安徽理工大學

授课教案设计

课程名称:	现代密码学
课程性质:	专业必修课
课程编号:	0602003120
所在部门:	计算机科学与工程学院
教师姓名:	方贤进
适用专业:	信息安全专业
课程网站:	http://star.aust.edu.cn/~xjfang/crypto/

No.1 密码学概论

教案设计

教师姓名： 方贤进

单　　位： 计算机科学与工程学院

课程名称： 现代密码学

适用对象：信息安全本科专业

教案设计•密码学概论

一、教学内容

第 1 章 密码学概论

1.1 信息安全与密码学

1.2 密码学发展史

二、教学目的和要求

1．知识目标

信息安全的定义、信息安全的目标（5 要素）

2．能力目标

掌握密码学的发展史，尤其是两个质的飞跃：（1）1949 年 Shannon 发表的论文“Communication Theory of Secrecy System”界定了“古典密码学”与“现代密码学”发展阶段。（2）1976 年 Diffie 和 Hellman 在刊物“IEEE Transactions on Information Theory”发表论文“New Directions in Cryptography”,提出了公钥密码体制(Public key Cryptosystem)的思想。

创新能力要求：阅读以上两篇论文。

三、教学重点和难点

1．教学重点

信息安全的定义、信息安全的目标（5 要素）。

2．教学难点

对信息安全的目标（5 要素）的理解。

四、教学方法

讲授、举例说明什么是信息安全的目标（5 要素）。

五、教学过程

1．课程导入内容“为什么要学习密码学，密码学与信息安全的关系”，参见自我设计的 PPT:

http://star.aust.edu.cn/~xjfang/crypto/intro_crypt.pptx

2．讲授内容：

第 1 章 密码学概论

1.1 信息安全与密码学

1.2 密码学发展史

3．作业：page 12：第 2 选择题，第 3 填空题，第 4 术语解释，第 5 简答题-（2）

六、教学反思

1．课程导入内容设计效果好，能激发学生对密码学的学习兴趣；

2．如何进一步加强学生对信息安全目标 5 要素的感性认识。

七、参考资料：网易公开课：什么是密码学？参见：

http://open.163.com/movie/2012/10/S/A/M99VI993U_M9A013QSA.html

No.2 密码学基础

教案设计

教师姓名： 方贤进

单　　位： 计算机科学与工程学院

课程名称： 现代密码学

适用对象：信息安全本科专业

教案设计•密码学基础

一、教学内容

第 2 章 密码学基础

2.1 密码学分类

2.2 保密系统模型

2.3 认证系统模型

二、教学目的和要求

1．知识目标

现代密码学的研究内容、有条件安全性、无条件安全性、计算上的安全性、实际安全性。保密系统的模型、认证系统模型。

2．能力目标

掌握密码体制的攻击的五种类型：唯密文攻击(ciphertext only break)，已知明文攻击(known plaintext attack)，选择明文攻击 (chosen plaintext break)，选择密文攻击(chosen ciphertext break)，选择文本攻击(chosen text break)。

创新能力要求：根据这五类攻击所掌握的信息量要求，能够理解具体的应用场景。

三、教学重点和难点

1．教学重点

保密系统的模型、认证系统模型。

2．教学难点

对密码体制的攻击的五种类型的理解。

四、教学方法

讲授、举例说明唯密文攻击、已知明文攻击、选择明文攻击、选择密文攻击、选择文本攻击的应用场景。

五、教学过程

1．为了说明密码学科的概念及其相关定义，课程导入内容“密码学是一门交叉学科，涉及到数论、近世代数、概率论、组合逻辑、复杂度理论、操作系统、算法与数据结构、计算机网络等多学科知识。”，参见自我设计的 PPT：

http://star.aust.edu.cn/~xjfang/crypto/ch2.pptx

2．讲授内容：

第 2 章 密码学基础

2.1 密码学分类

2.1.1 密码编码学

2.1.2 密码分析学

2.1.3 保密系统模型

2.1.4 保密系统的安全性

2.1.5 认证系统模型

2.1.6 认证系统的安全性

3．作业：page 42: 第 1 判断题(1)(3)(4)(6)，第 2 选择题（1）~（5)、(8)，第 3 填空题（1）~（5)，第 4 术语解释（1）~（8)，第 5 简答题（1）

六、教学反思

1．对保密系统的安全性、认证系统的安全性的讲解比较困难，学生相对较难理解。如何设计此方面的案例辅助讲解是以后教学中要解决的问题。

七、参考资料：“密码系统的安全性”，参见：

https://zhidao.baidu.com/question/1114127549276170859.html

No.3 古典密码体制（1/2）

教案设计

教师姓名： 方贤进

单　　位： 计算机科学与工程学院

课程名称： 现代密码学

适用对象： 信息安全本科专业

教案设计•古典密码体制（1/2）

一、教学内容

置换密码（列置换密码和周期置换密码）；代换密码（代换密码（单表代换密码、多表代换密码和维尔姆密码）；典型传统密码的分析（拟重合指数法破解 vigenere 加密）。

二、教学目的和要求

1．知识目标

置换加密算法、各种单表代换加密算法、多表代换加密算法（Playfair、转轮加密）的原理。

2．能力目标

对置换加密算法、各种单表代换加密算法、多表代换加密算法（Playfair、转轮加密）能够编程实现加密、解密。

创新能力要求：根据转轮加密算法，例如二战中的 Enigma 加密机的原理编程仿真实现。

三、教学重点和难点

1．教学重点

置换加密算法、单表代换加密、多表代换加密。

2．教学难点

转轮加密算法，例如二战中的 Enigma 加密机的原理的讲解及密钥空间大小分析。

四、教学方法

讲授、举例说明唯密文攻击、已知明文攻击、选择明文攻击、选择密文攻击、选择文本攻击的应用场景。

五、教学过程

1．导入内容(前节内容回顾)：现代密码学与信息安全的关系；密码学的发展史；现代密码学的主要研究内容；

本章主要讲解内容：置换密码（列置换密码和周期置换密码）；代换密码（代换密码（单表代换密码、多表代换密码、维尔姆密码、转轮加密算法）。

2．讲授内容：

第 3 章 古典密码体制

3.1 简介

3.2 置换密码

3.2.1 列置换密码的加密与解密

3.2.2 周期置换密码的加密与解密

3.3 代换密码

3.3.1 代码密码的分类

3.3.2 仿射加密

3.3.3 凯撒加密

3.3.4 单表代换密码
3.3.5 Playfair 多表代换密码
3.3.6 维尔姆密码
3.3.7 希尔尔密码(Hill Cipher)
3.3.8 转轮加密算法

