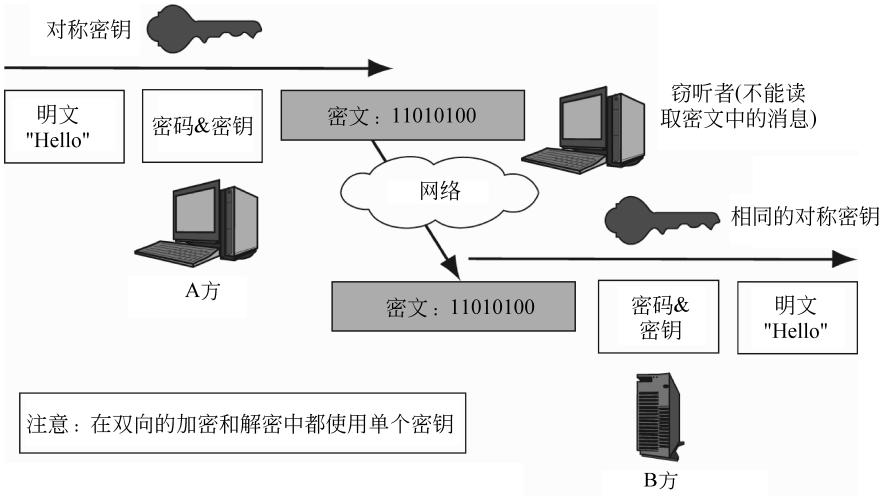


图 3-1　为保密性而进行的对称密钥加密

密码

如图 3-1 所示，加密和解密需要两个参数。第一个参数是密码，密码是在加密和解密中使用的特定的数学过程。目前有许多密码，且它们的操作都有所不同。发送方和接收方必须使用相同的密码，接收方才能解密消息。

密码是在加密和解密中使用的特定的数学过程。

密钥

加密和解密需要的第二个参数是密钥，密钥是 1 和 0 组成的随机字符串，长度为 40 位至 4000 位。长密钥难以猜测，因此具有更强的保密性。给定密码，对相同的明文，不同的密钥会生成不同的密文。

密钥是由 1 和 0 组成的随机字符串。

密钥保密

数学家 Auguste Kerckhoffs 认为，在实践中不可能保密密码，鲜有经得起完美测试的密码。通常能很容易地确定所用的密码。但幸运的是，Kerckhoffs 证明，只要密钥保密，则双方仍能保密。Kerckhoffs 定律认为，密钥保密是安全加密的秘诀[1]。

Kerckhoffs 定律认为，为了保密，通信双方只需保密密钥，而无须保密密码。

3.1.3　简单密码

图 3-2 给出了简单密码的示例。密码取自字母表中的字母。该图包含了三列。

- 第一列是相当平凡的明文。到了该说明一下的时间了。明文不包含大写字母和空格

1　Auguste Kerckhoffs, “La Cryptographie Militaire,” Journal des Sciences Militaires, Vol. IX, January 1883, pp. 5-83 and February 1883, pp. 161-191.

只是为了简化这个示例。

- 第二列是密钥。密钥是 1～26 的数字。
- 第三列是要发送的密文。

在这个密码中，通过将每个字母在字母表中向后移动，将明文变为密文。在字母表中，将明文字母向后移位 N 位，其中 N 是字母向后移动的位数。例如，如果明文字母是 b，密钥值是 2，则密文符号是 d。

- 在示例中，明文的第一个字母为 n，密钥值为 4。字母表中，n 向后移动 4 位，则字母为 r，因此，r 是第一个字母 n 的密文符号。
- 第二个明文字母是 o。此时，密钥值为 8。因此，密文为 w。
- 明文的第三个字母是 w，密钥值是 15。向后移动 15 位已超出了字母表的范围，这时要将字母表首尾相连，从 a 重新开始。最终，w 的密文符号为 l。

明文	密钥	密文
n	4	r
o	8	w
w	15	l
i	16	…
s	23	…
t	16	…
h	3	…
e	9	…
t	12	…
i	20	…
m	6	…
e	25	…

图 3-2　对称密钥密码的示例

到目前为止，我们得到了密文 rwl。在测试理解问题中，请读者自行完成所有明文到密文的转换，得到最终的密文。

如果你看过电视游戏节目“财富之轮”，你会知道字母表中最常见的字母是 e。在这个简单消息中，字母 e 出现了两次。然而，这两次的密钥值是不同的，分别是 9 和 25。如果简单密码使用随机密钥，则通过对密文进行字母频率分析来得到明文是不可能的。

这个示例使用字母表中的字母作为明文。而几乎所有计算机的信息都被编码为一组位串。密钥也是 1 和 0 的字符串。此外，真实的密码使用多轮计算。当加密完成时，密文已类似于纯随机的 1 和 0 的字符串。

3.1.4　密码分析

密码破译者是指破解加密的人。最简单的密码分析类型是暴力密钥破解：即密码破译者尝试所有可能的密钥，直到找到正确的密钥。然后，正如本章后面所介绍的，如果密钥很长，暴力密钥破解则因所需时间太长，而不能使用。

在某些情况下，密码破译者至少可以猜出部分消息。例如，在第二次世界大战中，日本海军的报告经常以同样的标准化开场致敬开始。当知道这一规律后，密码破译者至少能够很快地知道部分密钥。

此外，密码的实现可能很弱，每个消息都可能“泄露”部分密钥。802.11 无线局域网传输标准最初使用有线等效保密（WEP）的安全方法。WEP 使用了能泄露信息的 RC4 加密密码实现。目前，两三分钟就能破解 WEP 密钥。

新闻

俄罗斯公司 ElcomSoft 编写了软件，能自动找到 TrueCrypt、BitLocker 和 PGP 的解密密钥。在这几种加密软件中，用户已将加密软件配置为自动解密，并将解密密钥临时存储

