过渡中的密码学

亚伯拉罕 LEMPEL

Technton- Israel institute of Technology 电子工程学系，以色列哈法

本调查的重点是公开密钥密码系统的新概念，最近提出的实现方案，以及与密码复杂性有关的问题。此外，还简要概述了经典密码学，当今密码学的基本原则，以及现在官方的数据加密标准的简短描述。

*关键字和短语:*密码学，密码，加密，解密，密码系统，密码复杂性，公钥密码系统

*CR 分类:*3.15,3.71,5 14,5 30

前言

这项工作旨在向读者传达公共密码学目前所处的过渡阶段和不断发展的技术状态。这种过渡是多方面的:在相关范围内，它已经从处理军事和外交通信的政府垄断演变为一般商业的主要关注，特别是银行业，以及最近的广大公众。它的技术已经从纸笔和各种机械设备扩展到大型、高速的电子计算机。它的安全重点也从统计的不确定性转变为计算的复杂性。最后，但并非最不重要的是，在概念上它已经从传统的 pri- vat -key 方案发展到公钥密码系统——提供即时隐私和双向认证的术语。

这一最新转变也反映了密码学“艺术”的快速发展状态。由于它最近被学术界作为一个合法的学习和研究领域，公共密码学的支持者正在努力将其从一门艺术转变为一门科学，即用可靠的措施和标准取代直觉，依靠证明而不是认证。

本综述的主要重点是公钥密码学的新概念-术语和最近提出的实施方案(第 3 节)。本主题之前是按时间顺序的介绍，简要概述了经典密码学及其一些主要方案(第 1 节)，以及当今密码学的基本原则，简要描述了现在正式的数据加密标准(第 2 节)。第 4 节处理了有问题的密码复杂性概念;这个概念和 np -完备性的复杂性理论概念之间的差异通过一个容易被破解的 np -完备密码的例子来证明。还需要注意的是应用脱离上下文的复杂性度量的危险，以及需要一些基础研究而不是更多实现的扩散。

这项工作的初步版本，其中

这项工作是作者在马萨诸塞州萨德伯里的斯佩里研究中心休假期间进行的。

内容

---

port [LEMP78]，还包括密码学的注释参考书目。这个参考书目，由 Diffie 和 Hellman 编译，已经在其他地方出版[DIFF79]。

我们要指出的是，文中对“已知的”或“现有的”方法和方案的所有引用都是针对未分类和非专有知识的。在公钥系统领域，我们已经尽了最大努力涵盖 1978 年 8 月以来所有已知的方案;考虑到这个主题的快速发展状态，我们可能遗漏了一些内容。

密码学是一门设计和破解保密系统的艺术，或者可能是一门科学。它的设计或合成部分通常被称为密码学，而破译或分析部分被称为密码分析。作为一门艺术，密码学的历史可以追溯到有记载的历史早期;作为一门准科学，它正处于寻找适当的安全性标准和复杂性措施的早期阶段，仍需依靠人/计算机年的努力，而不是严格的证明。

最完整的密码学历史，涵盖了从古埃及法老时代一直到第二次世界大战的时期，记录在 1967 年 D.卡恩的书中，*密码破译者，秘密写作的故事*[KAHN67]。虽然它更多关注的是密码学的影响，而不是它的技术发展，但它为这个主题提供了一个很好的介绍。从 1978 年夏天的角度来看，卡恩的书所涵盖的许多世纪可以被统称为密码学的经典时代。尽管简单的凯撒密码(归功于朱利叶斯凯撒)和第二次世界大战中使用的复杂转子机器之间存在着巨大的复杂性差距，但它们的共同点在于它们早于电子计算机的出现。

随着电子计算机的引入而变得可用的计算能力开启了现代密码学时代;此后这种能力的急剧增长及其对社会的普遍影响，大大拓宽了密码学的相关范围。一个主要涉及安全军事和外交通信的建立和破坏的领域，直到不到十年前还被认为是在政府的严格控制下，如果不是完全由政府垄断的话，已经成为一般商业，特别是银行业，以及最近广大公众关注的主要问题。在不断增长的计算机数据库和电子资金转移(EFT)时代，人们不能高估加密方案的重要性，它提供足够的保护，防止未经授权的，通常是远程的，对存储数据的访问，使未经授权的监听者无法通过公开访问的通信链路理解数据，并纳入一个数字签名，可以作为可靠的双向认证。这些令人生畏的目标是为了满足真正的市场需求而设立的，数据加密标准{DES] [NBS77]部分地回答了这一问题，它是 IBM 路西法的简化和修改版本

DES 的主要缺点，与目前已知的任何其他正在使用的方案一样，是它需要在每一对通信者之间预先建立一个私钥，因此无助于缓解日益复杂的密钥管理问题。

1976 年，斯坦福大学的 Diffie 和 Hellman [DIFF76]和 Merlde [MERK78a]在这个方向上迈出了重要的一步，他们引入了“公钥分发”和“陷阱门单向函数”的概念，用于“公钥密码系统”，它不需要预先的密钥通道，并且允许不可伪造的数字签名。这些想法——起初看起来很聪明，但不太实用——得到了发展势头，很快就被麻省理工学院的 Rivest、Shamir 和 Adleman [RIvE78a]提出了一个易于实现的方案。Merkle 和 Hellman [MERK78b]和 McEliece [McEL78]提出了没有数字签名特性的其他实现方法。

这些新加密的影响

争议{BRAN76, DIFF77, MORR77, KOLA77a}，其中涉及的人担心中等大小的密钥(56 位)和 NBS 不愿意透露选择指定替代或“S”框背后的设计考虑，表明一个故意内置的弱点，使加密的数据可被国家安全局(NSA)读取，但没有其他人。NBS 在 1976 年夏天举办的两次研讨会并没有对解决争议起到多大帮助。一名被指控为 NSA 雇员的人试图阻止在公开科学会议上展示一些新的加密方案[SHAP77]，这一尴尬的尝试被公开，以及 DES 争议的持续发酵，促使参议院情报特别委员会对 NSA 参与的指控进行调查。在 1978 年 4 月的一份报告[SSCI78]的非机密摘要中，委员会得出结论，NSA 没有对与他们的公开加密日志研究有关的个人或组织施加压力。它进一步得出结论，NSA 间接地帮助 IBM 开发 S 盒，使 IBM 相信减小密钥大小就足够了，并且没有以任何方式篡改 DES m 的设计。考虑到对国家安全的影响，委员会建议 NSA 和国家科学基金会(NSF)制定安排，使 NSA 成为 NSF 拨款提案同行评审过程的一部分，并减少围绕公共密码学研究基金授予的模糊性。(关于公共密码学研究的法律地位的后续讨论见 SUGA78。)

方案并没有丢失任何感兴趣的各方:各种安全机构显然正在检查它们[KOLA78];工业界正在探索实施方案;而同样重要的是，作为这一切起源的学术界，已经将密码学作为一个合法的研究领域，并且是一个非常活跃的研究领域。

值得赞扬的是，应该指出的是，新的加密方案尚未被证明构成“一种需要数百万年才能破解的新型密码”，正如 1977 年 8 月《*科学美国人*》[GARD77]上一篇文章的标题所宣称的那样。同月，《*科学*》杂志[KOLA77b]上的一篇文章标题为“密码学:在革命的边缘?”，这个标题更为合适;从这个标题中去掉问号的工作还有待完成。问题在于，显然缺乏证据证明这些新方案中的任何一个确实像它们看起来那样难以破解。它们的优势在于用目前已知的方法来解决某些数学问题的计算复杂性。考虑到这种加密方案的深远影响，问题是底层数学是否能够承受一个高度积极的数学社区的共同努力，或者能够承受多久。另一方面，同样的动机可能会导致新方案的发明或建立适当的密码复杂性度量，这将更真实地与加密安全相关，从而为更严格的不可破解性断言铺平道路。

1.古典密码术

经典密码学的两大工具*是代码和密码*。两者都是为了将明文*消息*转换为隐藏文本*密码而设计的*。代码是一个固定的预先确定的字典，它将码字分配给最可能的消息，因此它的主要用途是用于那些可以由预先选择的消息组成的文本。代码的固定性质也削弱了它所提供的安全性，因此代码通常与密码结合使用以产生加密代码。