3．作业：page 63: 第 1 判断题（1）~（5)、(8)，第 2 选择题（1）~（8），第 3 填空题（1）~（9)。

六、教学反思

1．多表代换加密算法中的转轮加密算法相对较难，学生难以理解。但可以找一些关于二战时 Enigma 加密机的的资料作为学生的辅助阅读材料,另外也可以分析 Enigma 加密机的密钥空间的大小。Enigma 加密机两个转轮间触头触点的变化相当于 26 张代换表，那把右轮和中轮，中轮和左轮，左轮和反射板都考虑进来应该有 26×25×26 种可能，即相当于产生了 16900 张换字表（注意由于有所谓“双重步进”(Enigma 的特殊机械特点)，即左轮进位时还会带动中轮再次进位，相当于中轮一次走了两位,所以中轮只有 25 种排布可能);再加上一般转轮都是 5 选 3，这三个轮还可以随机排列，就是=60；再加上连接板可以使 6 对字母替换：12×11×9×…×3×1=100391791500。综合以上，Enigma 理论上可以产生 16900×60×100391791500=101797276581000000 张代换表。

七、参考资料：

（1）维基百科：https://en.wikipedia.org/wiki/Enigma_machine
（2）Enigma 密码机初级解析:
http://blog.sina.com.cn/s/blog_6f06b8b101016s9r.html

No.4 古典密码体制（2/2）

教案设计

教师姓名： 方贤进

单　　位： 计算机科学与工程学院

课程名称： 现代密码学

适用对象：信息安全本科专业

教案设计•古典密码体制（2/2）

一、教学内容

多表代换密码之维吉尼亚 Vigenere 加密算法；典型传统密码的分析（拟重合指数法破解 vigenere 加密——唯密文攻击）。

二、教学目的和要求

1．知识目标

多表代换加密算法——Vigenere 加密算法的原理；多表代换加密算法的特点。

2．能力目标

Vigenere 算法的加密、解密编程实现。

创新能力要求：利用拟重合指数法对 Vigenere 加密算法的唯密文攻击编程实现。

三、教学重点和难点

1．教学重点

Vigenere 加密算法的原理。

2．教学难点

利用拟重合指数法对 Vigenere 加密算法的唯密文攻击的原理与方法。

四、教学方法

讲授、自编程演示 Vigenere 加密算法、解密算法，从而说明其原理，参见：http://star.aust.edu.cn/~xjfang/crypto/vigenere.c

五、教学过程

1．导入内容：因为多表加密可以将同一字母进行多种替代，从而使字母和句子本身的特性消失，相当于冲掉了字母出现的高频率。频率分析法也就失效了。以 Vigenere 密码为代表的多表替代因其“不可破译”而被称为“密码之王”，这一直持续了大概 300 年，直到的查尔斯•巴贝奇出现。查尔斯•巴贝奇，计算机科学的先驱，设计过差分机、分析机，这些都是早期计算机的模板。多表代换加密的破解最早是德国人卡西斯基。多表加密就是有周期的多组单表替代，所以破译就是从这个“周期”切入。将密文内容按周期数横向排列，之后再观察纵列。这时的纵列，实际上已经是消除过周期干扰的单表替代加密了。因为纵列的字母实则是由一张代换表加密出来的。这时频率分析法就又有效了，多表加密也随着简化为多组单表加密而被攻破。

2．讲授内容：

第 3 章 古典密码体制

3.3 代换密码

3.3.9 多表代换加密——Vigenere 加密算法

3.3.10 典型传统密码的分析

3．作业：page 64：第 4 题术语解释（1）~（5），第 5 简答题（1）（2）（6）。

六、教学反思

自编程实现 Vigenere 加密算法的唯密文攻击的执行过程演示，自己觉得取得了良好的教学效果，能帮助学生更好地理解其方法和原理。如果照本宣科则教学效果肯定要差些。未来计划开发基于 Web 方式的 Vigenere 加密、解密算法、唯密文攻击算法的实现。

七、参考资料：

维基百科：Vigenere cipher:
https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher

No.5 分组密码（1/3）

教案设计

教师姓名： 方贤进

单　　位： 计算机科学与工程学院

课程名称： 现代密码学

适用对象：信息安全本科专业

教案设计•分组密码（1/3）

一、教学内容

分组密码的简介，分组密码的含义，分组密码的设计思想，分组密码的设计准则。

二、教学目的和要求

1．知识目标

分组密码的含义、分组密码的要求、分组密码的设计思想——混乱与扩散、分组密码的原理——SP 网络、分组密码的模型。

2．能力目标

掌握分组密码的设计准则：分组长度(能够抵御选择明文攻击)、密钥长度(能够抵御唯密文攻击)、轮函数 F 的设计准则、子密钥的生成方法、迭代的轮数。

创新能力要求：无

三、教学重点和难点

1．教学重点

分组密码的设计思想、分组密码的模型图。

2．教学难点

分组密码的设计准则及特点。

四、教学方法

讲授。

五、教学过程

1．导入内容：研究历史：现代分组密码的研究始于 20 世纪 70 年代中期，至今已有 40 余年历史，这期间人们在这一研究领域已经取得了丰硕的研究成果。研究内容：分组密码的研究包括三方面：分组密码的设计原理，分组密码的安全性分析和分组密码的统计性能测试。设计分析：分组密码的设计与分析是两个既相互对立又相互依存的研究方向，正是由于这种对立促进了分组密码的飞速发展。早期的研究基本上是围绕 DES 进行，推出了许多类似于 DES 的密码，例如，LOKI、FEAL、GOST 等。进入 90 年代，人们对 DES 类密码的研究更加深入，特别是差分密码分析（differential cryptanalysis）和线性密码分析（linear cryptanalysis）的提出，迫使人们不得不研究新的密码结构。

2．讲授内容：

第 4 章 分组密码

4.1 分组密码的定义

4.1.1 分组密码的含义

4.1.2 分组密码的置换

4.1.3 分组密码的要求

4.1.4 分组密码的设计思想：混乱和扩散

4.1.5 分组密码的原理

4.1.6 SP 网络的性质

4.1.7 分组密码模型

4.1.8 分组密码设计准则

4.2 分组密码的发展史

3．作业：page 121: 第 1 判断题（1）~(5)，第 4 术语解释，第 5 简答题（1）~（4）

六、教学反思

本次课程都是有关分组密码体制的概念、思想、模型，上课内容相对枯燥。

七、参考资料：

维基百科：Block cipher:
https://en.wikipedia.org/wiki/Block_cipher

No.6 分组密码（2/3）

教案设计

教师姓名： 方贤进

单　　位： 计算机科学与工程学院

课程名称： 现代密码学

适用对象： 信息安全本科专业

教案设计•分组密码（2/3）

一、教学内容

DES 算法的简介、DES 算法的实现、DES 算法的安全性、多重 DES

二、教学目的和要求

1．知识目标

DES 算法的加密流程、DES 加密过程的公式化描述、DES 的子密钥生成算法、DES 中的 S 盒、DES 设计的核心。

2．能力目标

掌握 DES 分组密码算法的编程实现、DES 互补性、弱密钥和半弱密钥的算法验证。

创新能力要求：DES 加密算法的安全性分析

三、教学重点和难点

1．教学重点

DES 算法的实现、轮函数、P 盒、S 盒、子密钥的生成算法。

2．教学难点

DES 算法的安全性分析。

四、教学方法

讲授。

五、教学过程

1．导入内容：1973 年，美国的国家标准局(National Bureau of standards,NBS)认识到建立数据加密标准的迫切性，开始征集联邦数据加密标准。有很多公司着手这项工作并提交了一些建议，最后 IBM 公司的 Lucifer 加密系统获得了胜利。经过两年多的公开讨论之后，1977 年 1 月 15 日 NBS 决定利用这个算法，并将其更名为数据加密标准(Data Encryption Stand, DES)。不久，其他组织也认可和采用 DES 作为加密算法，供商业和非国防性政府部分使用。