在主存储器中。ElcomSoft 推出了 299 美元的工具，能找到存储在内存中的解密密钥，之后能解密受保护的数据。此工具甚至能找到存储在休眠文件中的解密密钥。然而，如果关闭电源，且禁用休眠，则不能恢复解密密钥[1]。

测试你的理解

1. a. 定义加密。
   b. 什么是保密性？
   c. 区分明文和密文。
   d. 通过网络传输的是明文还是密文？
   e. 什么是密码？
   f. 什么是密钥？
   g. 为了保密性，在加密中必须保密什么？
   h. 什么是密码破译者？
2. 完成图 3-2 中的加密。

3.1.5 替换与置换密码

目前，密码中的具体数学过程非常复杂。但是，大多数密码都是替换和置换这两个基本数学过程的变种。

3.1.6 替换密码

在替换密码中，一个字符被另一个字符替换，但字符位置不变。这听起来像图 3-2 中所讨论的简单密码。的确如此，图 3-2 中的示例密码是一种非常简单的替换密码。每个字符被字母表中的另一个字符替换。但每个字符的位置是不变的。所以 n-o-w 变成了 r-w-1。

在替换密码中，一个字符被另一个字符替换。

3.1.7 置换密码

在置换密码中，基于字符在消息中的初始位置，依次在消息内移动。与替换密码不同，字符本身不变，只是改变字符在消息中的位置。

在置换密码中，字符在消息中移动，但字符不变。

图 3-3 给出了一个简单的置换密码。首先，将明文（nowisthet）排列成 3 乘 3 的矩阵，或根据消息大小排成合适的矩阵。密钥有 6 个数字（132231）。密钥第一部分（132）由矩阵中每列上的数字组成，密钥第二部分（231）由矩阵中每行上的数字组成。

1 John Leyden, “PGP, TrueCrypt-Encrypted Files CRACKED by f300 Tool,” The Register, December 12, 2012. http://www.theregister.co.uk/2012/.

密钥（第二部分）	密钥（第一部分）		
	1	**3**	**2**
2	n	o	w
3	i	s	t
1	h	e	t

图 3-3　置换密码

密码确定了如何从置换盒中取字符。第一个要取出字符的列密钥值为 1，行密钥值也为 1。在置换盒中，密钥值对(1,1)对应的是第一列和第三行，这个位置的字符是 h，所以 h 是第一个密文字符。

第二个要取出字符的列密钥值为 1，行密钥值为 2。在置换盒中，密钥值对(1,2)对应的是第一列和第一行。这个位置的字符是 n，所以 n 是第二个密文字符。到目前为止，我们得到了密文的前二位：hn。从置换盒中，以此类推，以列、行的顺序取出字母，就确定了其余的密文。

3.1.8　真实世界加密

在替换密码中，字母改变，但位置不变。在置换密码中，字母不变，但在密文中的位置改变。真正的密码要比所讲的示例密码复杂得多。首先，加密是在位上完成，而不是在字母表中的字母上完成。此外，真实世界的密码是几轮置换和替换的混合，以便得到完美的随机性。但非常幸运，组织中的安全专业人员不必理解实际的、具体的加密密码工作原理。

测试你的理解

3．a. 字母不变的是置换密码还是替换密码？

　　b. 字母保持原始位置不变的是置换密码还是替换密码？

4. 完成图 3-3 中的加密。

3.1.9　密码与编码

当你读本章时，可能一直期望看到的术语是编码而不是密码。密码是一种常用的加密信息的方式，而编码是有限的。

在密码中，单个字符被另一个字符替代，或者固定长度的位串被不同的固定长度的位串替换。通信双方只需知道密钥。如果通信双方真的进行加密通信，就能传输任何双方想要的消息。加密存在着利与弊，要加密就要经受密码分析的考验。

密码应用于单个字符，而编码用码符号表示完整的单词或短语。图 3-4 给出了第二次世界大战中所用的简化版日本海军操作编码 JN-25。

对于每个单词或标点符号，都对应着一个五位数的码字。在消息发送时，发送的是码字而不是单词或符号。为了对消息进行编码，发送方会查找单词或符号，写下它们所对应

的 5 位数码字。然后，以此类推，继续查找后面单词或符号所对应的编码。最初发送方查找“From”，找到其对应的编码是 17434，所以发送方的密文以 17434 开始。

消息	编码
From	17434
Akagi	63717
To	83971
Truk	11131
STOP	**34058**
ETA	53764
6 PM	73104
STOP	**26733**
Require	29798
B	72135
N	54678
STOP	**61552**

图 3-4　日本海军操作编码 JN-25（简化版）

对于常用的单词或符号，码本有多个对应的编码。例如，在消息中 STOP 出现了三次。第一次它的编码为 34058。第二次它的编码为 26733。第三次它的编码为 61552。相同的单词和符号对应着不同的编码，这增加了密码破译者破解编码的难度[1]。

编码是非常具有吸引力的。因为没有计算机，人们也能手动进行编码和解码。编码的缺点是必须提前分发编码本。如果编码本被拦截，则编码就完全失去了保密性。

另外，常用的单词和符号能对应的编码数也是有限的。因此，对密码破译者而言，在流量中，截获大量编码本进行分析是破译的最直接方法。与编码相比，密码可以加密任何对象，如果密码密钥足够长，且采取适当的措施确保用户对保密非常重视，则密码是强有力的保护措施。归功于技术的飞速发展，在所有终端，甚至在移动电话上都能进行数据的高速处理，所以复杂的密码计算不再妨碍密码的广泛应用。

