应用密码学基础

理论理解与实践 (Lecture Notes)

作者：李晓峰 (cy_lxf@163.com)

组织：北京联合大学智慧城市学院

时间：June 30, 2025

版本：v6.8

课程主页:

http://uisu.gitee.io/lxf/

https://yes-uisu.github.io/lxf/

Victory won't come to us unless we go to it. — M. Moore

前　　言

2018 年学院成立了信息安全专业，同年开始第一次招生，2020 年春季学期开始上“现代密码学”一课，后将课程名称改为“密码学基础”，在备课中形成此讲义。内容是在参考已有教材的基础上，按照自己对课程理解组织而成，希望符合本科生的特点。

本科密码学重点应该使学生了解各类密码算法和协议设计的基本思想，了解密码发展的脉络，能够看懂设计好的密码算法，能够编程实现基本密码算法，了解常用的几种密码分析方法。同时学生也应该了解与密码应用有关的法律、法规、标准 (特别是一些评价和测评标准) 等内容。

在编写此讲义的过程中，基本思路，预期达到的目的是：

1. 学生能够通过查阅相关基础材料，看懂一个密码算法、协议。
2. 学生能够编程实现一个密码算法、协议。算法的实现应该是基本能力要求，所以在授课中特别注意了实验课程的安排，本课程实验让学生通过码云（gitee）提交，主要是让同学们能够熟悉一些常用的工程工具。通过使用 GNU MP 库来实现基本算法，一是让学生了解如何使用第三方库来实现算法，二是没有用封装粒度更大的库，是想让学生了解一下算法底层实现细节。。
3. 学生了解常用的密码分析方法，并能够编程实现常见的分析算法。
4. 在讲义中有时会直接拷贝原始文献的内容，主要目的是想通过原始文献的内容，让学生更多了解、体会解决问题的思路和过程，而不是只了解结论。鼓励学生去看原始文献。考虑到由于时间的限制，阅读原始文献在语言上会对学生造成一定的障碍，产生找一些志愿者一起将经典文献翻译为中文的想法，目前已经翻译几篇，可公开下载，项目网页为http://uisu.gitee.io/infsecclat，或者 github 上的镜像https://yes-uisu.github.io/InfSecClaT/，欢迎大家参加。
5. 对密码相关法律、法规、标准 (特别是一些评价和测评标准) 有所了解。

在整理本书的过程中，我将觉得帮助大的资料直接放到本书里，并且给出了链接，这些资料在学习相关概念时应该有点帮助，有兴趣的同学可从这些点上扩展开来。

还有些资料没有放在正文里面，放在附录，这些资料的目的是希望能够扩展一下阅读，扩展启发一下思路，特别是对英文的一些术语有所了解，因为毕竟很多原始文献是来自于英文，在学习中积累一些专业词汇，有利于大家后面开展深入研究。

我在讲此课时的内容编排，可以看我的课程网页https://uisu.gitee.io/lxf/moderncrypto.html，或者 github 上的镜像https://yes-uisu.github.io/lxf/moderncrypto.html

本讲义的 PDF 格式的最新版可以从课程主页下载。为了方便大家在讲课、学习中使用本讲义，本讲义的 tex 文件上传到码云上 (https://gitee.com/uisu/modern_cryptography_free_book)，希望对大家有所帮助。

这本书也期望能够和上类似课的老师进行交流，这门课的理论作业和编程作业、编程作业评价标准也同时共享，通过几年的教学实践，让学生用 C 语言的标准库动手实现一些基本算法，对于学习者对算法理解和能力的培养很有帮助。

另外，我把每次上课的录音上次到 B 站，希望对一些学习者有点帮助，共享其中一个录音的链接：https://www.bilibili.com/video/BV1QdfFYrEAP/，其他的可以在我这个号里找。

由于水平有限，在整理此讲义过程中，难免会出现错误，请大家不吝赐教。

邮箱：cy_lxf@163.com

2025 年 4 月

致　　谢

首先，非常感谢沈晋慧老师在本门课程的建设和教学过程中提供的帮助。

其次列出对讲义提出修订意见并被采纳的人员名单：

2025.4.23 万柏麟 (北京联合大学信息安全专业 2023 级)，林沐阳 (北京联合大学信息安全专业 2023 级) 发现“公钥密码”章节的“背包加密方案”例 6.3 和例 6.4 答案有误，已经修正。