2．讲授内容：

第 4 章 分组密码

4.3 DES 加密

4.3.1 DES 概述

4.3.2 DES 加密流程

4.3.3 DES 一轮的实现流程图

4.3.4 DES 子密钥生成

4.3.5 DES 的 S 盒和 P 盒

4.3.6 DES 的解密算法

4.3.7 DES 的安全性

4.3.8 DES 的密钥搜索、查分分析、线性分析

4.4 多重 DES 加密

4.4.1 二重 DES

4.4.2 多重 DES 的四种模式

3．作业：page 121: 第 2 选择题（1）~（8），第 3 填空题(3)~(7)，第 5 简答题（4）（5）（6）。

六、教学反思

本次课程讲解的关键点是对 DES 加密算法采用自顶向下,逐步细化的方法讲解：16 轮加密→每轮加密的流程→轮函数 F→选择扩展运算→S 盒子→置换运算→子密钥生成算法。

七、参考资料：

维基百科：Data Encryption Standard:
https://en.wikipedia.org/wiki/Data_Encryption_Standard

No.7 分组密码（3/3）
——AES 加密算法
教案设计

教师姓名： 方贤进

单　　位： 计算机科学与工程学院

课程名称： 现代密码学

适用对象：信息安全本科专业

教案设计•分组密码（3/3）——AES 加密

一、教学内容

AES 算法的简介、AES 算法的实现、AES 算法与 DES 算法的对比、分组密码算法的运行模式

二、教学目的和要求

1．知识目标

AES 算法的加密流程、分组密码算法的运行模式。

2．能力目标

掌握 AES 分组密码算法的编程实现。

创新能力要求：AES 分组加密算法某种运行模式的实现。

三、教学重点和难点

1．教学重点

AES 分组长度、密钥长度、轮数的关系。AES 加密、解密算法流程图：字节代换（AES 的 S 盒）、行移位、列混淆、轮密钥加。分组加密的四种操作模式。

2．教学难点

AES 算法中子密钥的生成算法。分组加密操作中 CFB 模式、OFB 模式的原理。

四、教学方法

讲授。OpenSSL 平台下的 AES 加密算法各种操作模式的运用举例。AES 在线加密工具的使用：http://tool.chacuo.net/cryptaes

五、教学过程

1．导入内容：(1)为什么需要 AES？（2）AES 加密算法即密码学中的高级加密标准（Advanced Encryption Standard，AES），又称 Rijndael 加密法，是美国联邦政府采用的一种区块加密标准。这个标准用来替代原先的 DES，已经被多方分析且广为全世界所使用。经过五年的甄选流程，高级加密标准由美国国家标准与技术研究院 （NIST）于 2001 年 11 月 26 日发布于 FIPS PUB 197，并在 2002 年 5 月 26 日成为有效的标准。2006 年，高级加密标准已然成为对称密钥加密中最流行的算法之一。该算法为比利时密码学家 Joan Daemen 和 Vincent Rijmen 所设计，结合两位作者的名字，以 Rijndael 之命名之，投稿高级加密标准的甄选流程。（Rijdael 的发音近于 "Rhinedoll"。）

2．讲授内容：

第 4 章 分组密码

4.4 DES 加密

4.4.1 AES 简介

4.4.2 AES 加解密流程图

4.4.3 AES 设计上的考虑

4.4.4 AES 的安全性

4.5 分组密码的操作模式(四种)

3．作业：page 122: 第 2 选择题（9）~（11），第 3 填空题（10）（11），第 5 简答题（9）（10）

六、教学反思

AES 算法流程中的“字节代换”的细节和原理可以忽略讲，因为 AES 的字节代换以及逆字节代换完全都可以用“查表（S 盒）”来实现。

七、参考资料：

（1）AES 在线加密工具的使用：http://tool.chacuo.net/cryptaes

（2）维基百科：Advanced Encryption Standard:
https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

No.8 序列密码（1/2）

教案设计

教师姓名： 方贤进

单　　位： 计算机科学与工程学院

课程名称： 现代密码学

适用对象： 信息安全本科专业

教案设计•序列密码（1/2）

一、教学内容

序列密码的介绍，线性反馈移位寄存器，m 序列，LFSR 的特征多项式表示。

二、教学目的和要求

1．知识目标

序列密码的原理，序列密码体制模型，线性反馈移位奇存器理论、m 序列的概念、LFSR 的多项式表示及相关定义与定理。

2．能力目标

LFSR 的特征多项式表示，反之，利用特征多项式来构建 LFSR。

创新能力要求：无。

三、教学重点和难点

1．教学重点

线性反馈移位寄存器的概念，m 序列的概念，LFSR 和特征多项式之间的关系，不可约多项式、阶、本原多项式的概念。

2．教学难点

特征多项式为不可约多项式的条件判断，多项式的阶或周期、本原多项式的概念。

四、教学方法

讲授。流密码 RC4 在线加密工具的使用：http://tool.chacuo.net/cryptrc4

五、教学过程

1. 导入内容:RC4,RC4 加密算法是 RSA 三人组中的头号人物 Ron Rivest 在 1987 年设计的密钥长度可变的流加密算法簇。该算法的速度可以达到 DES 加密的 10 倍左右，且具有很高级别的非线性。1994 年 9 月，它的算法被发布在互联网上。由于 RC4 算法加密是采用的 xor，所以，一旦子密钥序列出现了重复，密文就有可能被破解。RC4 作为一种老旧的验证和加密算法易于受到黑客攻击，现在逐渐不推荐使用了。