测试你的理解

5．a. 在编码中，编码符号代表什么？
　　b. 编码的优点是什么？
　　c. 编码有什么缺点？
6. 完成图 3-4 中消息的编码。

3.1.10　对称密钥加密

我们前面所讨论的密码是对称密钥加密密码，因为双方使用相同的密钥进行加密和解密。在使用对称密钥加密的双向通信中，双方仅使用单个密钥进行双向的加密和解密。

1　图 3-4 给出了 JN-25 编码的另一个特性。船（Akagi）将于下午 6 点抵达特鲁克海军基地。它需要在基地进行维修。它没有说明确切的服务，而是用 BN 指代。BN 是什么意思呢？ JN-25 编码没有说。实际上，BN 是编码内的编码。即使 JN-25 编码被完全破解，密码破译者也不知道 BN 是什么意思。完整的 JN-25 编码还有许多细微和玄妙之处。此外，在创建编码消息之后，JN-25 对消息又进行了加密，增加一层防护，以进一步挫败密码破译者的密码分析。

在对称密钥加密中，单个密钥被用于双向的加密和解密。

对称密钥加密非常快，产生的计算机处理负担很小。因此，即使个人计算机和手持设备也具备足够的处理能力，能使用对称密钥加密进行加密。由于处理负担小，所以为了保密，文件传输、即时消息和其他流行应用的加密都会使用对称密钥加密。事实上，几乎所有为了保密而进行的加密都使用对称密钥加密。

几乎所有为保密而进行的加密都使用对称密钥加密。

密钥长度

我们知道，只有保密密钥才能使保密成功。攻击者获得密钥的一种方法是用穷尽搜索，即尝试所有可能的密钥，直到攻击者找到正确的密钥。阻止穷尽搜索的最简单方法是将密钥设置得足够长，从而造成攻击者破解密钥所需时间过长，即使破解了密钥，在实际中也没用了。

如果密钥长度为 N 位，则存在 2^N 个可能的密钥。平均来说，密码破译者在成功破译密钥之前，需要尝试一半的密钥。因此，应该需要大约（$2^N / 2$）次尝试才能破解密钥。例如，如果密钥长度为 8 位，则只有 256 个可能的密钥（2^8=256）。平均而言，密码破译者要试 128 次才能找到正确的密钥。

如图 3-5 所示，密钥每增加一位就会使破解密钥所需的时间加倍。将密钥长度从 8 位增加到 9 位，则密码破译者要尝试 512 个密钥（2^9 =512）的一半，而不是 256 的一半。这将使破解密钥所需的时间加倍。

密钥长度/位	可能的密钥数
1	2
2	4
4	16
8	256
16	65 536
40	1 099 511 627 776
56	72 057 594 037 927 900
112	5 192 296 858 534 830 000 000 000 000 000
112	5.1923E+50
168	3.74144E+50
256	1.15792E+77
512	1.3408E+154

注意：密钥增加一位，就会使密码破解者破解密钥所需的时间加倍。图中的阴影部分，密钥长度大于 100 位，目前我们认为这种长度的密钥是强对称密钥。长度小于 100 位的密钥被认为是弱对称密钥。公钥/私钥对（本章后面讨论）必须足够长，且一定要是强密钥。如果私钥被破解，会造成灾难性的后果。此外私钥也不能频繁更改。公钥和私钥的长度必须至少为 512 到 1024 位。

图 3-5　密钥长度和穷尽搜索的时间

密钥每增加一位就会使破解密钥所需的时间加倍。

加倍密钥长度会成倍地增加密钥的数量。例如，将密钥长度从 8 位增加到 16 位，可能的密钥数会增加 256 倍（65 536/256= 256）。举个更令人印象深刻的例子，将密钥长度从 56 位增加到 112 位，则使穷尽搜索增加 72 亿次！

一些国家限制出口产品的对称密钥长度为 40 位，以便政府机构在需要时具备破解密钥的能力。目前，40 位密钥可以很快被破解。在英国，《调查权力法案》（RIPA）可用于强制个人出示自己的加密密钥。有一些人因没有交出密钥而被送进监狱[1]。

在 20 世纪 70 年代，对称密钥加密的强对称密钥（即需要非常耗时才能破解的密钥），只需约为 56 位。目前长度至少为 100 位的对称密钥才会被认为是强密钥。随着密码破译者的计算机处理能力不断增强，强加密会需要更长的对称密钥。

目前，长度大于等于 100 位的对称密钥被认为是强对称密钥。

测试你的理解

7．a. 为什么在对称密钥加密中使用对称一词？
   b. 当双方使用对称密钥加密通信时，一共使用了几个密钥？
   c. 在加密中，几乎总是将哪种加密密码用于保密？
8．a. 阻止密码破译者的穷尽搜索的最好方法是什么？
   b. 如果密钥长度是 43 位，如果将它扩展到 45 位，则通过穷尽搜索需要多长时间才能破解密钥？
   c. 如果扩展到 50 位呢？
   d. 如果密钥长度是 40 位，平均来说，需要尝试多少密钥才能破解呢？
   e. 目前，多长的对称加密密钥才会被认为是强密钥？

3.1.11 密码学中的人类问题

使用足够长的密钥和经过良好测试的密码，从技术角度来说，要破解用于保密的对称密钥加密是不可能的。但如果发送方或接收方未能保密密钥，则窃听者可以得到密钥，然后读取每个消息。

更广义地说，较差的通信纪律可以击败最强的密码和最长的密钥。举个例子，在第二次世界大战期间，日本海军在无须发送消息时，仍经常发送消息。这就给盟军密码学家提供了大量的、用于分析的信息。如果日本人的通信纪律良好，则密码破译者的工作难度会更大。此外，如本章前面所讲，日本海军的报告通常以标准语开始，长达几个句子。在破解日本码本时，这种“已知明文”的情况是非常宝贵的。另外有用的一个事实是，传输常常遵循常见的设置格式，例如报告船的速度和罗盘方位等。

通信合作伙伴甚至有一种虚假的安全感，因为他们认为已破解的加密方法仍在保护着

1 Chlis Williams, “Two Convicted for Refusal to Decrypt Data,” TheRegister.com, August 1l, 2009. http://www.theregister.co.uk/2009/08/11/ripa_iii_figures/.

