Study and Practice on Teaching "Cryptology in Computer Networks"

Wu Shuhua, Kang Fei, Zhu Yuefei and Xiao Da
Information Engineering University,
ZhengZhou Mailbox 1001 No. 770, Henan, 450002

Abstract: This paper explores the features of Cryptology in Computer Networks and introduces our methods of teaching the class, including: From the shallow to the deep, heuristic explain cryptology technology; With literary reference, the story, vividly explain cryptology knowledge; Through the actual safety system, specifically explain cryptology application; by the typical programme code, detailedly explain specifically implementation. Practice shows that these methods can improve the effect of teaching and building students' ability to make full use of what they learned in class.

Keywords: Cryptology in Computer Networks, Teaching Methods, college teaching

《网络密码》教学研究与实践

吴树华，康　绯，祝跃飞，肖　达
信息工程大学
河南郑州市 1001 信箱 770 号，450002

【摘要】本文针对《网络密码》的课程特点，研究了在工科学生中开设该课程的教学方法，主要包括：由浅入深，启发式地讲解密码技术；联系典故、故事，生动地讲解密码知识；通过实际安全系统，具体地讲解密码应用；基于典型代码，详细地讲解密码实现。实践表明，这些方法能有效提高教学效果，培养学生的综合运用能力

【关键词】网络密码，教学方法，大学教学

1 引言

《网络密码》是一门专业课，主要目的是为非密码学专业的工科学生讲解网络中常用的密码技术及原理，使其能应用这些技术解决相关的网络安全问题。其内容要用到数论、代数和椭圆曲线理论等抽象的数学知识，工科学生普遍有畏难情绪，一看到就头疼，针对这些特点，我们采取了灵活多样的教学方法，对于提高教学效果，培养学生的综合运用能力均有明显的效果。

2 教学方法

2.1 由浅入深，启发式地讲解密码技术

现代密码一般都比较复杂，直接讲解，学生很难理解。在教学中，我们常常先由一些简单的例子讲起，再不断完善，逐步引导学生掌握复杂的密码技术。例如在讲解分组密码的 AES 时，如果直接讲 AES 算法本身，学生很难听懂，尤其是列混淆的原理。为此，我们先由 Caesar 密码讲起，得出其数学描述: 加密算法为 $C = (p + 3) \bmod 26$ ，解密算法为 $p = (C – 3) \bmod 26$，其中 a~z 这 26 个字母就分别用 0~25 来表示，明文字母的数值用变量 p 表示，密文字母的数值用变量 C 表示。接着引导学生得出更一般的数学描述:$C = (p + k) \bmod 26$，$p = (C – k) \bmod 26$，其中 k 为密钥，取值范围是 0……25。但由于 Caesar 密码的密钥 k 只有 26 种可能取值，因此并不安全，可以穷举进行破译。要增强 Caser 密码的安全性，自然得想办法扩大密钥的空间。那应该怎样才能做呢？再引导学生想到增加一个新的待定系数，设计出一个更安全的密码体制——仿射密码。注意到，Caesar 密码的加密函数为 $C=(p + k) \bmod 26$，对攻击者而言只有参数 k 是待定的，或者说是待定系数，注意 p 是函数的自变量，它的系数是 1，如果允许它变化，它又可成为一个新的待定系数，基于这种思想就可得到仿射密码的数学描述：C ＝

978-1-935068-09-9

$K_1 \times p + K_2 \bmod 26$， 其中 K＝（$K_1$，$K_2$）为密钥，并要求 K_1 和 26 互素，此时密钥空间大小为 12×26=312，但仍不够大，还是易受暴力穷举攻击。继续引导学生，采用类似方法设计出更加安全的密码体制——Hill 密码。要抵抗暴力穷举攻击，就必须进一步扩大密钥空间。那么还有什么办法能扩大密钥的取值空间呢？显然像前两个加密体制一样，把加密函数限制为单变元的一次函数，是没法再引入待定参数了。要引入更多的待定参数，直观的想有两种方法，一是增加变元的次数，二次增加变元个数。增加变元的次数，加密函数就是一个高次方程，但解密就得对一个高次方程求根，使解密变得很复杂，因此我们不增加变元的次数，仍考虑线性方程，但增加变元的个数，来达到目的。基于这种思想就可得到仿射密码的数学描述（以 m=3 为例）：

有了前面的铺垫，学生就能很容易地理解 AES 的列混淆的原理了，它实质上就是 Hill 密码和仿射密码的组合。

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{12} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \begin{pmatrix} p_1 \\ p_2 \\ p_3 \end{pmatrix} \bmod 26$$