密码是一种通用的方案

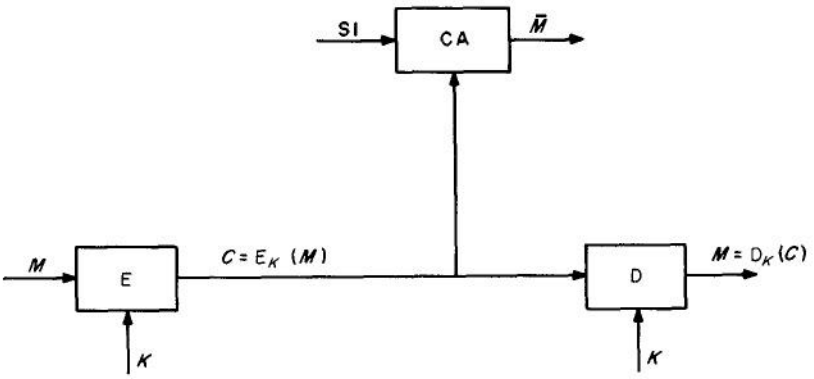


图 1 所　　密码系统的一般结构。

能够将任何明文转换为*密文的一组转换*。在任何给定时间应用的特定转换由当时使用的*密钥*控制。使用中的密钥被假定为(合法的)*发送方*和*接收*方都知道，但至少是先验的，目的是破坏系统的*密码分析*者不知道。

根据文献和实践的趋势，我们在这里只处理基于密码的*密码系统*，其一般结构如图 1 所示。E、D 和 CA 块分别表示*加密*、*解密*和密码分析方案。给定消息 M 和密钥 K，加密方案产生密文 C -~ E~(M)，其中这个函数符号(而不是 E(K, M))意味着，通常情况下，K 是一个加密/解密参数，对于相当数量的消息保持固定。给定 C 和相同的 K，解密方案可以很容易地生成原始密文

$$M = D_K(C).$$

密码分析师被认为对 E 和 D 方案有充分的了解，可以访问 C 和各种侧面信息 SI，例如语言统计、正在进行的通信的一般上下文和一些明文;他的任务是在给定 E、D、C 和 SI，而不是 K 的情况下，得出 M 的最佳估计 M。尽管在某些情况下，密码分析家可能在没有先找到 K 的情况下得出正确的 M，但破解密码系统通常意味着找到一个能够在给定“足够”SI 的情况下产生 K 的方案。

因此，给定的加密方案 E 所提供的保护通常是根据密码分析者在试图确定在 E 下可接受的潜在密钥中哪一个实际上正在使用时所面临的不确定性来衡量的。这种方案 E 的低效率是根据底层语言的统计冗余来衡量的，它可以扩展到包括 SI 的其他方面。

信息论的出现使得对不确定性和冗余等概念的定量处理成为可能。信息论的数学基础及其在经典密码系统中的应用是在香农的两部巨著中建立起来的[SHAN48, SHAN49]，他在 30 年前的结论和建议甚至在最近 nbs 批准的方案设计中也起到了指导作用。香农工作的细节不在本调查的范围之内。他的一些主要结论可以概括如下。

密码分析之所以成为可能，是因为冗余;因此，在加密之前对数据进行压缩，可以增强安全性。每个密码系统都可以关联一个正整数 No，这样，在最坏的情况下，一个长度为 No 的密码唯一地决定了所使用的密钥。香农称这个参数*为系统的唯一距离*，他已经证明，它可以用密钥的先验不确定性与语言的每个字符冗余的比率来近似表示。因此，一个唯一距离为 No 的密码系统，如果用于加密 No 或更多字符，则会呈现不安全。

虽然信息论模型的基本假设之一是密码分析者拥有无限的计算资源，但香农充分意识到所谓密码系统的*工作因子*的实际重要性，即密码分析的复杂性与解密的复杂性之比。从某种意义上说，它是现代方法成长的种子，这种方法将安全性建立在密码分析的复杂性而不是模棱两可的基础上。香农通过他所谓的“混淆和扩散”来增加功因子的建议在业内得到了很好的重视，它是许多当代系统的基石，包括 DES。其主要原则将在第 2 节中讨论。在本节的最后，我们对主要的经典密码进行了简短的回顾。在即将到来的所有示例中，我们都使用 26 个字母的英文字母表，其数字对应为 A ~-~ 0, B (-~ 1, C ~-, 2, …, z ~-。25，当涉及到算术运算时。

1.1 凯撒密码

最初，凯撒密码由一个密钥组成，对应的唯一变换是

$$\mathbf{E}: M \rightarrow M + \quad (\mathrm{mod} 26),$$

$$M = 0, 1, \ldots, 25.$$

后来被推广为指有 26 个密钥的密码，0 ~ K __ 25，对应字母表的 26 个循环移位:

EK:M + K (mod 26)。

密钥的数量如此之少，详尽的密码分析使得这个密码完全不安全。

1.2 简单替换

简单替换是一种密码，它允许使用英文字母上的任何排列作为逐个字母的替换密钥，因此包括凯撒密码作为一种非常特殊的情况。例如，

中的 F g hi I J . kl . m . nop . QRS TUVW X Y Z
THUV c wb p . dz
G j xqal ymrke

是将明文 MESSAGE 转换为密文 OIQQTWI 的密钥。数量这里有 26 把钥匙!> 4.1026 足以消除穷举密码分析的可行性。然而，对英语语言的统计分析揭示了相当高的冗余，每个字母约 3.2 位，导致该密码在统一密钥分布下的唯一距离为 No = 28 个字母。无论这个理论推导出的数字有多小，它都比 Friedman [FRIE67]所提到的实际断点 25 还要大。简单替代密码的密码分析速度很快，因为它保留了典型英语文本中高度不均匀的字母频率分布。为了更详细地描述这种密码分析技术以及随后描述的密码，读者可以参考 Sinkov [$ISK68]。

1.3 多字母密码

多字母密码使用 n 个替换字母的周期序列，通过平滑语言统计，显著提高了安全性。(同一个密文字母可能在一个地方代表一个频繁出现的明文字母，而在另一个地方代表一个不频繁出现的字母。)同时，可能的有效密钥数从 26 个增加了!到(26!)n。

多字母替换的一个非常流行的简化版本是 *Vigendre* 密码，它采用凯撒式替换的周期性序列作为密钥，通常由一些有意义的关键短语定义，使其易于记忆。例如，关键短语 BEST MAN 定义了将周期性重复的整数序列 1,4,18,19,12,0,13 添加(mod 26)到表示明文的整数序列的转换。周期为 n 的 Vigen~re 密码中的密钥数为 26”，与同一周期的一般多字母密码中可用的密钥数相比，这只是一小部分。然而，当 n——)~，或者在实际应用中，当周期长度与消息相同时

长度，一个人获得所谓的“一次性 pad”的*维尔南*密码，它提供

明显完美的安全性[SHAN49]。华盛顿和莫斯科之间的“热线”使用的是一次性密码本，据信[GARD77]是苏联特工被允许加密其信息的唯一方法。

一次性便笺簿的预先准备和分发过程中涉及的巨大密钥管理问题，以及它们对密钥符号的最低效利用，使得它们只适用于高度敏感的通信。

1.4 换位

换位是一种*分组*密码，它对长度为 n 的单词(块)进行操作，使用 n!位置排列将单词的字母进行调换。要加密，首先要将明文流分解成 n 个字母的单词，然后将使用的特定密钥规定的转置顺序应用于每个单词。例如，如果 n = 5，使用的密钥是

12345
43152

单词的第一个字母变成第四个，第二个字母变成第三个，以此类推;明文 TOP SECRET CIPHER 被解析成 TOPSE CRETC CIPHER 后，再转换成密文

PE OTSECRCTH RPIE

这种密码也保留了单个字母的频率分布，但与简单替换不同的是，它破坏了语言的双图、三图和高阶统计量，这在某种意义上[HELL77]使其成为比简单替换更好的自然语言密码。

1.5 Product cipher

虽然对于实际可行的 n 值，上述每个密码本身都相当弱，但当这些密码被适当地组合并迭代足够次数时，它们可能提供非常高的安全性。当由密码 T 加密的明文被密码 S 重新加密时，最终的密文可以看作是由*乘积密码* *R* =加密的结果