2．讲授内容：

第 5 章 序列密码

5.1 序列密码的简介

5.2 线性反馈移位寄存器

5.2.1 m 序列简介与特性

5.2.2 LFSR 的多项式表示

5.2.3 相关定义与定理

3．作业：page 154: 第 1 判断题（1）~(9)，第 2 选择题（1）（5）（8），第 3 填空题（1）~（8）。

六、教学反思

流密码具有坚实的数学基础作为支撑，也就是有限域上的多项式运算，包括不可约多项式、本原多项式、阶等概念，因此让学生掌握这部分的数学知识非常重要。

七、参考资料：

（1）流密码 RC4 在线加密工具的使用：http://tool.chacuo.net/cryptrc4

（2）维基百科：RC4:
https://en.wikipedia.org/wiki/RC4

No.9 序列密码（2/2）

教案设计

教师姓名： 方贤进

单　　位： 计算机科学与工程学院

课程名称： 现代密码学

适用对象： 信息安全本科专业

教案设计•序列密码（2/2）

一、教学内容

m 序列的生成算法、m 序列密码的破译、非线性序列、A5 算法、RC4 算法。

二、教学目的和要求

1．知识目标

m 序列的生成算法、m 序列密码的破译、非线性序列、A5 算法、RC4 算法。

2．能力目标

掌握如何寻找一个 n 次本原多项式，根据此 n 次本原多项式构建一个能产生 m 序列的 LFSR。

创新能力要求：RC4 算法的编程实现。

三、教学重点和难点

1．教学重点

m 序列的生成算法、m 序列密码的破译、A5 算法、RC4 算法。

2．教学难点

寻找一个 n 次本原多项式，根据此 n 次本原多项式构建一个能产生 m 序列的 LFSR；A5 算法流程。

四、教学方法

讲授。

五、教学过程

1．导入内容：A5 简介：它用于对从电话到基站连接的加密，先后开发了三个版本记作 A5/1、A5/2、A5/3，如果没有特别说明，通常所说的 A5 是指 A5/1，关于 GSM 加密问题，一些人认为会因为密码的问题阻碍手机的推广，另一些人则认为 A5 太弱，不能抵抗一些情报机构的窃听，A5 的特点是效率高，适合硬件上高效实现，它能通过已知的统计检验，起初该算法的实际没有公开，但最终不慎泄漏。A5 计算过程：A5 算法由三个线性反馈移位寄存器（LFSR）R1、R2、R3 组成，寄存器的长度分别是 n1=19,n2=22 和 n3=23。所有的反馈多项式系数都比较少。三个 LSFR 的异或值作为输出。A5 用不同的时钟控制。每一个寄存器由基于它自己中间位的时钟控制，并且三个寄存器的中间位的反向门限函数相异或。通常，在每一轮中时钟驱动两个 LFSR。针对 A5 的攻击：有一种直接攻击需要 2^{40} 次加密：先猜测前两个 LFSR 的内容，然后试着通过密钥序列决定第三个 LFSR。这种攻击实际上是是否可行尚待讨论，但是目前一个硬件密钥搜索机正在设计中，并且将解决这个问题。总之，有一点可以明确，那就是 A5 的基本思路是好的，它的效率非常高。它能通过所有已知的统计测试，它已知的仅有的弱点是寄存器太短而不能抗穷举攻击。带较长寄存器和稠密反馈多项式的 A5 的变型是安全的。

2．讲授内容：

第 5 章 序列密码

5.3 m 序列及其生成算法

5.4 m 序列密码的破译

5.5 A5 算法

3．作业：page 155: 第 4 术语解释（1）（4）（6），第 5 简答题（4），第 6 综合分析题.

六、教学反思

流密码具有坚实的数学基础作为支撑，也就是有限域上的多项式运算，包括不可约多项式、本原多项式、阶等概念，因此让学生掌握这部分的数学知识非常重要。

七、参考资料：

（1）维基百科：A5/1:

https://en.wikipedia.org/wiki/A5/1

（2）A5/1 算法的 C 语言实现：

```
/*A5 算法 C 语言实现*/
#include<stdio.h>
#define N 256                    /*循环次数*/
lfsr(int a,int b,int c,int d,int T[]); /*移位寄存器函数*/
void main()
{int     A[19]={1,0,1,1,0,0,1,1,0,0,0,0,1,0,1,0,1,0,1};     /*A、B、C 三个移位寄存器*/
int    B[22]={0,0,1,0,0,0,1,1,1,0,0,1,0,0,1,0,1,0,1,1,1};
int    C[23]={1,0,0,0,1,0,1,1,0,1,0,0,1,0,0,0,1,0,1,0,1,0,1};
for(int i=0;i<N;i++)
{if(i%8==0)
printf("\n");
int j=A[9]+B[11]+C[11];
if(j==0)                 /*j 可能等于 0-3 之间*/
{printf("%d ",A[18]^B[21]^C[22]);
lfsr(13,16,17,18,A);
lfsr(12,16,20,21,B);
lfsr(17,18,21,22,C);}
else if(j==1)
{printf("%d ",A[18]^B[21]^C[22]);
if(A[9]==0)
lfsr(13,16,17,18,A);
if(B[11]==0)
lfsr(12,16,20,21,B);
if(C[11]==0)
lfsr(17,18,21,22,C);}
else if(j==2)
{printf("%d ",A[18]^B[21]^C[22]);
if(A[9]==1)
lfsr(13,16,17,18,A);
if(B[11]==1)
lfsr(12,16,20,21,B);
if(C[11]==1)
lfsr(17,18,21,22,C);}
else if(j==3)
{printf("%d ",A[18]^B[21]^C[22]);
lfsr(13,16,17,18,A);
lfsr(12,16,20,21,B);
lfsr(17,18,21,22,C);}
}}
lfsr(int a,int b,int c,int d,int T[])
{int i;
 for(i=d;i>0;i--)
{T[i]=T[i-1];}
 T[0]=T[a]^T[b]^T[c]^T[d];
}
```

No.10 HASH 函数与消息认证码（1/2）

教案设计

教师姓名： 方贤进

单　　位： 计算机科学与工程学院

课程名称： 现代密码学

适用对象： 信息安全本科专业

教案设计•HASH 函数与消息认证码（1/2）

一、教学内容

hash 函数的定义，hash 函数的通用结构，MD5 算法及其它 hash 函数。

二、教学目的和要求

1．知识目标

散列函数的定义，散列函数的通用结构，MD5 算法。

2．能力目标

掌握根据一个消息，如何进行填充、如何根据 MD5 算法生成其 HASH 值的方法。

创新能力要求：MD5 算法的安全性分析。

三、教学重点和难点

1．教学重点

hash 函数的通用结构，MD5 算法。

2．教学难点

MD5 算法的流程，16 次迭代过程中 A,B,C,D 四个寄存器的值的变化。

四、教学方法

讲授。

五、教学过程

1．导入内容：（1）为什么要讲到 HASH 函数？因为为了实现信息安全目标之一“完整性”的需要。（2）消息认证（Message Authentication）的目的： 验证消息的完整性，确认数据在传送和存储过程中未受到主动攻击。（3）消息认证的方式：①消息加密函数：加密整个消息，以消息的密文文件作为认证，可使用对称密码或公钥密码体制进行加密；②散列函数（Hash）：将任意长度的消息变换为定长的 消息摘要，并加以认证；③消息认证码（MAC）：依赖公开的函数（密钥控制下）对消息处理，生成定长的认证标识，并加以认证。

2．讲授内容：

第 6 章 HASH 函数与消息认证码

6.1 hash 函数的定义

6.2 hash 函数的通用结构

6.3 MD5 算法及其它 hash 函数

3．作业：page 186: 第 1 判断题（1）~（6），（12）（13），第 2 选择题（1）~（5）。

六、教学反思

（1）在 MD5 算法流程的讲解中，需要注意的 4 轮执行过程的处理对象都是原消息的 512bits 分组，只是在每轮计算中这 16 个字（16*32bits=512bits）的排列顺序不一样，这一点在讲解时应注意。（2）MD5 算法中 4 轮 16 次迭代过程中，