自己。在第二次世界大战中，德国人有名为 Enigma 的加密机，Enigma 的技术非常先进。然而，波兰军方获得了机器的副本，并利用反向工程，揭开了 Enigma 的工作原理。在德国占领波兰后，波兰人把破译结果发给了英国，英国继续反向工程。最终，英国可以阅读大量的用 Enigma 加密的德语消息。过度自信的德国人在自我感觉良好的情况下，发送了大量的敏感信息。

注意一个事实，加密不是自动保护。只有公司必须安全执行组织过程，才能使用好密码技术。

测试你的理解

9. 为什么加密不是自动保护？

安全战略与技术

永远在线的 HTTPS

大多数人认为自己的网上冲浪是匿名的、安全的，并在必要时，需经过认证。但大多数链接并非如此。好好分析下面的三个简单案例，就能明白浏览行为存在的差异性。

案例 1：提供网上银行服务的银行普遍使用 HTTPS 来保护链接。在对用户进行安全认证之后，加密所有后续的银行业务。除银行之外，任何人都无法查看用户的操作。

案例 2：允许用户浏览网站的新闻或信息，这类信息网站提供的链接通常是匿名的，既不安全也未经认证。用户不必登录就能浏览网站内容，任何人都能查看你的操作。攻击者可以知道用户请求的网页及内容。

案例 3：社交网站等都要求先对用户进行认证，然后才能与网站内容（即帖子内容）进行交互。社交类网络提供安全认证。但是，会话的其余部分并不安全。攻击者可以拦截用于认证的 Cookie，然后模仿用户发布内容。这是一种类型的会话劫持。

Firesheep

2010 年 10 月，Eric Butler 发布了 Firefox 的扩展版，允许用户（劫持者）拦截用于认证其他用户的 Cookie[1]。扩展版使用包嗅探器来读取开放网络的数据包。然后，对在特定网站（Twitter、Facebook、Amazon.com 等）之间传输的 Cookie 进行定位。

然后，Firesheep 在边栏中显示使用这些 Cookie 的链接。之后，用户（劫持者）可以点击该图标并使用被劫持的账户。用户可以在任何被盗用的账户上发布内容。由于这些会话不使用 HTTPS，因此是不安全的，容易受到会话劫持攻击。在撰写本文时，大多数知名的社交网站都易受到这类会话劫持的攻击[2]。2009 年年底，Google 宣布所有 Gmail 流量都加密，并使用 HTTPS。

1　Jason Fitzpatrick, “Firesheep Sniffs Out Facebook and Other User Credentials on Wi-Fi Hotspots,” Lifehacker.com, October 25, 2010. http://lifehacker.com/5672313/.

2　Eric Butler, “Firesheep,” Codebutler.com, October 24, 2010. http://codebutler.com.

永远在线的 HTTPS

由于开放式无线网络无处不在，所以特别容易受到会话劫持攻击。劫持者可以坐在网吧或咖啡店，拦截许多不安全的会话。此外，在有线网络中，劫持者也能利用这种会话劫持漏洞。

有一些方法可以保护用户免受会话劫持攻击。其中一种方法是始终强制进行 HTTPS 安全链接。这将防止劫持者捕获用于识别用户的 Cookie。其缺点是用户必须手动输入“http://”到每个域名。即使用户尝试强制始终使用 HTTPS 安全链接，但有的网站不允许使用。

保护大多数用户的最简单方法是使用名为 HTTPS Everywhere 的 Firefox 组件[1]。HTTPS Everywhere 在用户通过身份验证后，甚至会加密整个会话。但是，此附加组件并不适用所有网站或网站中第三方的内容。

对业务的影响

用户经常会问，为什么网站不在所有时间都使用 HTTPS 呢？HTTPS 会一直保护用户及用户的内容。究其原因，其中最大的因素是成本。加密所有流量要求在线业务安装附加硬件，以处理增加的处理需求。这样做成本巨大，在线业务没有足够的资金来做出改变。

在撰写本文时，作者从著名的某社交网站得到了多个“忙”响应。该网站超载，不允许用户登录。Internet 原型可能没有资金或技术资源来实施 HTTPS。然而，随着用户对安全链接需求的日益增长，用户可能需要所有的链接都使用 HTTPS 安全链接。

大多数早期的讨论都侧重于使用 HTTPS 防止会话劫持这一优势。但安全 HTTPS 链接对雇主的影响还是要考虑的。雇主可以查看通过其网络发送的所有未加密流量。但是，如果员工访问使用 HTTPS 链接的站点，则监控不当的、非法和行为会变得更加困难。因此，全面考虑加密的优点与缺点是非常重要的。

3.2 对称密钥加密密码

使用对称密钥加密时，用户可以选择各种不同的密码。密码都能完成生成加密消息这一最终目标。然而，密码的功能不同，对强度、速度和计算的要求也有所不同。通信伙伴如果希望进行安全通信，则需要选择特定的对称密钥加密密码。经过良好测试的常用对称密钥加密密码只有几个，用户要在这几个密码中做出选择，这是非常重要的。下面分析经过良好测试的最常用密码 RC4、DES、3DES 和 AES。图 3-6 对这几种密码进行了比较。

3.2.1 RC4

目前常用的最弱密码是 RC4，通常发音为“ARK FOUR”。与其他的流行加密算法相比，RC4 有两个优点。

1 Seth Schoen, “HTTPS Everywhere,” EFF.org, September 16, 2010. https://www.eff.org/https-everywhere.

第一个优点：RC4 非常快，只使用少量的 RAM[1]。这意味着它是小型手持设备的理想选择，且对于最早的 802.11 无线接入点，RC4 也是可行的。因此，RC4 成了无线局域网的加密基础，声名狼藉的 WEP 加密系统就使用了 RC4。我们将在第 4 章中分析 RC4。