ST. Shannon [SHAN49]充分认识到产品密码在工作因子(以及安全性)增益方面的广泛潜力，并从此成为当今加密系统所基于的主要原则。该原理的最终用途是由于这样一个事实，即作为低成本构建块的简单替换和换位的非常基本的方案可以有效地组合成非常复杂的密码，如 DES。

2.基本原则目前-天密码

当今几乎所有密码的安全性都是基于破解它们所需的工作量，而不是统计上的不确定性。假设密码分析人员有足够的侧信息来确定唯一的密钥，如果他能负担得起详尽的搜索。例如，在香农模型下，这意味着密码学家拥有的密文数量超过了唯一距离。拥有几乎无限的密文现在被认为[DIFF76]是密码分析师可以访问的最低级别的侧信息。

在已知的密文下，系统所面临的威胁被称为*纯密文*攻击，任何针对它的方案都是完全无用的。一种更现实的方法是假设密码分析者拥有相当数量的对应明文和密文。在这种情况下，系统会受到*已知明文*攻击，这是一个更可怕的威胁。除了“物理获取”密钥之外，最终的威胁是*选择明文*攻击，即假定密码分析者能够获得他选择的相应明文和密文。在所有这些攻击中，都假定密码学家对被攻击系统的结构有充分的了解。

目前最合适的方法是根据密码抵御选定的明文攻击的能力来评估密码。根据 Hellman 等人的研究[HELL76]， NBS 在对 DES 的测试中应用了不太强大的已知明文攻击

认证仍然是一个启发式的过程，而不是一个严格的过程，只有更保守的密码强度估计才应该依赖。

在本节的其余部分中，我们将回顾当前使用的私钥密码系统设法应对上述威胁的主要原理和实现技术。最新的公钥概念和建议的实现将在第 3 节中描述。由于大多数当前数据都是以二进制形式存储、传输和处理的，因此我们将注意力限制在二进制{0,1}字母表上的密码上，而不会失去一般性。因此明文和密文都是以位串的形式呈现的。当对明文字符串进行逐位加密时，相应的密码称为*流*密码;否则，明文字符串首先被分解成单词，然后逐字加密。最常见的是，由于同步和缓冲的考虑，单词的长度是固定的 n，在这种情况下，相应的方案被称为*分组*密码。

2.1 流密码

当今的流密码是 Vigen~re 密码的精炼现代版本。它不使用相对较短、易于记忆的密钥短语，而是使用一个密钥串生成器，通常是一个反馈移位寄存器，其可控的初始状态和反馈布线充当紧凑的加密密钥。密码分析人员被假定知道密钥串生成器的固定特征，因此一旦他知道了压缩密钥，就可以生成整个密钥串。在许多情况下，密钥串的足够长的子串唯一地决定了密钥串的其余部分，这使得流密码容易受到已知明文攻击，除非特别注意使密钥串位成为其前任的非常复杂的函数。这就排除了任何线性生成的密钥串，包括由低成本 n 级移位寄存器生成的最吸引人的最大长度(2" - 1)伪随机序列。已知明文的 2n 长片段足以破解这样的密码[GEFF73]。

设计 se-的主要指导方针

治愈流(以及~s 块)密码是*扩散*和*混淆的香农原理*。扩散要求尽可能长时间地在子串上传播或“分散”密钥串变量之间的相关性和依赖性，从而最大化密码分析所需的明文长度。混淆要求使相关变量之间的功能依赖关系尽可能复杂，从而最大限度地延长密码分析所需的时间。最近已经发表了几种根据该原理生成密钥字符串的方案[GEFF73, PERL76, PLES77]。其中最新的是 Vera Pless [PLES77]，这是一个有趣的 J-K 触发器网络的应用。

2.2 块密码(Block cipher)

当今典型分组密码的基本结构是迭代积密码，其主要组成部分是换位和简单替换[FEIs73]。典型的分组长度从 32 到 128 不等，通常为 8 的倍数。DES 块长度为 64。密钥大小通常等于块长度;当较短时，如 DES 的 56 位密钥，它被人为地扩展以适应整个块长度。

系统的换位组件很容易以所谓的 P 盒(P 代表置换)的形式实现全块长度，如图 2 中 n ffi 16 所示。然而，在整个块长度字符上实现简单替换的全部功能是不可行的。一个长度为 n 的块可以代表 2 个“不同字符，允许 2 个”中的任何一个!不同的替换接线。因此，加密方案的替换阶段在块的小段(通常为 4 位)上并行执行。

这种 4 位替换或“S”盒的内部结构如图 3 所示。它由三个阶段组成:第一个阶段是二进制到十进制转换器;第二阶段是对小数进行排列的 P 盒;第三个是十进制到二进制的转换器。

一个典型的 n = 16 的乘积密码，由 P 和 S 盒子交替层组成，是

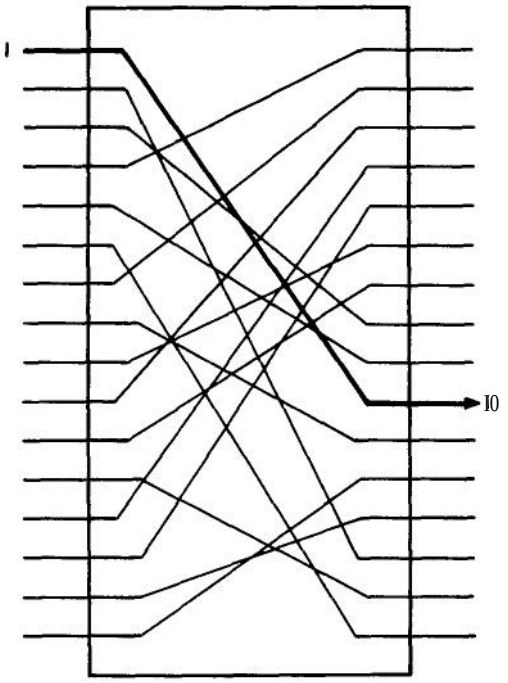


图 2。一个 P 盒，用于实现块位的特定排列。

如图 4 所示。P 盒通常是固定的或不带钥匙的，它们唯一的功能是提供扩散。S 盒是有键的，用来执行非线性代换，从而产生混淆。图 4 示例中的 16 位密钥将使每个 S 盒由两个比特进行键控，从而允许每个 S 盒执行四种不同的键相关替换。IBM 的路西法是

是一种 128 位分组密码，按照这些通用准则设计[SMIT71, FEIS73]。它在所有层中使用固定的 P 盒，并且为了保证高度混淆，每个 S 盒由单个密钥位控制，该密钥位在两个精心预选的非线性替换之间进行选择。(一个完全通用的 S 盒可能会意外地以一种可能危及系统的方式被键入。)

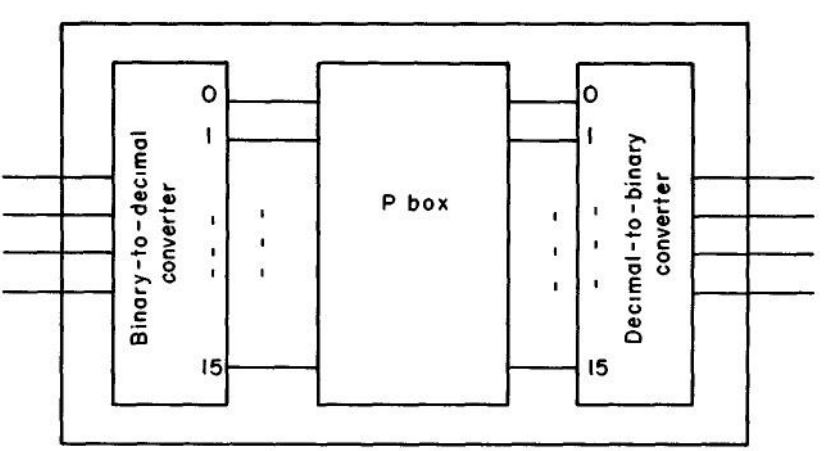
2.3 数据加密标准

DES [NBST7]是官方的(1977 年 1 月通过的)国家标准局(NBS)方案，由联邦部门和机构以及其他部门使用，用于计算机数据的加密保护。它是 ibm 开发的路西法的简化版，具有 64 位数据块和 56 位密钥。为了使密钥达到完整的块大小，通过选择每个 8 位字节的最后一位，人为地将其扩展为获得 64 位的“KEY”，以确保该 KEY 字节的奇偶校验，从而提供一定程度的错误检测。