每轮中 A,B,C,D 四个寄存器的变化过程应该跟学生讲清楚。

七、参考资料：

（1）参考 MD5 算法的 C 语言/Java 语言实现：
https://baike.baidu.com/item/MD5/212708?fr=aladdin
（2）对 md5 等全球通用公开的加密算法进行反向查询：
http://www.cmd5.com/
（3）MD5 在线加密：https://md5jiami.51240.com/
（4）维基百科：MD5，https://en.wikipedia.org/wiki/MD5
（5）Vulnerability Note VU#836068，MD5 vulnerable to collision attacks：
https://www.kb.cert.org/vuls/id/836068

No.11 HASH 函数与消息认证码（2/2）

教案设计

教师姓名： 方贤进

单　　位： 计算机科学与工程学院

课程名称： 现代密码学

适用对象： 信息安全本科专业

教案设计•HASH 函数与消息认证码（2/2）

一、教学内容

其它 hash 函数，消息认证的概念，消息认证的几种模型，生日攻击，生日悖论，MD5/SHA-1 碰撞攻击的时间复杂度研究进展。

二、教学目的和要求

1．知识目标

其它散列函数算法参数与特性，消息认证的几种模型，生日攻击的时间复杂度分析。

2．能力目标

消息认证模型的使用、生日攻击的时间复杂度分析方法。

创新能力要求：查阅资料掌握最新的 hash 函数的碰撞攻击的研究进展。

三、教学重点和难点

1．教学重点

消息认证模型的使用、生日攻击的时间复杂度分析方法。

2．教学难点

生日攻击的时间复杂度分析方法。

四、教学方法

讲授。

五、教学过程

1. 导入内容：Hash 函数把变长信息映射到定长信息，Hash 函数不具备可逆性，Hash 函数速度较快，Hash 函数与对称密钥加密算法有某种相似性，对 Hash 函数的密码分析比对称密钥密码更困难，Hash 函数可用于消息摘要， Hash 函数可用于数字签名。

2．讲授内容：

第 6 章 HASH 函数与消息认证码

6.4 消息认证

6.4.1 消息认证的概念

6.4.2 消息认证的四种模型

6.5 生日攻击

6.5.1 生日悖论

6.5.2 生日攻击

3．作业：page 188：第 4 术语解释（2）（3）（5）（6），第 5 简答题（8）（9）（11），第 6 综合应用题。

六、教学反思

生日悖论、生日攻击是本次课程的难点，在此需利用概率论、排列组合、数据结构中的知识进行 hash 函数碰撞攻击的时间复杂度分析。也可以提供一些关于此

方面的最新参考文献供学生阅读。

七、参考资料：

（1）SHA-1,百度:
https://baike.baidu.com/item/SHA-1/1699692?fr=aladdin
（2）SHA-1 在线加密：http://www.qqxiuzi.cn/bianma/sha-1.htm
（3）维基百科：SHA-1，https://en.wikipedia.org/wiki/SHA-1
（4）关于碰撞攻击, Vulnerability Note VU#836068, MD5 vulnerable to collision attacks：https://www.kb.cert.org/vuls/id/836068

No.12 公钥密码体制（1/4）

教案设计

教师姓名： 方贤进

单　　位： 计算机科学与工程学院

课程名称： 现代密码学

适用对象：信息安全本科专业

教案设计•公钥密码体制（1/4）

一、教学内容

公钥密码体制的思想及加解密模型，基本单项陷门函数的原理，RSA 密码算法简介，欧拉函数与欧拉定理，RSA 密钥生成算法。

二、教学目的和要求

1．知识目标

掌握公钥密码体制的思想，公钥密码体制所依赖的原理。

2．能力目标

RSA 密钥生成算法的编程实现。

创新能力要求：大数运算的实现技巧，包括大数的素性判定、乘法、大数的扩展 Euclid 算法在模运算下求乘法逆元等的实现技巧。

三、教学重点和难点

1．教学重点

掌握公钥密码体制的模型，包括加密与数字签名。

2．教学难点

欧拉函数与欧拉定理，针对大数的 RSA 密钥生成算法的编程实现。

四、教学方法

讲授。

五、教学过程

1．导入内容：对称密码体制的缺陷(公钥密码体制产生的必要性)：（1）密钥分配问题：通信双方要进行加密通信，需要通过秘密的安全信道协商加密密钥，而这种安全信道在实际中很难实现。（2）密钥管理问题：在有 n 个用户的通信网络中，每个用户要想和其它 n-1 个用户进行通信，必须使用 n-1 个密钥，而系统中的总密钥量将达到 n(n-1)/2。当 n 较大时，这样大的密钥量，在产生、保存、传递、使用和销毁等各个环节中都会变得很复杂，存在着安全隐患。（3）数字签名问题：对称密码体制中通信双方拥有同样的密钥，所以接收方可以伪造签名，发送方也可以否认发送过某消息，难于解决陌生人之间的身份认证和交易信息认证的问题。

2．讲授内容：

第 7 章 公钥密码体制

7.1 公钥密码体制的基本概念

7.2 RSA 算法

3．作业：page 12：第 1 判断题（1）~（5），第 2 选择题（1）~（3）

六、教学反思

公钥密码体制的思想是现代密码学的一个重要标志，但公钥密码体制的安全性都是依赖于数学难题的求解，其中设计到数论（欧拉函数、欧拉定理）、有限域等众多数学知识，因此要注重学生数学知识特别是数论知识的培养。

七、参考资料：

（1）RSA 算法,百度：
https://baike.baidu.com/item/RSA%E7%AE%97%E6%B3%95/263310?fromtitle=RSA&fromid=210678&fr=aladdin
（2）在线 RSA 公钥加密/解密：http://tool.chacuo.net/cryptrsapubkey
（3）维基百科：RSA，https://en.wikipedia.org/wiki/RSA

No.13 公钥密码体制（2/4）

教案设计

教师姓名： 方贤进

单　　位： 计算机科学与工程学院

课程名称： 现代密码学

适用对象： 信息安全本科专业

教案设计•公钥密码体制（2/4）

一、教学内容

RSA 加密、解密算法；RSA 加解密算法的证明；RSA 大数运算相关技巧（大数幂模运算）；RSA 安全性分析。

二、教学目的和要求

1．知识目标

掌握 RSA 公钥密码体制加解密过程，RSA 算法的安全性。

2．能力目标

RSA 加解密算法中相关大数运算的技巧；能利用 RSA 算法对明文消息进行加密、解密的编程实现。

创新能力要求：能利用 RSA 算法对消息实现工业级别的加解密。

三、教学重点和难点

1．教学重点

RSA 加密、解密算法；RSA 大数运算的技巧。

2．教学难点

RSA 加解密算法的证明；RSA 安全性分析。

四、教学方法

采用案例式教学。先讲解算法的执行步骤，再通过小整数域上 RSA 加解密算法的实例进行讲解。

五、教学过程

1. 导入内容：上次课已讲解了 RSA 算法的密钥生成算法，有了 public key=(e, n), private key=(d,n)，就可以实现加解密了，但还有另一个问题就是对明文消息的编码、分组。例如对 plaintext=cyber great wall，按照字母表序号进行编码为：02/24/01/04/17/06/17/04/00/19/22/00/11/11；分组大小的原则是分组长度不超过 $\log_2 n=\log_2(p*q)$bits。Encoding, block 完成后即可讲解 RSA 加解密算法。