此外，实践证明， 其它的古典密码体制，如单表代替密码、简单置换密码也很有助与对现代分组密码 AES 的理解。

2.2 联系典故、故事，生动地讲解密码知识

单纯讲解密码知识，既抽象又枯燥，再加上学生对其中所涉及的数学知识的畏惧，很难调动学生的积极性。在教学中，我们常常联系一些典故、故事来介绍密码知识，就可以有效地激发学生的学习兴趣，促进学生积极地思维。例如在讲解单表代替密码的破译时，如果单纯地按教材[1]讲解，非常枯燥，很难收到良好的教学效果。我们通过爱伦·坡的小说《金甲虫》[2]中的密码破译过程来讲解，收到了很好的效果。故事讲的是海盗基德在苏里文岛上埋下大批财宝，死后指示藏宝地点的地图失落了。住在岛上的勒格朗偶然间得到了“宝藏图”，并破译了藏宝图上的密码，最终找到了宝藏。小说中的那张藏宝图就是采用单表代替密码加密的：

53##$305))6；4826)4#·)4#)；806*；48$8¶；60))85；]8*；：#*8$83（88）5*$；46（；88*96*？；8）*$（；485)；5*$2：*#（；4956*2 （5*-4）8¶；8*；4069285)；）6$8)4##；1（#9；48081；8：8#1；48$85； 4）485$528806*81(#9；48；（88；4（#？34；48）4#；161；：188；#？;*

破译的主要思想是，在英文中，每个字母并非等可能的用到，经过统计， 人们发现 **e** 是用得最多的字母 ，其次是 R, N, I, O, A, S，而 Z,J,K,Q,X 出现的概率最低。因此，首先，对这段密文的各符号进行统计，发现， “8”出现的次数最多，一共出现了 33 次，此外“；”出现的次数也比较多，出现了 26 次。那么到底是“8”对应字母 e，还是“；”对应字母 e 呢？不难发现两个 8 字还常连在一起出现，果 8 代表 e，则 e 在英文里，应该常常迭用。随便一想，有很多这样的例子，如‘meet’，‘been’，‘agree’等单词里，都含有 ee，这说明 e 常常迭用，8 符合 e 的这一特点。而“；”虽然出现的频率比较高，但密文中没有迭用，与 e 的这一特点不吻合。因此，现在就可以断定 8 代表字母 e 。实际上，除了可以考察单频特性外，还可以考察一些字母组合的统计特性。经过观察，发现“；4e”经常出现，在这段密文中一共出现了七次之多。在英文里，三个字母组合出现频率较高，而最后一个是 e 的是，只有‘the’ 。因此，就可以假定 “；4e” 对应‘the’ 。把知道的符号替换过来就是：

53##$305))6*the26)h#·)h#)te06*the$e¶t60))e5t]e：#*e$e3(ee)5*$th6（tee*96*？te）*$（the5)t5*$2：*#（th956*2 （5*-h ） e¶te*th0692e5)t ） 6$e)h##t1（#9the0e1te：e#1the$e5th）he5$52ee06*e1(#9thet (eeth（#？3hthe）h#161t:1eet#？T*

此时发现，有的地方已经比较容易切入了。例如，加框的地方就只有一个符号还不知道。由于 the 在英语中是一个单词 the ，这样 the 后就应该是下一个单词的开始了。不妨先假设这是一个单词，填上哪一个字母可以拼成一个单词？所有字母试了以后发现，拼不出任何一个单词。于是，可以认为 th 很可能属于下一个单词，那么这会对应哪个单词？不难发现只有把（换为字母 r，可拼出单词‘tree’。于是又确定了一个符号，再把它换过来。依此类推，就可以最终破译为：

A good glass in the Bishop's hostel in the Devil's seat—twenty-one degrees and thirteen minutes—northeast and by north—main branch seventh limb east side—shoot from the left eye of the death's head— a bee line from the tree through the shot fifty feet out.

一面好镜子在皮肖甫客店魔椅——二十一度十三分——东北偏北——最大

树枝第七根桠枝东面——从骷髅头左眼射击——从树前引一直距线通过子

弹延伸五十英尺.