要加密，明文块首先要经过初始排列 IP，然后经过复杂的依赖密钥的计算，包括 16 次功能相同的迭代，最后通过将第 16 次迭代的输出置于初始排列的逆 IP -I 来获得密文块。

密钥依赖计算的第 i 次迭代的输入为 *L，_~，R，-1* 和 K~，1 _ i ___ 16，其中 L0 和 R0 分别为，respect -

FIGURW 3。一个特定 16 的 4 位 S 盒实现。字符替换。



C~ 调查，签 11日，12 月 4 日，1979

实际上，ip 排列明文块 K 的左右 32 位部分是 i 和 KEY 的 48 位函数，K, KS(i, KEY)和

$$L_i = R_{i-1}, \qquad R_i = L_i \oplus f(R_{i-1}, K_i)$$

其中@表示加法 mod 2，函数 f5 是方案的核心。

是一个非线性的，多对一的替换。得到 f 的 32 位输出如下所示。首先，将 32 位的 R-展开为 48 位的 E(R-);接下来，K 和 E(r -)被逐位相加，取模 2，它们的和 Q 被划分为 Q-0,QQa，其中每个 Q, 1j <8，是 6 位长;然后，每个，被送入一个固定的非线性 6 输入 4 输出替换盒 S. f. nallv, 8 个 S，盒的组合 32 位输出被送入一个输出为 f 的 P 盒。关于 IP P, KS, E, S，盒和 P 盒的完整细节，请参阅 NBST7

为了解密，将密文块置于完全相同的过程中，以相反的顺序应用 K，即从 Kis 开始以 K 结束。这样，第一个解密步骤 IP 将解密 IP -1 的最后一个加密步骤 L，， R。

成对将按照相反的顺序再生

$$R_{i-1} = l \qquad L_{i-1} = R_i \oplus f(L_i, K_i)$$

以及最后的解密步骤。iP -1 将撤销第一个加密步骤 iP 并显示原始明文块。

正如引言中提到的，DES 的采用激起了一种控制。这一争议有待解决。评论家提出的主要意见和建议如下 DIFF77 MORR771:

1)一台一天的穷尽搜索机在 20 世纪 80 年代是可行的。(1976 年 8 月的 NBS 车间估计，这种机器最早的交付日期是 1990 年。)

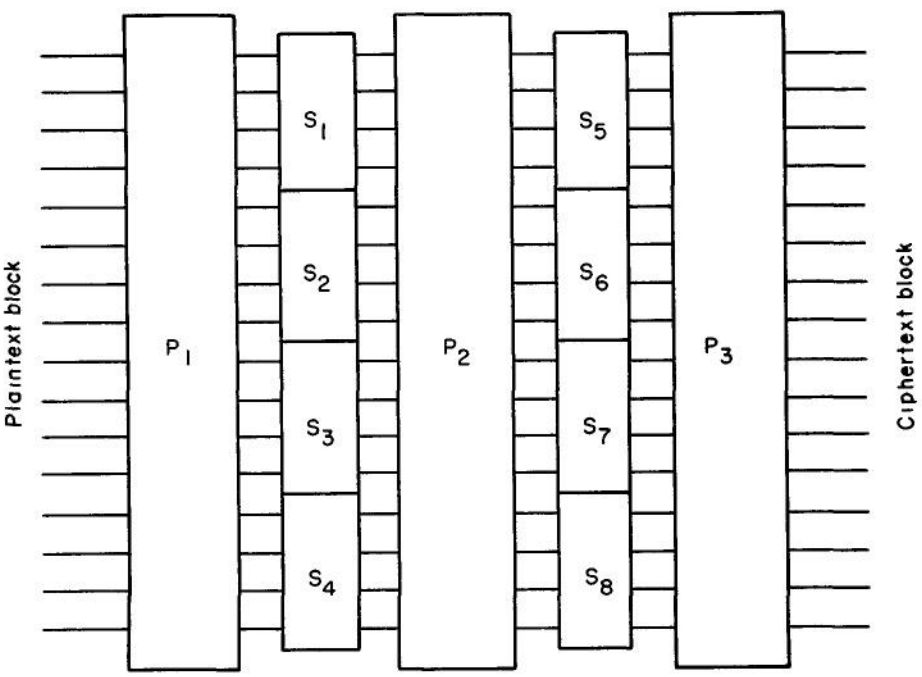
Kev 的大小应该增加到至少 64 位，最好是 128 位。

迭代次数应该翻倍

应该使用公开设计的 S 盒

5)不应采用建议的 DES，但如果采用，则应使用多重加密

FIGURE 4 A product cipher for blocks of length 16 with fixed P boxes and keyed S boxes.



这些激烈的争论已经过去三年了。DES现已正式公布，解决争议的是时间，而不是理性。无论它的其他目的是什么，这场争议无疑是激发人们对密码学重新产生兴趣和近两年取得新成果的一个因素。

3.公钥密码体制

公钥密码系统的概念是在1976年由Diffie和Hellman [DIFF76]提出的，他们设想了一个私有通信系统，该系统采用一个公共目录，每个订阅者在其中放置一个过程E，供其他订阅者用于向他发送的消息的加密，同时对其相应的解密过程D保密。为了使这样一个系统可行，必须有一个简单的方法，每个订阅者可以通过该方法生成自己的E和D过程。而且，将这些过程分别视为消息集和密码集{M}和{C}上的运算符，这些过程必须具有以下属性:

i)如果C -= E(M)，则对于每个M, M = D(C)或D(E(M)) ffi M。

ii) E和D都是快速且易于应用的。

iii)公开披露E不会损害D，也就是说，从E推导D在计算上是难以处理的。

这样一个系统的存在将使以前从未见过面或通信的订户之间能够即时安全通信。例如，订阅者A要向订阅者B发送私信M，他在B下的目录中查找EB，并公开传输C = EB(M)。通过iii)，只有B可以通过将他的秘密DB应用于C来解密C。

为了实现数字签名特性，Diffie和Hellman提出使用具有以下附加性质的E-D对:

iv) D可以应用于每个M，如果S = D(M)，则M = E(S)或E(D(M)) ffi M对于每个M。

当iv)成立时，订阅者A可以“签名”他的消息发送给订阅者B，首先计算其消息相关签名S ffi DA(M)，然后计算密码C ffi EB(S)。现在，只有B可以通过计算DB(C) ffi DB(EB(S)) ffi S从C中恢复S，当他计算EA(S) ffi EA(DA(M)) = M时，B可以确定M来自A，因为没有其他人可以应用A的秘密DA来计算S = DA(M)。

如上所述的数字签名起到了双向认证的作用。除了*消息*依赖之外，S还依赖于*签名者*。虽然B可以确定收到的消息确实来自A，但通过对他的消息进行签名，A可以确定没有人能够将他没有发送的消息归因于他。S的双重依赖也可以防止签名被附加到虚假的消息上。

虽然在他们的优秀文章[DIFF76]中对这些优雅的概念进行了完整的描述，但Diffie和Hellman没有给出公钥密码系统的实际实现。然而，他们指出，任何这样的实现方式都会导致计算上的难题，比如所谓的单向函数的反转。自[RwE78a, MERK78b, McEL78]以来发表的各种实现都是基于这样的问题。*如果函数f可逆且易于计算，则称函数f是单向*的;但对于f定义域内的几乎所有x，对x求解y ffi *f(x)*在计算上是不可行的。换句话说，从f的完整描述中计算f-~在计算上是不可行的

如果*函数f-~一旦知道某些私有的“陷门”*信息就很容易计算，并且在没有这些知识的情况下f是*单向*的，那么函数f就被称为陷门单向函数。

很明显，任何陷门单向函数f及其逆函数f-~都可以作为公钥密码系统的E-D对。当且仅当f也是消息集(M)上的一个置换时，数字签名特征才会是系统的一部分。

Diffie和Hellman [DIFF76]以及独立的Merkle [MERK78a]也引入了*公钥分发系统的概念*。这样一个系统的目的是使每一对订阅者都能安全地通过an交换私钥

为此，作者提出了以下实现方案:

Diffie 和 Hellman 方法的安全性是基于对素数取模计算对数的难度。给定一个素数 q 和一个整数 X, 1 _< X _ q - 1，就可以计算

$$Y = a\ X\ (\text{mod} q),$$

其中 a 是 GF(q)的一个固定原始元素，使用最多 2 个 log2q 乘法(见 KNUT69, pp. 398-422)。另一方面，对于精心选择的素数 q，最著名的取对数的方法，即从 Y 计算 X，需要大约 *q~/2* 次运算[PoHL78]。现在，每个用户 A 从集合{1,2，…， q - 1}并计算出 YA =一个 *XA* (mod q)。在保密 XA 的同时，他将 YA 放在一个公共目录中。当用户 A 和用户 B 想要通信时，他们使用 gAB = *YA xa = YB xa = A XAXB* (mod q)作为他们的私钥。尽管 A 和 B 中的每个人都可以通过使用自己的秘密 X 和合作伙伴的公开 Y 来轻松计算 KAB，但拦截者 C 必须从 YA 和 YB 中计算 ka。由于 KAB = *YA l ° g ″ e*~(rood q)，系统的破坏难度最多和计算对数 mod q 的难度一样大。这两个问题是否真的等价还没有解决。

Merkle 的方法是基于“谜题”的概念。*谜题*是来自密码系统的密码，可以在可行的步骤数 *O(n)内被破解*。然而，数字 n 应该足够大，使得需要 *O(n 2)*步的计算难以处理。每个用户发布(或根据请求传输)n 个谜题，每个谜题“谜题”一个由两个组成部分组成的消息:一个随机分配的唯一标识谜题的 ID 和一个从预定的密钥空间随机选择的密钥。当用户 A 想要与用户 B 通信时，他随机选择 B 的一个谜题，以 *O(n)* 步将其破解，在公开的情况下将该谜题的 ID 传送给 B，并使用相应的密钥对他发送给 B 的消息进行加密。如果第三方 C 希望找出该密钥是什么，他唯一的办法就是以某种随机的顺序逐个解决 B 的谜题，直到截获的 ID 被破解。预期的

viously O (n2)。

更传统的密钥生成和分发方法用于加密系统，如 DES，最近发表在 *IBM 系统杂志* 的一个特殊的密码学部分 [EHRs78, MATY78]。我们现在继续描述现有的公钥密码系统的实现。

计划

RSA 方案[RIvE78a]中的消息和密码以 0 到 n - 1 之间的整数形式出现。(任何将数据块表示为整数的标准方法都可以。)每个用户以下面描述的方式选择自己的 n 和另一对正整数 e 和 d。用户放置在公开文件中的加密密钥由 in, e)对组成，对应的解密密钥由 in, d)对组成，其中的分量 d 是保密的。消息 M 的加密算法 E 和密码 C 的解密算法 D 分别为

$$E(M) = M\ E(\text{mod} n),$$

$$D(C) — C\ D(\text{mod} n)。$$

(注意，这两个操作执行起来都很简单，加密和解密的结果都是 0 到 n - 1 之间的整数。)选择整数 e 和 d 来满足

$$(xe)\ d = (Xd)\ e = X\ ed = X\ (\text{mod} n)$$

对于 0 到 n 之间的每一个整数 X，因此，

$$\mathbf{E(D(}X\mathbf{))} = \mathbf{D(E(}X\mathbf{))} = X \quad (r$$

RSA 方案的安全性取决于分解大数的难度。这个难度发挥作用的方式如下。每个用户(私下)选择两个大素数，p 和 q，使用一些随机选择过程和最近发表的有效素数测试之一[MILL75, RABI76, SOLO77]。然后取整数 n 为(秘密)p 和 q 的乘积，然后从相对素数小于~(n) = (p - 1)(q - 1)的整数集合中随机抽取一个数字 d > max(p, q})。最后，

使用欧几里得算法的一种变体(参见KNUT69中的练习4.5.2.15)，整数e, 0 < e < ~(n)，由~)(n)和d计算为d模q~(n)的乘法逆。也就是说,

e.d. - (模式

Rivest、Shamir和Adleman [RIvE78a]用p =- 47、q = 59和d -~ 157的例子说明了他们的方案。这些素数产生了n = 47.59 ~ 2773, ~)(n) == 46.58 = 2668, e = 17。由于n > 2626，我们可以使用替换来编码每个块的两个字母:blank = 00, A =- 01, B - 02 ....， z = 26。有了这种数字表示，每个块都是四位数长，并且消息IT is ALL GREEK TO ME be-出现了

0920	1900	0112	1200	0718
0505	1100	2015	0013	年

由于二进制(e) = 10001，每个块M的加密可以用5次乘法来完成:M 17 =- (((M2)2)2)2。M.对于第一个块，我们得到92017 = 948 (mod 2773)，整个消息被加密为

0948	2342	1084	1444	2663
2390	0778	0774	0219	年

明文可以通过将每个密文块提升到d——157模2773的幂来复制。

现在，已知已公布的n和e，尝试破解密码的一种方法是将n分解为p和q，计算~(n) = (p - 1)(q - 1)，并使用欧几里得算法从6(n)和e计算d，所有这些都非常简单，除了分解部分。使用已知最快的方法(R. Schroeppel，未发表)分解200位n (Rivest等人推荐的大小[RIvE78a])所需的运算次数超过1023，对于1-#s/运算的计算机将需要超过3.109年才能完成。

有人可能会考虑其他方法来打破这个方案，这些方法不会重新排序到因数分解。在*密码学*[SIMM77]中提出了一种这样的方法，但该方案的发明者已经准备好反驳它[RIvF.78b]。最近，有人(由M. Rabin，未发表)表明，打破一个稍微更一般的方案，使用任何方法，实际上都等同于因式分解。这个最新的结果使RSA方案处于一个相当安全的位置，只要分解仍然困难。

值得注意的是，与Diffie和Hellman公钥分发方案类似，破解RSA方案也可以被视为计算模对数的问题，其额外的复杂性是模是复合而不是素数。关于选择和生成素数p和q以及整数d和e的方法的要点，请参阅RIvE78a。

3.2 Merkle-Hellman (MH)方案

MH方案[MERKT8b]中的消息是二进制n向量，M = *(blb~…bn), bj*

(0,1}，而公开加密密钥是一个所谓的*活门背包*n向量a——*(ala2…An)*，其中的aj是正整数，选择的方式将在下面描述。消息M的加密算法为

$$\mathbf{E}(M) = AM^{\mathrm{T}} = \sum^{n} a_j b_j,$$

结果是0到a之间的整数c = ~yzl a~。对应的密码C是C的标准二进制表示形式，C =- binary(C)，使用[log2(1 + a)]位，其中[x]表示最小整数_x。

虽然从M计算C很简单，但对于某些精心选择的背包向量A，反过来显然是非常困难的，除非知道内置的活板门。在我们进一步阐述密码分析的难度之前，我们先来描述生成陷阱门背包的方法和隐含的解密算法。

陷阱门信息或秘密解密密钥是一对大的正整数w和m，它们满足:

I) w小于且相对素数为m;即w有一个乘法逆w -~，0 < w -1 < m模m。

ii)若dj = *w-laj*(对m取模)，则

$$\hat{a}_j > \sum_{i=1}^{j-1} \hat{a}_i, \qquad j = 2, 3, \ldots, n$$

$$\sum_{i=1}^{n}$$

很容易验证 i)和 ii)暗示了以下简单的解密过程。给定 C = binary(C)，

1)从 c 计算 c;

2)计算~ = *w*-~*c*(mod m);

3)计算 *M = (bib2⋯Bn)*， *bj* =0,1，根据

3.1) set b， = 1 当且仅当~_> d，;

3.2) forj=n- 1,n -2 .....1, setbj =

$$\text{for } i = n-1, 1$$

$$\sum_{i=j+1} \hat{a}_i b_i$$

方案通过一个 n = 5, m = 8443, w = 2550, A =(171, 196, 457, 1191, 2410)的例子。然后由 A = *wA*= (5457, 1663, 216, 6013, 7439) (mod 8443)和 w -~ = 3950 (mod 8443)给出活板门背包。给定的和