2．讲授内容：

第 7 章 公钥密码体制

7.2 RSA 算法

- ●RSA 加密过程
- ●RSA 解密过程
- ●RSA 加解密证明
- ●RSA 加解密举例
- ●RSA 计算技巧
- ●RSA 安全性分析

3．作业：page 216：第 1(6)(7)，第 2 填空题(4)(7)，第 5 术语解释(2)(3)。

六、教学反思

RSA 加解密算法本身并不复杂，但是具体到工业级别 RSA 算法实现时，要解决

大整数运算问题，包括大整数的素性判定、大整数相乘、大整数幂模运算、求一个大整数在有限域上的乘法逆元等问题，这部分是具体算法实现的重点，可以鼓励学生做探索性的研究。

另一个难点就是 RSA 算法的安全性，包括 RSA 同态性质、选择密文攻击、针对 n 分解的攻击、侧信道攻击、短明文、针对 RSA 算法参数的攻击等。这部门讲解比较困难，不易理解，关键是构造相应的针对 RSA 攻击的例子，且这部分对学生数论知识掌握度要求较高。

七、参考资料：

（1）RSA 算法,百度:
https://baike.baidu.com/item/RSA%E7%AE%97%E6%B3%95/263310?fromtitle=RSA&fromid=210678&fr=aladdin
（2）在线 RSA 公钥加密/解密：http://tool.chacuo.net/cryptrsapubkey
（3）维基百科：RSA，https://en.wikipedia.org/wiki/RSA
（4）维基百科，RSA 算法以及“已公开的或已知的攻击方法”:
https://zh.wikipedia.org/wiki/RSA%E5%8A%A0%E5%AF%86%E6%BC%94%E7%AE%97%E6%B3%95

No.14 公钥密码体制（3/4）

教案设计

教师姓名： 方贤进

单　　位： 计算机科学与工程学院

课程名称： 现代密码学

适用对象： 信息安全本科专业

教案设计•公钥密码体制（3/4）

一、教学内容

椭圆曲线的定义；有限域上的椭圆曲线及其运算所构成的 Abel 群及其几何意义；有限域上椭圆曲线点集的计算方法；有限域上椭圆曲线的点加、倍点运算规则。

二、教学目的和要求

1．知识目标

掌握有限域 GF(p)上的椭圆曲线的点集关于加法运算所构成的 Abel 群；有限域上的椭圆曲线的点加运算规则、倍点运算规则。

2．能力目标

有限域上 GF(p)上的椭圆曲线的点集计算、点加运算、倍点运算的算法编程实现。

创新能力要求：在 p 是一个很大素数的情况下，有限域上 GF(p)上的椭圆曲线的点集计算（Schoof 算法）、点加运算、倍点运算的算法编程实现。

三、教学重点和难点

1．教学重点

有限域 GF(p)上的椭圆曲线及其运算所构成的 Abel 群及其几何意义。

2．教学难点

有限域上 GF(p)上的椭圆曲线的点集计算、点加运算、倍点运算方法。

四、教学方法

采用自身开发的可视化工具在线演示实数域上的椭圆曲线点的运算及其几何意义、有限域上的椭圆曲线点的运算及其几何意义。参见：http://star.aust.edu.cn/~xjfang/crypto/

五、教学过程

1．导入内容：（1）RSA 已经是广泛使用的公钥密码体制，已应用于数字签名机制，但为什么还要讲解椭圆曲线加密体制 ECC 呢？（2）阐述 ECC 的优点：安全性高，即在达到与 RSA 同等安全的情况下，所要求密钥长度（即素数 p 的位数）相对较小；密钥量小；灵活性好；（3）ECC 有可能称为未来公钥密码体制的标准，已应用于 TLS,PGP,SSH 当中。

2．讲授内容：

第 7 章 公钥密码体制

7.3 椭圆曲线加密算法

- ●椭圆曲线的定义
- ●实数域上的椭圆曲线
- ●有限域上的椭圆曲线
- ●有限域上 GF(p)上的椭圆曲线的点集计算
- ●有限域上 GF(p)上的椭圆曲线的点加、倍点运算规则

●例题讲解及模 p 下的计算技巧

3．作业：page 216: 第 2 选择题(6)。补充作业：计算有限域 GF（37）上的椭圆曲线上离散点集 E37(-1,3): $y^2 \equiv x^3-x+3 \pmod{37}$，同时对于一个点 P(2,3), Q(21,20)要求计算 5P, P+Q 的结果。

六、教学反思

现代密码学课程中椭圆曲线加密系统（ECC）教学牵涉到椭圆曲线几何、集合论、Abel 群、有限域等很多数学知识，要应用模运算、扩展的欧几里德算法、椭圆曲线在有限域上的点加运算、倍点运算等，导致进行 ECC 教学难、学生难以理解 ECC 等问题，因此开发了一个可视化的工具辅助教学（http://star.aust.edu.cn/~xjfang/crypto/）起到了一个很好的效果，该辅助工具包括椭圆曲线的代数与几何特性的认识、可视化；椭圆曲线下的 Abel 群的定义及几何意义可视化教学；有限域 GF(p)下椭圆曲线点计算可视化教学。

七、参考资料：

（1）Elliptic-curve cryptography:
https://en.wikipedia.org/wiki/Elliptic-curve_cryptography
（2）椭圆曲线密码学：
https://zh.wikipedia.org/wiki/%E6%A4%AD%E5%9C%86%E6%9B%B2%E7%BA%BF%E5%AF%86%E7%A0%81%E5%AD%A6
（3）C++ Elliptic Curve library beta 下载：
https://sourceforge.net/projects/libecc/files/

No.15 公钥密码体制（4/4）

教案设计

教师姓名： 方贤进

单　　位： 计算机科学与工程学院

课程名称： 现代密码学

适用对象：信息安全本科专业

教案设计•公钥密码体制（4/4）

一、教学内容

有限域 GF(p)上的椭圆曲线的点构成的 Abel 群的阶、子群、子群的阶、生成元及其求解算法；

明文消息如何进行编码、分组；

明文分组如何映射到有限域 GF(p)上的椭圆曲线的点；

利用 ECC 进行加解密时的公钥、私钥对生成算法；

利用 ECC 进行加密、解密；

二、教学目的和要求

1．知识目标

有限域 GF(p)上的椭圆曲线的点构成的 Abel 群的阶、子群、子群的阶、生成元的概念。

2．能力目标

利用 ECC 进行加密、解密时公钥、私钥对生成算法的编程实现；利用 ECC 对一段明文消息进行加密、解密的方法实现。

创新能力要求：实现一个工业级别的 ECC 加密、解密系统（难度较高）。

三、教学重点和难点

1．教学重点

有限域 GF(p)上的椭圆曲线的点构成的 Abel 群的阶、子群、子群的阶、生成元及其求解算法；利用 ECC 进行加解密时的公钥、私钥对生成算法；利用 ECC 进行加密、解密。

2．教学难点

明文消息如何进行编码、分组；明文分组如何映射到有限域 GF(p)上的椭圆曲线的点；

四、教学方法

理论、算法讲解+案例教学。理论包括很多数学基础 Abel 群的阶、子群、子群的阶、生成元，算法包括公钥私钥对生成算法、ECC 加密解密算法。通过具体的一段明文消息，讲解如何进行 encoding→block→mapping→encryption/decryption 的过程。