第二个优点：RC4 可以变长密钥。对于大多数密码而言，密钥长度越长越好。但 RC4 广泛使用的主要原因在于，其最短的可选密钥长度是 40 位。如本章前面所述，许多国家的国家出口限制一度将商业产品加密限定为 40 位。因此，40 位 RC4 成为 WEP 的标准密钥长度。

但非常不幸，RC4 是一种非常危险的密码。如果 RC4 没有被正确实现，则起到的保护作用非常小。弱的 RC4 实现是使 WEP 成为最弱无线局域网保护系统的主因。

	RC4	DES	3DES	AES
密钥长度（位）	大于或等于 40	56	112 或 168	128、192 或 256
密钥强度	很弱 40 位	弱	强	强
RAM 需求	少	中	中	多
处理需求	低	中	高	低
备注	可使用变长密钥	产生于 20 世纪 70 年代	用 2 个或 3 个密钥应用 3 次 DES	当今的黄金标准，未来的霸主

图 3-6　主要的对称密钥加密密码

测试你的理解

10．a．RC4 的两大优点是什么？

b. 为什么常常使用长度为 40 位的 RC4 密钥？

c．RC4 是强密钥吗？

3.2.2　数据加密标准（DES）

1977 年，美国国家标准局，即目前的美国国家标准与技术研究所（NIST）制定了数据加密标准（DES）。DES 迅速成为使用最广泛的对称密钥加密方法。

目前一直广泛使用 DES 的原因在于，首先是因为除了强有力的穷举搜索攻击之外，它几乎能对抗所有已有的攻击。其次是由于它应用范围广。还有就是硬件加速器支持 DES。

56 位密钥

DES 密钥长度是 56 位。它是一个 64 位的块，其中 56 位是密钥，其他 8 位是冗余位。如果用户知道其他 56 位，则可以计算出这 8 位冗余。利用冗余，双方能检测出错误的密钥。

目前，对于大多数业务交易和高度敏感的商业机密而言，56 位密钥长度太短[2]。然而，对于大多数普通消费应用来说，56 位足够了。正如下面所介绍的，为了实现工业级的安全，

1　分析一下为什么 RC4 要快一点？一个方法是注意 RC4 的实现代码只有约 50 行。相比之下，黄金标准的 AES 算法的代码约有 350 行（http://www.informit.com）。代码行越多则处理每个密钥时间就越长。

2　为了公平地对待 NIST，DES 设计使用期仅有十年左右，到 20 世纪 80 年代中期停止使用。在此期间，56 位的密钥是相当强的密钥。

密码学家将 DES 扩展到了 3DES。56 位的 DES 对 RAM 的需求量居中，处理速度也居中。

块加密

图 3-7 给出了 DES 块加密标准。DES 是一次加密消息的 64 位。加密的输入是密钥和 64 位的明文块。输出是 64 位的密文块[1]。

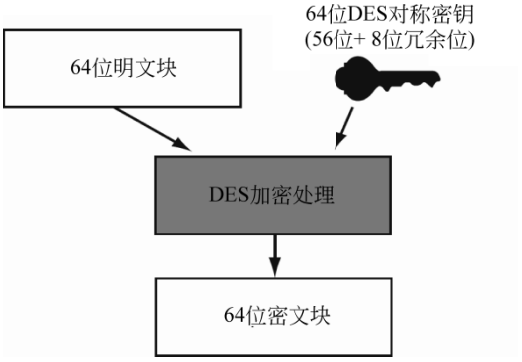


图 3-7　DES 块加密

测试你的理解

11．a．DES 密钥有多长？

b．DES 密钥是强密钥吗？

c．描述 DES 块加密。

3.2.3　三重 DES（3DES）

当企业需要比 DES 更强的加密时，可以转向使用三重 DES（3DES）。3DES 以简单的方式扩展了有效密钥的长度，但 3DES 的运行速度是让人痛苦的缓慢，对 RAM 的需求量也居中。

168 位 3DES 运算

为了增加密钥强度，168 位 3DES 算法仅简单地在每行应用 3 次 DES[2]。通常在应用 3 次密钥时，每次 DES 都用不同的密钥。因此，有效的密钥长度是 168 位（56 的 3 倍）。168 位密钥很强。

112 位 3DES

112 位 3DES 是 3DES 的变种，只使用两个密钥。在这种方法中，发送方的第三次运算是使用第一个密钥加密第二阶段的输出，即第三次使用的密钥与第一次所用的密钥相同。

1　在块加密中，完成加密的具体方式被称为模式。图 3-7 给出了具体的电子码本模式，这是最简单的 DES 块加密模式。更复杂的 DES 模式能提供更好的保护。

2　实际上，3DES 用第一个密钥加密明文块，用第二个密钥解密第一步的输出，然后用第三个密钥对第二个步骤的输出进行加密。加密、解密、再加密的这种模式是不是非常奇怪？算法之所以应用这种模式，原因在于双方共享一个 DES 密钥。使用 DES 密钥加密明文，然后使用相同的密钥解密第一步的输出，返回原始明文。那么，第三次加密相当于传统的单一 DES。这意味着 3DES 软件可以同时处理 3DES 和 DES。另外，只使用 DES 的接收方，通过单个密钥也能与 3DES 发送方通信，反之亦然。当然，仅使用单个密钥时，有效密钥长度只有 56 位。