C = 1663 + 6013 + 7439 = 15115，

，解密通过首次计算进行

3 = *w*-~*c* = 3950。15115 = 3797 (mod 8443)。

由于 E > d~，我们设 b~ = 1。然后根据 3.2)的规则，我们确定 b4 = 1, b3——0,b2 =1，和 bl = 0。

Merkle 和 Hellman 推荐使用长度为 n_ > 100 的背包向量。对于 n = 100，他们建议 m 从 2 TM + 1 和 *2202* -1 之间的整数中均匀选择;a~s 从(2 ~-~ - 1)21° ° + 1 和 21° ° + j - 1, j = 1,2 .....之间的整数中均匀选择 n;并从 2 到 m - 2 之间的整数中均匀地选择 TB，然后反复除以 gcd(TB, m)得到 w，使得 gcd(w, rn) = 1 (gcd 代表最大公约数})。然后据此计算出 aj

aj = (modm),

并被列入公共档案。这些选择确保满足 i)和 ii)，并且 a/s 具有随机选择的一组整数的外观。

为了增强安全性，默克尔和 Hellman 建议对暗门遮挡变换 aj = *WDJ*(mod m)进行多次迭代，每次使用不同的 w 和 m 对。他们还提出了他们的方案的“乘法-生物-背包”版本，并建议结合这两个版本来生成迭代的活地门背包。然而，随着每次迭代，区块长度都会略有增加，这解释了该方案不具有“onto”属性;也就是说，并不是密码学范围内的每个整数 c 都可以作为 aj 的某个子集的和来获得。因此，MH 方案不具有直接的数字签名特性。在他们引用的文章中，作者提出了一种修改后的签名过程，对于一个足够密集的“into”映射，在执行修改后的签名之前，将需要有限次数的尝试。一种生成具有修改签名特征的密集背包的改进方法正在准备中[MERK78C]。

MH 方案的安全性基于所谓的背包问题的难度，在当前上下文中，背包问题可以表述为确定给定 n 个正整数集合的子集的问题，该子集成员的和具有规定值。这个问题属于一类被称为 np 完全的难题(见 KARP72, AHO74 节)。然而，仅仅基于背包问题是 np 完全而接受 MH 方案是安全的，存在三重威慑。首先，目前还没有证据表明，在 MH 陷阱中，问题仍然是 np 完全的;其次，np 完全类的成员资格是根据最坏情况确定的;第三，我们还不完全清楚 np 完全问题的最坏情况样本有多难。下一节的讨论和例子将进一步阐明这些观点。

基于 McEliece 方案[McEL78]

线性纠错码的一般解码问题的难度，尽管长期以来都被认为是困难的，但直到最近才证明[BERL78]是 np 完全的。公开加密密钥

是秩为 k 的 k × n 二进制矩阵 G，作为一个明显任意的(n, k)线性代码的生成器。实际上，G ~ S(~P)，其中

为易于解码的 Goppa 码[McEL77，第 8 章]的生成矩阵，S 为随机二进制 k × k 非奇异扰码矩阵，P 为模糊 g 的代数结构的随机置换矩阵，对于足够大的 m，码长为 n ffi 2 m，码维为 $k >\_ n - mt$，其中 t 为码的纠错能力。密码消息为二进制 k 向量，消息 M 的加密算法为

$$\mathbf{E}(M) = MG \oplus Z,$$

其中 Z 是一个局部生成的随机向量，长度为 n，权重为 t(注意，生成的密码长度为 n)。

秘密活板门信息分别由矩阵 P 和 S 的逆 P-~和 S -~组成。密码 C 对应的解密过程很容易执行，如下所示:

1)计算 C -~ *CP* -~。(注意，C 是 g 生成的 Goppa 代码的码字。)

2)应用 Patterson 的算法[PATT75]将(~)解码为~/——ms(运算次数为 *O(nt))*。

3)计算 M -~. ~7/S-~。

McEliece 加密方案只覆盖了一小部分密码空间，因此缺乏签名特性。

在讨论该方案的强度时，McEliece 建议，最有希望的攻击方法是随机选择 n 个加密比特中的 k 个，希望这些比特都不会出错(因为 Z 的 t 个非零比特)，并通过反转相应的 g 的 k × k 子矩阵来计算 M，如果可能的话，对于 n = 1024, k = 524 和 t - 50, McEliece 计算出找到 M 所需的预期操作数约为 10 TM。对于相同的参数，他计算出能够对一个随机选择的长度为 1024 的向量进行“签名”的概率只有 2 -21g 左右，这确实是一个非常小的分数。

3.4 Graham-Shamir (GS)方案

GS 方案是 MH 方案的一种变体，其本质区别在于隐藏的、易于求解的背包 a =((1152⋯静脉)。在十进制表示法中，每个背包数 d~的形式为

$$\hat{a}, = R,_1 I,0' R,_2$$

其中 Rjl 和 R~2 是随机的 50 到 100 位数字，t 是一个由 t 个零组成的字符串，/j 是一个 n 元组，第 j 位为 1，其他位置为零。整数 t 被选择为每个 Rj2 乘以 9(消息是十进制 n 元组)并加上 n 个乘积 9- R~2 所产生的“*进位*溢出”中的位数。很容易验证，在这些条件下，~…A~T 的十进制表示在 dj 表示中单位向量部分(/j)占据的 n 个位置上有消息 M。

在 MH 方案中，公共背包 A = *(A ~a2⋯的一个或多个迭代得到GS 方案的 an}*

形式 *aj* -~ *WDJ*(mod m)， $= 1, 2, \ldots, n,$

其中 m > 9 . y，~-i d，和 gcd(w, m)——1。Graham 和 Shamir 认为，简单背包 A 的组成部分的随机侧面(Rj~和 Rj2)使其公共背包 A 的伪装程度比 MH 方案中可能的更高。(注意，从每个 aj 中删除 RjI 部分会得到一个背包，其组件满足简易 MH 背包的强优势特性 ii)。

3.5 纯签名方案

纯公共签名(Public signature-only, PSO)方案使用公共签名目录提供不可伪造的双向认证，但不提供隐私。也就是说，PSO 方案保护消息的发送者免受预期接收者或冒名顶替者的伪造;它保护消息的每个接收者免受发送者的否认或冒名顶替者的植入，但它需要额外的手段来对拦截器隐藏签名消息的内容。

这个未发表的方案是由贝尔实验室的 Ron Graham 和麻省理工学院的 Adl Shamlr 独立提出的，并在这里用他们的双年结进行了描述

虽然我们在本文中主要关注的是提供隐私(有或没有身份验证)的系统，但我们简要概述了 Adi Shamir [SHAM78]最近发表的(1978 年 7 月)PSO 方案，因为它突出了隐私和身份验证之间明显固有的权衡。MH 和 GS 方案通过使用可逆(但不是上)的活地门背包来实现隐私，Shamir 使用上(但不是可逆)的活地门背包来实现身份验证。他的 PSO 方案的工作原理如下。

每个订户放置一个长而随机的背包向量 *a = (al a2⋯A2k)*放在一个公共文件中，供其他订阅者用来验证他签名的消息。3 消息 m 是 0 到 n - 1 之间的整数，其中 n 是 k 位数字。秘密活板门信息是一个 k × 2k 的随机二进制矩阵 R，它的选择与 a 的选择相协调，以满足(详见 SHAM78)

(modn),

其中 B =(21)⋯2 k - ~)。

要签名一条消息 m，首先要随机得到

QA T (modn),

其中 Q 是一个 2k 位的随机二进制向量。接下来，利用 n~的二进制表示 M，我们可以写出

(mod n)

where $\hat{C} = \hat{M}R$. Finally, we have

$$m = \hat{m} + QA^{\mathrm{T}} = (\hat{C} + Q)A^{\mathrm{T}} \pmod{n}$$

对(m, C)的真实性可以很容易地通过对公共向量 A 检查 m = *CA*t 的等式来验证。如果给定 m 和 A，对 C 求解这个等式确实是难以处理的，则签名是 failsafe 的。这种 PSO 方案所提供的实际安全性当然是未定的。关于这个问题的详细讨论以及增强方案安全性的方法，读者可参考 SHAM78。

这个方案的一个微妙之处在于，它在不可伪造方面提供的安全性

3 Shamir 建议选择一个约为 100 的 k

签名是以牺牲隐私为代价的。当可逆线性变换的密度增加时，例如由一对一背包方案(或 McEliece 方案)提供的密度增加，反转它的难度降低。在极限情况下，当变换是映上时，问题就简化为对一个非奇异矩阵求逆的问题。为了使问题保持困难，变换必须变为奇异或非唯一可逆，从而对于隐私目的变得无用，因为它不能保证无二义性解密。