五、教学过程

1．导入内容：（1）ECC 的数学基础包括 Abel 群的阶、子群、子群的阶、生成元的相关总结。（2）如何理解椭圆曲线进行加密、解密呢？引入公钥、密钥对的生成算法中要利用循环子群、生成元、阶等。（3）导入 ECC 具体实现时，要涉及到明文 encoding→block→mapping→encryption/decryption 等过程。

2．讲授内容：

第 7 章 公钥密码体制

7.3 椭圆曲线加密算法

- ●有限域 GF(p)上的椭圆曲线的循环子群、生成元、生成元的阶
- ●基于给定有限域 GF(p)上的椭圆曲线的公钥、私钥对生成算法
- ●明文消息的编码方法
- ●明文消息的分组方法
- ●一个明文分组映射到椭圆曲线上的点的方法
- ●利用 ECC 加密算法过程
- ●利用 ECC 解密算法过程
- ●例题讲解

3. 作业：page 218:第 5 简答题第(8)、(9)题。

六、教学反思

现代密码学课程中椭圆曲线加密算法（ECC）要去 RSA 复杂多了，其中涉及到很多数学知识，增加了 ECC 的神秘性。另外要实现一个实用的 ECC 加密解密系统，还得鼓励学生阅读大量的课外资料。本次课程具有一定的授课难度。

七、参考资料：

（1）Elliptic-curve cryptography:
https://en.wikipedia.org/wiki/Elliptic-curve_cryptography
（2）椭圆曲线密码学：
https://zh.wikipedia.org/wiki/%E6%A4%AD%E5%9C%86%E6%9B%B2%E7%BA%BF%E5%AF%86%E7%A0%81%E5%AD%A6
（3）C++ Elliptic Curve library beta：
https://sourceforge.net/projects/libecc/files/
（4）在线加解密工具：http://tool.chacuo.net/cryptdes

No.16 数字签名技术（1/2）

教案设计

教师姓名： 方贤进

单　　位： 计算机科学与工程学院

课程名称： 现代密码学

适用对象： 信息安全本科专业

数字签名技术教案设计（1/2）

一、教学内容

数字签名的概念；数字签名的安全要求；数字签名算法应满足的要求；数字签名方案的组成；数字签名的过程；数字签名的模型；直接方式数字签名方案；带仲裁的数字签名方案。

二、教学目的和要求

1．知识目标

数字签名的概念的掌握；数字签名的过程；数字签名的模型。

2．能力目标

专业能力：数字签名模型是实际中的应用，例如收发电子邮件的双方对邮件进行签名。

创新能力：利用 PGP 对电子邮件签名与加密的方案与实现。

三、教学重点和难点

1．教学重点

数字签名的概念；数字签名方案的组成；数字签名的过程；数字签名的模型。

2．教学难点

数字签名的过程及模型。

四、教学方法

讲授法、讨论法（主要讨论在现实中通信的双方出现了发送方的抵赖、接收方的伪造的争论，如何解决？）

五、教学过程

（1）课程导入

现实和传统中用于表示“确认”的手写签名，如写信、签订协议、支付、文件批复等，特点是防伪造和抵赖。

数字签名是电子信息技术发展的产物，是针对电子文档的一种签名确认方法，所要达到的目的是：对数字对象的合法化、真实性进行标记，并提供签名者的承诺。随着信息技术的广泛使用，特别是电子商务、电子政务等快速发展，数字签名的应用需求越来越大。

（2）讲授内容

第 8 章 数字签名技术

- 数字签名简介
- 手写签名与数字签名的异同
- 数字签名的概念
- 数字签名的理解
- 数字签名的安全要求
- 数字签名的方案
- 数字签名的过程
- 数字签名的模型
- 直接方式的数字签名方案
- 带仲裁的数字签名方案
- 小结

（3）作业：page243，第 2 选择题（1）(2)（3）（4），第 3 填空题（1）（2）（3）（4）（6），第 4 题术语解释（1）。

六、教学反思

本次课程主要讲授的概念、模型、方案等，相对比较枯燥，但结合具体的应用能起到一定的效果，例如：布置一个课外题目，让学生利用 PGP 实现电子邮件的签名与加密的应用平台。

七、参考资料

（1）Digital signature, https://en.wikipedia.org/wiki/Digital_signature

（2）数字签名，

https://baike.baidu.com/item/%E6%95%B0%E5%AD%97%E7%AD%BE%E5%90%8D

No.17 数字签名技术（2/2）

教案设计

教师姓名： 方贤进

单　　位： 计算机科学与工程学院

课程名称： 现代密码学

适用对象：信息安全本科专业

数字签名技术教案设计（2/2）

一、教学内容

RSA 数字签名方案；RSA 数字签名方案正确性证明；RSA 数字签名方案的安全性。

ECC 数字签名方案；ECC 数字签名方案正确性证明；ECC 数字签名方案的安全性。

二、教学目的和要求

1．知识目标

分别掌握 RSA、ECC 数字签名方案中的签名算法、验证签名算法。

2．能力目标

专业能力：RSA、ECC 数字签名方案中的签名算法、验证签名算法的实现与应用。

创新能力：RSA、ECC 数字签名方案的安全性分析。

三、教学重点和难点

1．教学重点

RSA、ECC 数字签名方案中的签名算法、验证签名算法。

2．教学难点

本次课无教学难点，RSA/ECC 数字签名方案的参数初始化、签名算法、验证签名算法相对比较容易理解。

四、教学方法

讲授法、案例法（通过例题说明 RSA/ECC 数字签名方案中的签名算法、签名的严重算法。）

五、教学过程

（1）课程导入：数字签名方案必须要靠算法实现，目前的数字签名算法包括 ElGamal 数字签名、Schnorr 数字签名、DSA 数字签名。由于时间关系，本次课程只讲解 RSA 数字签名方案、ECC 数字签名方案。

（2）讲授内容

第 8 章 数字签名技术

- RSA 数字签名方案初始化；
- RSA 数字签名算法

- RSA 数字签名算法验证
- RSA 数字签名算法正确性
- RSA 数字签名举例
- ECC 数字签名方案初始化；
- ECC 数字签名算法
- ECC 数字签名算法验证
- ECC 数字签名算法正确性
- ECC 数字签名举例

（3）作业：page245，第 5 简答题（1）（3）（4）（5）（6）。

六、教学反思

本次课程主要讲授的签名方案、算法、举例等，相对比较枯燥，但如果未来开发一个具体的通信双方发送短消息的签名系统（用 RSA 或 ECC 签名算法），可能会起到较好的效果。

七、参考资料

（1）Elliptic Curve Digital Signature Algorithm:
https://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm

No.18 密钥管理（1/2）

教案设计

教师姓名： 方贤进

单　　位： 计算机科学与工程学院

课程名称： 现代密码学

适用对象： 信息安全本科专业

密钥管理 教案设计（1/2）

一、教学内容

密钥管理简介；密钥的生命周期。

二、教学目的和要求

1．知识目标

掌握密钥管理的过程、目的、原则；密钥的层次结构；密钥的生命周期（生成、存储、建立、使用、备份/恢复、更新、存档/撤销/销毁）等相关知识。

2．能力目标

专业能力：能利用密钥管理的层次模型贯穿于应用系统的密钥管理中。

创新能力：能进行密钥交换协议的实现及安全性分析。

三、教学重点和难点

1．教学重点

密钥的层次结构；密钥的生命周期（生成、存储、建立、使用、备份/恢复、更新、存档/撤销/销毁）

2．教学难点

密钥管理系统的组成及实现技术。

四、教学方法

讲授法、读书指导法。

五、教学过程

（1）导入内容：密钥是密码系统中的可变部分。现代密码体制要求密码算法是可以公开评估的，整个密码系统的安全性并不取决对密码算法的保密或者是对密码设备等保护，决定整个密码体制安全性的因素是密钥的保密性。也就是说，在考虑密码系统的设计时，需要解决的核心问题是密钥管理问题，而不是密码算法问题，密钥管理是密码学许多技术（如机密性、实体身份验证、数据源认证、数据完整性和数据签名等）的基础，在整个密码系统中是极其重要的，密钥的管理水平直接决定了密码的应用水平。历史表明：从密钥管理途径窃取秘密要比单纯从破译密码算法窃取秘密所花费的代价要小得多。

因此密钥管理在整个安全系统中是多么的重要。

（2）讲授内容

第 10 章 密钥管理技术

10.1 密钥管理的简介

- 密钥管理的目的
- 密钥管理的原则
- 密钥的层次模型

10.2 密钥的生命周期

- 生成
- 存储
- 建立
- 使用
- 备份/恢复
- 更新
- 存档/撤销/销毁

（3）作业：page299，第 1 判断题（1）（2）（3）（4）（5），第 2 选择题（1）（2）（3）（4），第 3 题填空题（1）（3）（4），第 5 简答题（1）（2）（4）。

六、教学反思

本次课程主要讲授密钥管理的过程、目的、原则；密钥的层次结构；密钥的生命周期。内容相对抽象、枯燥。

七、参考资料

（1）维基百科•密钥管理（crytographic key management system）：https://zh.wikipedia.org/wiki/%E5%AF%86%E9%92%A5%E7%AE%A1%E7%90%86。

（2）下列是一些开放源代码或专有的密钥管理系统。

a) Barbican, the OpenStack security API.
b) KeyBox - web-based SSH access and key management.
c) EPKS - Echo Public Key Share, system to share encryption keys online in a p2p community.
d) Kmc-Subset137 - key management system implementing UNISIG Subset-137 for ERTMS/ETCS railway application.
e) privacyIDEA - two factor management with support for managing SSH keys.
f) StrongKey - open source, last updated on Sourceforge in 2013.
g) Vault - secret server from HashiCorp.

No.19 密钥管理（2/2）

教案设计

教师姓名： 方贤进

单　　位： 计算机科学与工程学院

课程名称： 现代密码学

适用对象：信息安全本科专业

密钥管理 教案设计（2/2）

一、教学内容

公钥数字证书、密钥分配、密钥协商、密钥托管。

二、教学目的和要求

1．知识目标

掌握公钥数字证书的结构及其管理、公钥基础设施 PKI 模型、密钥协商（交换）协议、密钥托管体制。

2．能力目标

专业能力：掌握公钥数字证书的结构、生命周期及使用；密钥分配的基本方法；掌握 Diffie-Hellman 密钥交换协议及改进，以防止中间人攻击。

创新能力：Diffie-Hellman 密钥交换协议及改进的算法实现与应用；各种密钥分配协议的实现及安全性分析。

三、教学重点和难点

1．教学重点

公钥数字证书的概念与结构；密钥分配方案及协议；密钥交换协议。

2．教学难点

Diffie-Hellman 密钥交换协议、漏洞、中间人攻击、协议的改进。

四、教学方法

讲授法、读书指导法（见参考资料）。

五、教学过程

（1）导入内容：证书类似现实生活中的个人身份证。身份证将个人的身份信息(姓名、出生年月日、地址和其他信息)同个人的可识别特征(照片或指纹)绑定在一起。个人身份证是由国家权威机关(公安部)签发的，该证件的有效性和合法性是由权威机关的签名或签章保障的，因此身份证可以用来验证持有者的合法身份的信息，称为验证身份鉴定。

公钥密码体制中，由于公钥是公开的、非保密的，因此一个最大问题就是要确保获得对方公钥的身份。例如 A 要发送消息 M 给 B，并保证机密性，则 A 用 B 的公钥对 M 进行加密后获得 M’再发送给你 B，如果 B 的身份被 C 冒充，则 A 发送的消息尽管被加密了，但由于是用 C 的公钥进行了加密，C 仍然能够对加密后的消息进行解密。

因此公钥数字证书在实际应用中非常重要。

（2）讲授内容

第 10 章 密钥管理技术

10.3 公钥证书

10.4 密钥分配

10.5 密钥协商

10.6 密钥托管

（3）作业：page299，第 1 判断题（13）~（17），第 2 选择题（7）~（12），第 4 题术语解释（1）（4）（5），第 5 简答题（6），第 6 综合应用题。

六、教学反思

本次课程把密钥分配协议、密钥交换协议作为教学的重点，因为在一个安全系统中这些过程起着非常重要的作用。如果密钥分配协议、密钥交换协议中有安全漏洞，则后果非常严重。但此部分内容的讲授理论性较强，如果用算法模拟实现则比较完美。

七、参考资料

（1）Diffie－Hellman key exchange:
https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange

（2）Key-agreement protocol:
https://en.wikipedia.org/wiki/Key-agreement_protocol

No.20 复习、总结

教案设计

教师姓名： 方贤进

单　　位： 计算机科学与工程学院

课程名称： 现代密码学

适用对象： 信息安全本科专业

复习、总结 教案设计

一、教学内容

复习、总结本门课程的重点。

二、教学目的和要求

1．知识目标

总结古典密码学的两种方法：置换与代换，掌握现代密码学中的分组加密算法 DES/AES 的执行过程；流密码的思想及主要算法；hash 函数 MD5 算法及在消息认证中的应用；公钥密码体制的思想以及 RSA、ECC 算法的执行过程；数字签名的方案与模型及 RSA/ECC 数字签名算法；密钥管理的含义、数字证书、密钥分配协议与密钥交换协议等。

2．能力目标

专业能力：掌握现代密码学中的基本思想与算法。

创新能力：在一个系统中利用现代密码学的思想解决工程应用中的机密性问题、完整性问题、抗否认性、认证性问题。

三、教学重点和难点

1．教学重点

现代密码学中的基本概念、理论、模型、方法、算法的复习与总结。

2．教学难点

安全性分析部分的复习和总结、ECC 加密算法的计算过程等。

四、教学方法

讲授法。

五、教学过程

（1）导入内容：无

（2）讲授内容：现代密码学中的基本概念、理论、模型、方法、算法的复习与总结。

（3）作业：无

六、教学反思

七、参考资料

无