这种 3DES 变种提供了 112[1]位加密，有效的密钥很强，且只需安全分发两个 DES 密钥。

反思 3DES

从安全角度来看，3DES 提供了强对称密钥加密。然而，从实际应用角度来看，DES 速度很慢，必须 3 次使用 DES，则速度更慢，因此处理成本很高。

测试你的理解

12．a．3DES 是如何工作的？
b．3DES 中，两个常用的有效密钥长度是多少？
c．3DES 的密钥长度能满足公司通信对安全的要求吗？
d．3DES 的缺点是什么？

3.2.4　高级加密标准（AES）

为了应对 DES 的弱密钥长度以及 3DES 的处理负担，在 2001 年，NIST 发布了高级加密标准（AES）。AES 在处理能力方面足够高效，对 RAM 需求也不高。因此，可用于各种设备，甚至用于蜂窝电话和个人数字助理（PDA）[2]。

AES 提供三种可选的密钥长度：128 位、192 位和 256 位。即使是 128 位密钥也是很强的。一秒钟内能破解 56 位 DES 的暴力破解系统将需要超过 100 万亿年的时间来破解 128 位的 AES。AES 较长的密钥长度足够强，即使对于必须保密多年的资料也是如此。目前，许多加密系统都支持 AES。在不久的将来，AES 应该在保密的加密领域占主导地位。

测试你的理解

13．a. 与 3DES 相比，AES 最大的优势是什么？
b．AES 提供的三种密钥长度都是多少？
c. 在小型移动设备上能使用哪些强对称密钥加密密码？
d. 在不久的将来，哪种对称密钥加密密码会占主导地位？

3.2.5　其他对称密钥加密密码

除了前面介绍的几种对称密钥加密密码之外，还有许多其他的对称密钥加密密码。它们是经历多年的海量的密码分析之后，幸存下来的仅有的少数密码。其中，最重要的有欧洲使用的 IDEA、韩国使用的 SEED、俄罗斯使用的 GOST 和日本使用的 Camellia。

但非常不幸的是，许多公司自豪地宣传“新的和专有的”加密密码。他们认为，由于

1　有些人称这种类型的加密为 128 位 DES。虽然 DES 密钥只有 56 位密钥强度，但它还有 8 位冗余位，所以长度是 64 位。

2　3DES 需要 48 轮加密处理。AES 只需要 9～13 轮加密处理，具体几轮取决于密钥长度。虽然 3DES 和 AES 的轮数并不完全相当，但是，经过这个简单比较，用户也可以了解为什么 AES 要比 3DES 快得多。

攻击者不知道密码的算法，所以不能破解加密。然而，安全专业人员将这种行为嘲讽为隐藏式安全（security through obscurity），因为其依赖于保密或者攻击者无法获取有关密码算法的信息，而不是依靠密码本身的鲁棒性。如果攻击者知道未测试密码的算法详细信息，则安全会遭到毁灭性打击。

隐藏式安全原则是隐藏潜在的漏洞，依靠保密来创造安全。

实际上，即使攻击者不知道详细的密码，也能快速破解使用专有算法加密的密文。生成无漏洞的加密密码是非常困难的，即使是密码学领域的专业人士也很难做到。这就是组织为何只能使用经过良好测试密码的原因。在计算机科学系的安全课程中，学生通常要学习如何设计新的加密密码。相比之下，信息系统的安全课程从来不让学生编写自己的加密算法。

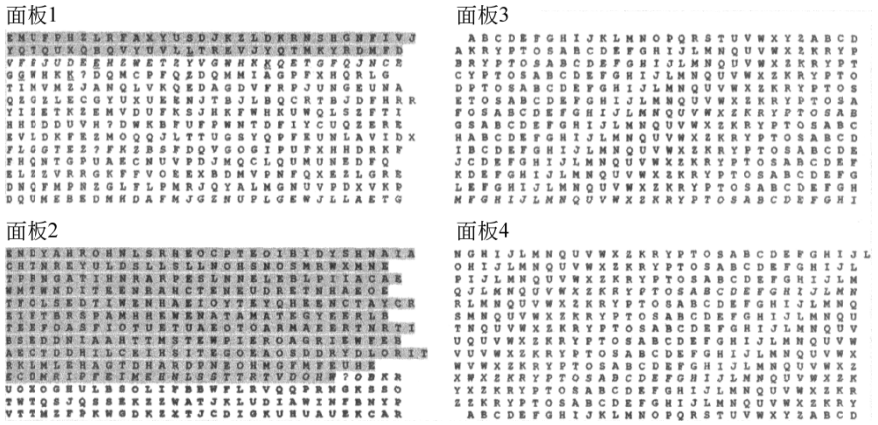
在计算机科学系的安全课程中，学生通常要学习如何设计新的加密密码。相比之下，信息系统的安全课程从来不要求学生编写自己的加密算法。

安全@工作

Kryptos

曾经研究过的最著名的加密信息刻在 Kryptos 雕塑上，该雕塑位于弗吉尼亚州兰利的中央情报局（CIA）总部。Kryptos 是希腊语，含义是“隐藏的”。Kryptos 是艺术家 Jim Sanborn 于 1990 年完成的作品[1]。

Kryptos 雕塑有四个面板。第 1 个面板和第 2 面板包含四个隐藏的消息。第 3 个面板和第 4 个面板结合起来形成一个 Vigenere 曲面。前两个消息隐藏在面板 1 中，后两个消息隐藏在面板 2 中，第一个和第三个消息是阴影部分。



Kryptos 面板

1 Steven Levy, “Mission Impossible: The Code Even the CIA Can’t Crack,” Wired.com, April 20, 2009. http://www.wired.com/science/discoveries/magazine/17-05/ff_kryptos#.