因此，是否应该对 MH、GS 和 McEliece 方案进行限制以达到一定程度的密度是值得怀疑的，这种密度在使签名在统计上可行的同时，可能会超出容忍范围地损害隐私。相比之下，RSA 方案是基于非线性变换的，尽管变换既是可逆的，又是正的，但打破它显然是一个难题。

CRYPTOCOMPLEXITY

目前实践的密码学(DES 和新的公共方案)的主要缺点之一是缺乏证据证明这些方案确实像它们被认为(或声称)的那样难以破解。尽管 DES 的发明者和赞助者引用了许多人/计算机年的时间来徒劳地试图破解它，但新公钥密码的发明者援引了密码分析师所面临的计算任务的难处，这些密码分析师使用了最知名的因式分解、整数背包打包、线性代数代码解码等算法。(我们之所以强调“公开”这个词，是因为如果某个有保密动机的组织有一个可行的算法，比如说，分解 200 位整数，它几乎不会倾向于公开这一事实，更不用说公布算法了。)

虽然在确切的日期上存在分歧，但围绕 DES 争论的各方都同意它只是一个

再过几年(5 到 10 年，取决于哪一方)，它的当前版本就会变得容易受到资金雄厚、利益相关方的攻击。考虑到公钥密码系统的重要性和深远影响，问题是最近提出的实现是否(或何时)会屈服于一个高度积极的数学社区(学术或其他)的共同努力。

真正的任务和挑战是提出适当的加密安全性标准和相应的加密措施——这将有助于用更严格的不可破解性断言取代目前对模糊的密码“认证”概念的依赖。

这一领域的许多工作者都有一种强烈的感觉，即研究密码复杂性的适当框架与已有十年历史的组合复杂性理论密切相关。这一理论的一个主要成就是认识到，许多表面上不相关的工程难题，多年来吸引了研究人员的兴趣和努力，但从计算复杂性的角度来看，它们属于一个等价类的问题，这些问题可以相互简化。

如果存在一种确定性算法，能够在“问题*长度*”(例如，用二进制表示问题参数所需的比特数)的某个多项式限定的计算时间内解决问题的每个样本，那么这个问题就被称为属于 P 类。

在许多有趣的问题中，到目前为止还没有找到这样的算法(不是因为缺乏动机)，包括旅行推销员问题、图着色问题、背包打包问题和许多其他问题 [KARP72, AHO74]。所有这些都属于一个被称为 *NP*(非确定性多项式)的类，它的定义是，对于 NP 中的每个问题，存在一个非确定性算法(即，具有无限并行性)，该算法在多项式时间内解决问题的每个样本。另一种说法是，对于 NP 学中的每个问题，存在一个确定性算法，对于问题的每个样本，都可以检入多项式时间是猜测解的正确性。

很明显，NP 类包含 P 类。组合复杂性的一个未解决的大问题是 NP 是否严格大于 P。Karp [KARP72]已经确定了 NP 的一个子类 NPC (C 表示完全)，其区别在于，如果发现 NPC 的任何一个问题属于 P，那么所有 NP 都属于 P，这意味着 P = NP。以上提到的所有问题都存在于 NPC 中。

考虑到为 NP 问题寻找多项式时间算法所付出的努力及其 NPC 子类的区别性质，相信 P = NP 等式的人很少。难怪许多密码学家认为 NPC 问题是建立密码系统的潜在候选问题。在下面的例子中，我们的目标是提请读者注意可能存在的陷阱，因此，在检查此类模型时需要谨慎。

例子:一个容易破坏的 NP-Complete 密码

这个例子是由作者 Shimon Even 和 Yacov Yacobi 共同推导出来的。它演示了一个密码，即使在选择的明文攻击下，破解其密钥的问题也是 np 完全的。然而，给定足够的已知明文，以接近统一的概率，破解密钥可以简化为在 n 个未知数中求解 n 个独立线性方程的简单问题，其中 n 是密钥位的数量。

该方案是一种传统的私钥分组密码，其总体结构如图 1 所示。密钥长度为 n 位，*K = (xlx2…x，)*，消息是长度为 m 的二进制块，其中 m = [log2(1 + ~%1 aj)]， A = *(ala2 A，，)*是一个任意的具有正整数分量 A ~的背包，假设密码分析者知道。要获得消息 M 的密码图 C，请按照以下步骤进行:

1)在本地生成一个特设的随机二进制向量 R;

2)计算数字 s——A (K•R)T;

3)集合 *C = (M~ S, R)*，其中 S——二进制(S)。

n, m•S 的 m位后跟 R 的 n 位，并且对于每个 m 生成一个新的 R。解密也很简单:因为合法的接收者知道 K，他可以把 K 加到接收到的 R 中，计算出 s，从中他可以得到 s，从而得到 M。

从密码分析者的角度来看，最糟糕的情况是，对于他所有已知的明文，特设向量 R 保持不变。然后，在已知和选择明文攻击下，破解密钥需要解决方程 s -A (K @ R)T 对于给定 s, A 和 R 的 K。当然，这相当于解决 np 完全的背包问题。

一个可能性更大的事件是，给定足够多的已知明文，密码分析师将有 n 对*(M, C，)*，其中 C，= (M，*@ St, R，)*，i = 1,2 .....n，使得 n 个向量 U = 1" - 2R 在实数上是线性无关的(1n 是 n 个 l的向量)。对于每一个 i = 1,2 .....M，我们有

其中*表示组件式乘法。因此，

$$= R, R\ K \sim + K$$
$$* U,$$

$$= A(K \Phi R_t)$$
$$= A(R_t + K * U_t)'$$
$$= AR_t^{\mathrm{T}} + A(K * U_t)^{\mathrm{T}}$$

令 *t，= s，- ARz t*，将 n 个方程写成矩阵形式，我们得到

由于 U~是独立的，并且对于所有 j 都有 aj > 0，可以很容易地解出关键分量 x~。可以证明(见 LEMP78，附录 1)N >_ N 对(M, C)产生 N个线性无关的 U, s 的概率下界约为~，对于 N = N;当 N = N + 1 时，下界加倍，随着 N - N 的增加，下界迅速趋近于 1。

这个例子并不是要减损以任何方式从作为加密方案基础的难题的潜在有用性。我们的目的只是提醒读者，np 完备性的复杂性度量，以及在 NPC 类中未解决的困难问题的公认难度，就加密复杂性而言可能脱离了上下文。通过将 Mer- kle-Hellman 方案与我们的示例进行比较，进一步强调了所涉及的复杂性。这两种方案都是基于背包问题，虽然还不清楚 NPC 是否会破坏 MH 方案，但我们的例子中的方案肯定是这样的。然而，破解后者非常简单，而破解 MH 方案的可行方法尚未找到。

还应该指出，示例方案的大部分(如果不是全部)弱点是由于 C 对 m 的线性依赖。长期以来，密码中的线性一直被认为是密码学家的诅咒和密码学家的祝福。当我们讨论具有某种线性的方案中的隐私和身份验证之间的权衡时，我们已经在第 3 节的末尾解决了这一点。

很容易修改我们示例的方案，使其密码分析像任何已知的一样困难。例如，可以用 ms (mod *pq)代替 M $ S*，就像在 RSA 方案中一样，或者用 DES(M, S)代替 M $ S，也就是说，通过将 DES 方案应用于 M 而 S 作为 DES 密钥的结果。我们不提这一点，是为了提出另一个方案，其难解性是一个猜想问题。如前所述，我们认为需要的是努力建立一些在密码复杂性背景下真正有效的标准，然后才尝试发明符合这些标准的方案。正如 RABI77 中所指出的那样，我们离实现这一目标还很遥远。

作者很高兴地感谢我在准备这项调查时得到的帮助。特别感谢马丁•科恩(Martin Cohn)在内容和风格上提供的宝贵帮助，感谢马丁•赫尔兰(Martin Hellraan)帮助修改斯佩里的原始报告，并感谢 Ron•格雷厄姆(Ron Graham)和阿德尔•沙姆(Adl Shamtr)允许描述他们的未出版之处

hsh 方案。作者还要感谢 Len Adleman、Shimon Even。利兰·加德纳。Martin Hell- nan, Ralph Merkle, Nick Pippenger, Michael Rabir Ron Rivest, Adi Shamir, Nel Sloane, Shmuel Winograd 和 Yacoh Yacobi 进行了有益的讨论:

BEFERENCES

啊 O 74 霍，A.V.霍普克罗夫特，J.E.和乌尔曼，J. D.计算机算法的设计与分析。Addı son-Wesler Reading, Mass。, 1974 年

BERl.78 Berlekamp, e.r, McEliece, rj。和范提尔堡，h。“论某些 codir 问题的固有顽固性”，IEEitAE 翻译。通知。概率。t-24,3(1978 年 5 月)，384-386。

BRAN76 布兰斯塔德，d. k.步态。J. AND . KATZKE, S.关于支持计算机安全的密码学研讨会的报告，NBS 代表 NBSIR 77-1291, 21-22, Nat. Bur. 的立场。， 1976 年 9 月

DIPF76 IFFIE, W. AND HELLMAN, M . E. anhy,EEE《密码学的新方向》，2011 年 11 月

DIFF77 1976), 644-654

迪普菲 w.和 HELLMAN e.“NBS 数据加密标准的密码分析”，计算机 10。

DIFF79 6(1977 年 6 月)，74-84

迪菲 w.和 HELLMAN e.“Pr- vacy and authentication: a introduction: an introduction on cryptography Proc. I lare 1979)。

EHRS78 埃尔萨姆，w. f.马蒂亚斯，s. m .迈耶，c. h .和塔奇曼，w. l .。“一个用于实现数据加密标准的 crypp - tographı c 密钥管理方案 IBMSust 17 91978) 106- 125

FEIs7: Fristei, h. c .

我和我的计算机隐私，”Scl。Am 228(1973 年 5 月)，15-23。

FRIE67

GARDT 弗里德曼，w. f .;《密码学》，《大英百科全书》，1967 年第 6 卷，第 844-851 页

GEPF7E 加德纳,M。“一个需要数百万年才能打破的新 kı nd 盖弗”《科学杂志》237(1977 年 8 月)120- 124

HELL76 格菲，p.r。“如何用真正难以破解的密码保护数据。电子学 46,1(1973 年 1 月 4 日)99-101。

HELLMAN，m. e.默克尔，r.…施罗普-佩尔，r.华盛顿，1，迪菲，w。pollig, S.和 SCHWEITZER, P.对 NBS 数据进行加密的人工尝试的结果是一种数据加密标准。代表 SI 2, Informatı on 系统实验室。，Stanford U Ctr。系统研究，1976 年 9 月 9 日。

HeLLTT

KAHN67 HELLMANe.“香农理论方法对密码学的扩展。”IEEE 翻译通知。T23 理论。3(1977 年 5 月)，289-194。安。D.密码破译者:秘密写作的故事。Macmullan。新 Vork

KARP72 卡普。r.m。“Reproducı 性

复杂组合问题“在计算机计算中，r.e.米勒和 j.w.撒切尔(编)，全会出版社。纽约，1972，第 85-104 页。计算机程序设计的艺术，卷 2:半数值算法，Addison-Wesley, Reading, Mass, 1996

KNUT69

Kolaa g b .;“C

Ko ı A77 ı A 〈s:1> Computer encryptı on 与国家安全局的联系”，《科学》197(1977 年 7 月 29 日)。438 - 440。

Kola77H KOLATA，G. B。“密码学正处于革命的边缘?《科学》197(1977 年 8 月 19 日)，747-748

kola78 KOLATA, G. B《密码学:国际开发协会的秘密会议?》Seence 200asecret meeting and (19)

lemp78 LEMPEL, a . transton 中的密码学:一项调查，Rep. SCRC-RP-78-43, Sperry Rand Res. Ctr。，马萨诸塞州萨德伯里;978 年 9 月

Mar y 78 MATYAS, S. M. AND MEYER, C . H . 《加密技术的生成、分发和安装》

MCEL77 。17,2 (1978phic keys, IBM Svsr MCELIECEncclopeda of mathematics and its applications, vol. Theory of information and coding, Addison-Wesley, Reading)。质量。J.一种基于代数编码的公钥密码系统。ory。DSN 进度任 49。t 公关。

McEL78 44 .斥力实验室。，1 月和 b。1978 年海尔哥哥。

MERK78a MERKLE, R. Secure communicatı on over insecure channels，”common ACM 1,4(1978 年 4 月)，294-299。

MERK78 b

MERK78c r .MERKLE 和 m.e.赫尔曼。“把制服和收据藏在活板门背包里。IEEE 翻译。通知。理论 IT-24(1978 年 9 月)。

MERKLE。r.prvat

MRGate 沟通。ER,emann 的假设和原数检验，”第七届 ACM 年会。《计算理论》。墨西哥新墨西哥州阿尔布格格市 1975 年 5 月，第 234-239 页，扩展版为 Res rep CS-75-27。Dep of computer。科学。，滑铁卢大学。滑铁卢，安大略省，加拿大。1975 年 10 月。

MoRR77

NBS77 莫里斯,RIS。R.斯隆，n.j.a.，和 Wy。NER, A. D.AN，国家标准局提出的联邦数据加密标准评估，《密码学》1,3(1977 年 7 月)，281-291。国家标准局，联邦信息处理标准。出版 46。

PATT75 代数解码器-z 的 Go odesaede gorm。《理论》2(1975 年 3 月译)。- 203 - 207

PERL76 PERLMAN, M.安全通信密码系统中的密钥生成，NASA 技术，Bnef 75。10278,1976 年 2 月。

PLES77 PLESS, V.计算机机密性的加密方案。”IEEE 翻译。第一版。C-26。11(1977 年 11 月)。1133.

。

POHL78 Pohlig, s.和 hellman, m .;GF(p)及其密码学中 computı ng 对数的改进算法

RABI76 意义重大。”IEEE 反式。通知。的。ory it-24,1(1978 年 1 月)，106-110。

RABI77 拉宾，m .;Probabı ı stı c 算法节奏，在算法和复杂性 J. F. Traub(编辑)。Academı c 出版社，纽约，1976 年，第 21-40 页，primalı ty 测试的改进版本提交给 J.数论

RivE78a 拉宾，莫。计算的复杂性——ACM 图灵奖演讲，公共 ACM 20,9(1977 年 9 月)625-635

撕开 78b Rivest, r. l ..SHAMIR，一个…和期刊。一种获得 dag 的方法

SHAM78 数字签名和公钥密码系统-术语，“公共”。ACM21,2(1978 年 2 月)，120-126

SHAN48 Rivest, r. l . 。 “ 对 拟 议 中 的 cryptanalytı c 攻击 M.IT 的评论。Pub - ic-key 密码系统。密码学 2.1(1978 年 1 月)62-65

A. SHAMIR。一个快速签名方案。技术备忘录。麻省理工学院/ LCS / tm - 107。MIT'Cambrı dge,Mass.;1978 年 7 月

香农 CF mathematı cal

communı cation 的理论， “贝尔。stutly and october 1994)， 379-423, y 623-

SHAN49 汉农，c.e.;“Communicatı on 保密系统理论”，贝尔系统公司。J. 28(1949 年 10 月)，656-715。

SHAP77 SHAPLEY, D.和 KOLATA, G. B .《密码学:科学家对公开研究和出版的威胁感到困惑》。科学 197(1977 年 9 月 30 日)，1345-1345 西蒙斯，g.j.和诺里斯。M. J .“Mi 公钥密码系统的初步评论”，《密码学》1.4(1977 年 10 月)，406-414。

SIMM77

SINK68 a . SINKOV，小学 cryptanalysı s，一种数学方法。新的数学。兰登书屋 22 号图书馆，纽约，1968 年。

SMT71 luctfer 的决定，cryptographı c 数据通信设备，众议员 RC3326, IBM 白原，纽约

SoL077 SoLOVAY, R.和 STRASSEN, V.。“对prı malty 的快速蒙特卡罗测试”，SIAM J. Comput. 6(1977 年 3 月)，84-85。

SSCI78 参议院 Sele 的工作人员报告，Select Cor

情报委员会，《非机密摘要:国家安全局参与制定数据加密标准》，1978 年 4 月。

SUGA78 苏格曼,R。“密码学研究和出版的自由仍未解决，IEEE 频谱 2,5(1978 年 5 月)，新闻增刊。”

65

收到了 1978 年 11 月，最终修订接受 197 年 2 月?