读过《金甲虫》的人都知道，这里有很多隐语。像好镜子是指望远镜，而皮肖甫客店、魔椅、骷髅头均暗指一些地名。这段话大意是，在某个地方，放一面望远镜，以某个角度朝某个方向看，就可以看到宝藏的位置。通过这个例子说明单表代替密码的一般破译步骤如下：首先统计单频，依据语言的冗余度进行分析，再根据分析假设某些结论，然后在假设的前提下，推断出一些结论，并根据双频，字母跟随关系，构词规则，词义等进行验证，逐步分析出正确的明文消息。

联系这个故事来讲解单表代替密码的破译，大大的激发了学生的学习兴趣，给他们留下了很深的印象，教学效果非常好。

2.3 通过实际安全系统，具体地讲解密码应用

网络密码课的最终目的在于运用。以前很多学生在学完该课程以后，面对实际的安全问题还是束手无策，很难灵活应用所学的知识。经过我们调查发现，主要原因是缺少实际运用的例子，只是单纯地介绍各种密码技术，有的虽然有个别运用的例子，但都是针对单一密码技术的，而现实中的安全问题，往往需要综合运用各种密码技术才能解决，因此，难以让学生达到灵活运用的目的。面对这一问题，我们经过实践发现，选用可信计算为例来讲解各种密码技术在一个系统中的运用，能够让学生较好地掌握如何解决实际问题的方法。这个例子是根据可信工作组[3]的文档[4]整理出来的，在实际教学中，得到了学生的普遍欢迎。

可信计算工作组对可信的定义为：可信是一种期望，在这种期望下设备按照特定的目的以特定的方式运转。一旦信任建立，被信任的用户或实体就能执行那些只有被授权的用户或实体才能执行的功能。安全 PC 通过嵌入可信平台模块 TPM 这一硬件来作为信任建立的基础，首先假设一个最小的配置——信任根是可信的，就可以由它对其它更多部分进行检测，并把检测结果安全地记录于 TPM 的 PCR 寄存器中以供感兴趣的实体访问并据此判别是否可信，一旦接受这些部分也是可信的，起始的可信配置就可以加入这部分配置把可信的边界扩大，如此反复进行扩展，就可以得到一个平台是否可信了，如果可信，则称之为可信平台，而可信 PC 就是其中的一种可信平台。检测的过程就叫完整性测量，即获取对平台完整性（可信度）有影响的特征指标数据，保存这些数据并把它们的 Hash 值存于相应的 PCR 中的过程。完整性报告及证实完整性存贮内容的过程。

测量过程是由测量核完成的，由它来产生测量事件。一个测量事件是由两类数据构成的：1）测量值，它表征可信 PC 内嵌的数据或程序代码；2）测量值的摘要, 即前一类数据的摘要，它相当于机器操作状态的一张快照。这两类数据是分开存放的，测量值的摘要须存放于 TPM 的 PCR 中，而测量值可虚拟地存放于任何地方，或者这些值就根本没有存，而是必要时再重新生成。测量数据描述了受测组件的性质和特征，SML 日志中就存有一系列相关的测量数据。由于 SML 可能会变得很大，因而不存于 TPM 中。验证测量事件需重新产生测量摘要，并与 PCR 存放的摘要值进行简单的比较即可。

可信报告有两个功能：其一是把完整性测量存贮区内受保护的内容揭示出来，其二就是根据平台的身份证实所存内容的正确性。为此，用身份证实密钥 AIK 对完整性报告进行数字签名以证实 PCR 的值，签名时要加入 nonce 以防重放攻击。但 TPM 可生成并管理多个 AIK，也可使用多个 AIK，使用不同的 AIK 是为了在平台所有者担心结果发生碰撞时能保护秘密信息。AIK 通常不存放在 TPM 内，而 TPM 内部可以嵌入一个称为 EK 的密钥，EK 用于 AIK 证书发布过程及建立平台所有者的过程中。平台所有者可以建立存贮根密钥（SRK），SRK 用来加密 TPM 的其它密钥，如 AIK，使得它们可存放在 TPM 外，而又仅有该 TPM 能解密。TPM 中仅存放 EK，SRK，认证数据（Authorization Data）等信息，而 AIK 等其它密钥则用 SRK 加密后存在 TPM 外，需要时再临时调入并进行脱密使用。需要指出的是 EK 是在交到用户手里前就已产生好存放在 TPM 中的，它与该平台和其上的 TPM 是永久绑定的，而 AIK 是由平台使用者创建并发布 AIK 证书，发布证书的过程能确保 AIK 与平台的身份也是唯一绑定的，从这个意义上说，AIK 是 EK 的替代密钥，因为出于安全性考虑不能使用 EK 进行签名。

完整性报告的过程是这样的：首先由挑战者向平

978-1-935068-09-9 © 2010 SciRes.