1999 年，Jim Gillogly 破解了前三条消息[1]。消息 1 使用关键字 palimpsest 和 kryptos 进行了解码。消息 2 使用关键字 abscissa 和 kryptos 进行了解码。消息 3 使用置换解码。以下是由 Gillogly 发布的解密消息，包括有意的拼写错误。

消息 1

在黑暗的世界里，在飘忽的阴影下，弥漫着幻影的气息。

Central Intelligence Agency Source: Getty/Danita Delimont
Source: http://www.gettyimages.com/detail/photo/seal-in-lobby-at-cia-headquarters-in-high-res-stock-photography/94450348

消息 2

完全看不见。这怎么可能？他们利用地球磁场。X 通过地下渠道，信息被收集并传送到未知的地点。X Langley 知道这一切吗？他们应该知道：它被埋在某个地方。X 谁知道确切的位置？只有 WW 知道。这是他最后的消息。X 三十八度五十七分六点五秒北七十七度八分四十四秒西。按行的 ID[2]。

消息 3

慢慢地，缓缓地，移动了留在门口下面通道的碎屑遗体。我用颤抖的双手在左上方开了个小洞。然后把洞稍微弄大一点，塞进一支蜡烛，向里四处张望。蜡烛的火苗随着墓穴里的热空气闪烁不定，不过很快房间里的一切就通过薄雾映在眼前。你能看到什么呢？

最后的消息仍然是个谜。然而，在 2010 年 11 月 20 日，Sanborn 公开了一条线索，说当正确解码时，字母 NYPVTT（粗体）将破译为 BERLIN。Sanborn 说：“我假定密码会在相当短的时间内被破解。”[3]在撰写本书时，第四条消息仍未被解码。

？OBKRUOXOGHULBSOLIFB
BWFLRVQQPRNGKSSOTWTQSJQ
SSEKZZWATJKLUDIAWINFB**NYP**
VTTMZFPKWGDKZXTJCDIGKUH
UAUEKCAR

1　John Markoff, “C.I.A.’s Artistic Enigma Yields All but Final Clue,” NYTimes.com, June 16, 1999. http://www.nytimes.com/library/tech/99/06/biztecWarticles/16code.html.

2　Sanborn 说他在雕塑中犯了错误。第二条消息的最后一部分应更正为“FOUR SECONDS WEST X LAYER TWO”，而不是错误版本“FOUR SECONDS WEST ID BY ROWS”。

3　John Schwartz, “Clues to Stubborn Secret in C.I.A.’s Backyard,” NW’imes.com, November 20, 2010. http://www.nytimes.com/2010/11/21/us/2 Icode.html.

测试你的理解

14．a. 据称，新的和专有的加密密码非常好，因为密码破译者不知道它们。对此观点进行讨论。

b. 什么是隐藏式安全，为什么隐藏式安全很差？

3.3 加密系统标准

3.3.1 加密系统

直到最近，保密一直是密码学的主要目标。密码学已经非常成熟。军事和商业组织都知道为了实现保密，加密是消息交换所需的保护方式。在实践中，是由密码系统提供加密保护，密码系统是用于保护对话的一组密码对策集。

加密系统是用于保护对话的一组密码对策集。

当双方使用密码系统进行通信时，需要使用特定的加密系统标准。这个标准规定了要用的保护以及提供保护的数学过程。流行的加密系统标准包括 SSL/TLS 和 IPSec。

3.3.2 初始握手阶段

当双方（设备或程序）通过加密系统标准通信时，需要经历三个握手阶段，如图 3-8 所示。

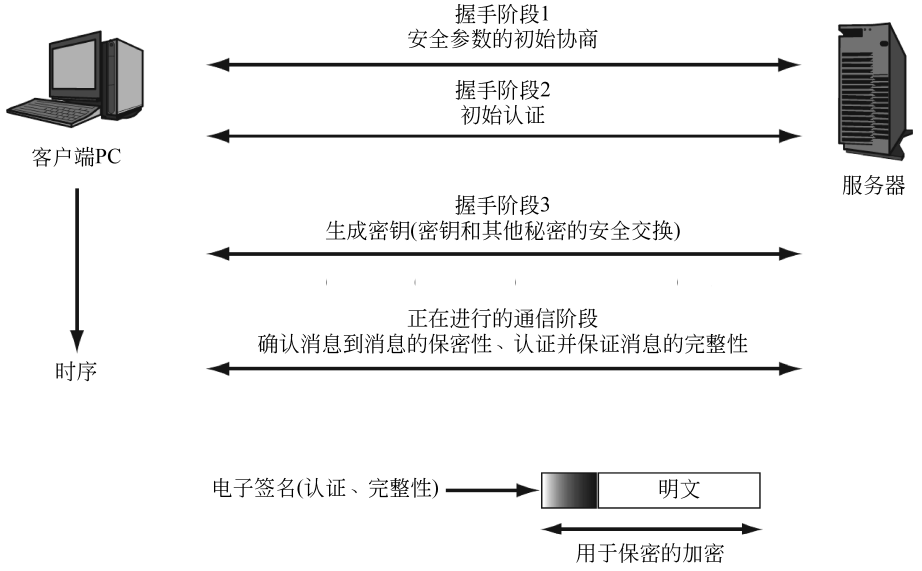


图 3-8 密码系统阶段

安全参数的初始协商

几乎所有的加密系统标准都为通信提供多种加密方法，而几乎所有的加密方法都有多个选项。因此，第一个握手阶段是协商通信中所用的加密方法和选项。在 SSL/TLS 中，特定的选项集称为密码套件。在双方开始 SSL/TLS 连接之前，必须协商通信会话所用的特定密码套件（其他加密系统标准的方法与选项的组合所用的名称会有所不同）。

密码套件是指特定密码系统标准的特定选项集。

初始认证

第二个握手阶段是初始认证。因为冒名顶替者也可以发送消息，所以双方在开始通信之前，必须进行相互认证。认证就是测试通信伙伴的身份。因为要在通信开始之前完成测试，所以将这种测试称为初始认证。如本节后面所讲，会对双方发送的每个消息进行后续的消息到消息的认证。