台提出完整性报告请求，该平台收集 SML，并让 TPM 报告相应的 PCR 值，TPM 对这些 PCR 值用 AIK 进行签名后连同签名值一齐返回给该平台，该平台把有关的证书和 PCR 值及其签名一并报告给挑战者。挑战者用 AIK 证书提供的 AIK 公钥对签名值进行验证以确认平台的身份，然后根据 SML 重新计算摘要与 PCR 里的值进行比较，以确认 SML 的完整性，最后根据平台证书里的相应内容对 SML 放映出来的平台的可信度进行评估。应指出，通常平台证书仅仅提供平台正确配置下测量结果的摘要，即 SML 的摘要值，此时只要对比相应的摘要值即可。

通过这个例子，学生可以看到 Hash、公钥加密、公钥签名、密钥管理以及证书的管理等多项密码技术的运用。而且它又贴近信息安全的前沿，对于拓展学生的视野和培养综合运用的能力都很好，经过近几年的教学实践，都取得了很好的效果。

2.4 基于典型代码，详细地讲解密码实现

对于工科学生，仅是理论教学还不够，还需要能与计算机编程结合起来，以提高他们的实践开发能力。事实上，微软公司在 NT4.0 以上版本中提供了一套完整的 Crypto API 的函数，微软的 CryptoAPI 是 PKI 推荐使用的加密 API，其功能是为应用程序开发者提供在 Win32 环境下使用加密、验证等安全服务时的标准加密接口， 而在用这些 API 进行加密解密的时候，只需要知道如何去应用它们，而不必知道它们的底层实现。因此，很有必要让学生学会如何使用 Crypto API 函数来编程。为了达到这个目的，我们通过数据加密的 C 程序片断[5]为例，来讲解 CryptoAPI 的使用方法。

CryptoAPI 的编程模型同 Windows 系统的图形设备接口 GDI 比较类似，其中加密服务提供者 CSP 等同于图形设备驱动程序 ，加密硬件（可选）等同于图形硬件，其上层的应用程序也类似，都不需要同设备驱动程序和硬件直接打交道。因此，首先通过调用 CryptAcquireContext 函数获得一个 CSP 句柄（此时一个会话就相应的建立了，该会话直到 CryptReleaseContext 调用后结束），接着再调用 CryptDeriveKey 函数来创建一个会话密钥，然后再调用 CryptEncrypt 函数使用此会话密钥来加密数据，加密完之后，需调用 CryptDestroyKey 函数来擦除该话密钥，最后调用 CryptReleaseContext 来结束本次会话。需要指出的是 CryptDeriveKey 函数通常是根据一个散列值来创建会话密钥的，例如由一个用户口令的散列值来创建会话密钥，具体过程为，先调用 CryptCreateHash 函数创建一个 hash 对象，再调用 CryptHashData 函数由用户口令来产生一个散列值，然后再通过调用 CryptDeriveKey 函数由该散列值生成所需会话密钥。各函数的详细说明，可以参阅资料[6]。

通过上述例子，学生听后就能基本掌握 CryptoAPI 的使用方法了，之后再通过一些编程作业，如让学生来实现密钥交换，数字签名以及证书管理等功能就可以完全掌握基于 CryptoAPI 的开发方法。此外，在毕业设计时我们还指导学生利用 CryptoAPI 实现许多高级的安全性服务，如用于电子商务的 SET，用于加密客户机/服务器消息的 PCT，用于在各个平台之间来回传递机密数据和密钥的 PFX，代码签名等等。经过实践，这种方法受到的学生的普遍欢迎，起得了很好的教学效果。

4 总结

本文介绍的就是我们在教学中采用的主要方法。但教学无定法，要把《网络密码》这门课程教好，因素很多，需要结合实际情况进行不断的探索。只有不断地总结经验， 探索和改进教学， 才能取得良好的教学效果。

References (参考文献)

[1] W. Stallings. *Cryptography and Network Security, Fourth Edition, Pearson Education (singapore) Pte. Ltd*, 2009.
[2] E. A. Poe. *The Gold-Bug, Dover Pulications, INC. New York, 1991*.
[3] Trusted Computing Group. https://www.trustedcomputinggroup.org.
[4] Trusted Computing Group, “TCG Specification Architecture Overview”, version 1.2, 28 April 2004. URL: https://www.trustedcomputinggroup.org/groups/TCG_1_0_Architecture_Overview.pdf.
[5] Cuick. Microsoft CryptoAPI Encryption technology, http://www .vckbase. com/document/viewdoc.asp?id=974
[6] CryptoAPITrainingGuide, http://www.infosecurity.org.cn/ content/pki_pmi/crypto_ pi_doc.pdf.