当双方彼此进行认证时，我们称之为相互认证。但有时，认证只由单方完成。例如，当用户登录服务器时，服务器会对用户进行身份认证，但用户不会对服务器进行身份认证。

在认证中，通信伙伴相互证明自己的身份。

请注意，初始认证发生在协商阶段之后。原因很简单，是因为只有在双方协商认证方法和选项之后，双方才能进行认证。

生成密钥

第三阶段是生成密钥。如前所述，为了保密密码，则需要密钥。稍后会介绍，身份认证还需要秘密。密钥和秘密都是长的位串，是通信双方必须保密的数据。在大多数情况下，必须安全地发送密钥和秘密。安全地发送密钥或秘密通常称为生成密钥。稍后我们会分析生成密钥的两种方法。

请注意，认证之后才生成密钥。这一点是必要的。因为除非先进行认证，否则第三方很容易窃取生成密钥的方法。

3.3.3　正在进行的通信

在双方完成相互认证及交换密钥之后，握手阶段结束，通信开始。在通信期间，双方要来回发送许多消息。双方通常以消息到消息为基础，在通信中应用一些加密保护。

- 首先，发送方向每个消息追加电子签名。接收方据此对每个消息进行认证。消息到消息的认证能阻止冒名顶替者将假消息插入到对话流中。
- 其次，所有良好的电子签名技术都提供消息完整性认证。这意味着如果攻击者能捕获消息，并更改消息，如更改客户的银行账户余额，则认证过程会拒绝被篡改的消息。
- 第三，为了保密，发送方要使用加密消息和电子签名的组合。

测试你的理解

15．a. 区分加密与加密系统。
b. 区分加密系统和加密系统标准。
c. 为什么第一个握手阶段要协商安全方法和选项？
d. 什么是冒名顶替者？
e. 什么是认证？
f. 什么是相互认证？
g. 为什么安全的密钥生成阶段是必需的？

16．a. 以消息到消息为基础，密码系统能提供三种什么样的保护？
b. 什么是电子签名？
c. 通常电子签名能提供两种什么样的保护？
d. 区分握手阶段与正在进行的通信。

3.4 协 商 阶 段

我们在前面非常简要地介绍了加密系统的 4 个阶段。目前，我们从协商阶段开始，详细地分析加密系统的每个阶段。

3.4.1 密码套件选项

如本章前面所讲，密码套件是特定密码系统标准（如 SSL / TLS）的特定安全方法与选项的集合。密码套件包括一组特定的方法和选项，用于初始认证、密钥交换以及发送消息的保密性、认证和完整性。

图 3-9 给出了 SSL/TLS 提供的可选密码套件的少量子集。在 3.10 节，我们将详细介绍流行的标准 SSL/TLS。图 3-9 按升序方式给出了这些子集的加密强度。在本章后面和其他章节，将学习图中所涉及的加密方法。

密码套件	密钥协商	数字签名方法	对称密钥加密方法	用于 HMAC 的散列方法	强度
NULL_WITH_NULL_NULL	无	无	无	无	无
RSA_EXPORT_WITH_ RC4_40_MD5	RSA 出口强度（40 位）	RSA 出口强度（40 位）	RC4 (40-bit key)	MD5	弱
RSA_WITH_DES_CBC_ SHA	RSA	RSA	DES_CBC	SHA-1	强但还不是很强
DH_DSS_WITH_3DES_ EDE_CBC_SHA	Diffie-Hellman	数字签名标准	3DES_ EDE_CBC	SHA-1	强
RSA_WITH_AES_256_ CBC_SHA256	RSA	RSA	AES 256 bits	SHA-256	非常强

图 3-9　所选的 SSL/TLS 密码套件

3.4.2　密码套件策略

在加密系统标准中，最弱的密码套件能提供的保护很少，或者根本不能提供保护。例如，在图 3-9 中，第一行的密码套件完全不提供安全性。第二行仅使用出口级的加密。因此，第二行与第一行相比，虽然略强一些，但保护性仍然很弱。最后一行的密码套件安全性非常强。

由于 SSL/TLS 密码套件的安全强度差异很大，为了选择适合的密码套件，公司必须制定基于风险的策略，所选定的密码套件强度要与应用风险相匹配。IPSec 加密系统标准（本章稍后讨论）可以集中设置安全方法和选项的策略，并强制所有通信伙伴都应用所设置的策略。

测试你的理解

17．a. 在 SSL/TLS 中，什么是密码套件？

b. 为什么公司需要制定策略，来定义公司合作伙伴之间所用的特定应用的安全方法和选项？

3.5　初始认证阶段

在建立加密系统对话中，一旦安全协商阶段完成，下一个握手阶段就是认证。目前有几种初始认证的方法。我们只分析基于服务器密码认证的 MS-CHAP。

3.5.1　认证术语

在身份认证中，试图证明自己身份的一方是请求者，而另一方是验证者。请求者向验证者发送凭证（身份证明）（如图 3-10 所示）。在相互认证中，双方会轮流成为请求者和验证者。

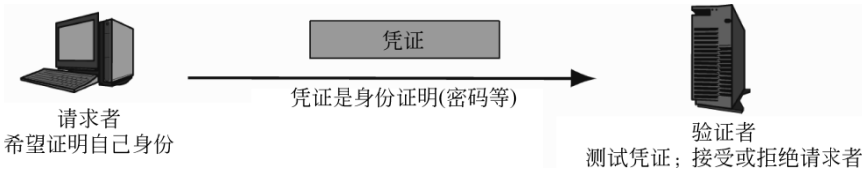


图 3-10　认证：请求者、验证者和凭证

测试你的理解

18．a. 在认证中，区分请求者和验证者。

b. 什么是凭证？

c. 在双方的相互认证中，有多少请求者和验证者？请说明。