目　　录

1 引言 **1**

1.1 信息 (information) 的定义 1
1.2 一个具体的信息传输实例 2
1.3 Information vs. Message 3
1.4 数据 (data) 4
1.5 编码 (coding) 5
1.6 计算机字符显示分析示例 7
1.6.1 信息的表达 7
1.6.2 字母和数字的计算机内编码 7
1.6.2.1 ASCII 编码表还编码了什么字符 7
1.6.2.2 汉字编码 8
1.6.2.3 如何知道字符编码 8
1.6.3 字符在计算机屏幕上如何显示 9
1.6.3.1 如何解释同一个字符有不同字体（宋体、黑体） . 9
1.6.4 字体的显示方式如何编码 9
1.6.4.1 直接描述点阵 9
1.6.4.2 描述轮廓 10
1.6.4.3 两种方式的区别 10
1.6.4.4 如何编辑字体 10
1.6.4.5 对于新造的字如何输入 11
1.6.5 字符的输入编码 12
1.6.5.1 汉字输入 12
1.6.6 为什么搞这么多编码 12
1.7 信息的度量 12
1.8 何为安全 13
1.8.1 安全威胁 (threats) 16
1.9 信息安全模型 (Information Security Model) 17
1.9.1 保密通信模型 (Secret Communication Model) 17
1.9.2 BLP 模型 18
1.9.3 Biba 模型 19
1.9.4 RBAC 20

1.10 柯克霍夫斯原则 20
1.11 密码系统的安全概念 21
1.11.1 完全保密 (Perfect secrecy) or 香农安全 (Shannon Security) . . 21
1.11.1.1 完全保密 (Perfect secrecy) 21
1.11.1.2 一次一密（one-time pad） 23
1.11.2 可证明安全 (Provable Security) 23
1.11.3 语义安全 (Sematic Security) 26
1.11.3.1 攻击游戏 (attack game) 26
1.11.3.2 语义安全定义 27
1.12 加密的常识 27
第 1 章 习题 28

2 密码学研究内容 29
2.1 密码设计 29
2.1.1 密码体制 29
2.1.2 基于计算困难问题的密码体制设计 30
2.1.3 常见的密码困难假设 (Common cryptographic hardness assumptions) 33
2.2 密码分析 34
2.3 密码测评 34
第 2 章 习题 35

3 古典密码 (Classical Encryption) 36
3.1 简单替换密码 (Simple Substitution Cipher)[1] 36
3.2 换位 (固定周期 d)(Transposition (Fixed Period d))[1] 36
3.3 凯撒密码 (Caesar cipher) 37
3.4 移位变换 (shift transformation)/加法密码 37
3.5 Vigenère 及其变种 (Vigenère and Variations)[1] 38
3.6 乘法密码 (multiplication cipher) 39
3.7 仿射变换 (affine transformation) 39
3.8 多表代换密码 (polyalphabetic substitution cipher) 39
3.8.1 游乐场密码 (The Playfair Cipher)[1] 40
3.8.2 自动密钥密码 (Autokey Cipher)[1] 40
第 3 章 习题 40

4 流密码 (Stream Ciphers) 43
4.1 基本概念 44

4.2 密钥的产生 . . . 45
4.2.1 线性同余发生器 LCG(Linear Congruential Generator) . . . 46
4.2.2 线性反馈移位寄存器 LFSR(Linear Feedback Shift Register) . 49
4.2.2.1 有限域上的多项式 . . . 51
4.2.2.2 生成函数 (Generating Function) . . . 59
4.2.2.3 LFSR 的多项式表示 . . . 60
4.2.2.4 LFSR 的矩阵表示 . . . 65
4.3 序列的伪随机性 . . . 66
4.4 伪随机序列名称的由来 [2] . . . 68
4.5 流密码的一种分类 . . . 69
4.6 m 序列的破解 . . . 70
4.7 非线性序列 . . . 75
4.7.1 Geff 发生器 . . . 76
4.8 RC4 . . . 76
4.9 流密码的应用 . . . 76
第 4 章 习题 . . . 77

5 分组密码 (Block Ciphers) 78
5.1 Feistel 结构 . . . 78
5.2 SPN 结构 . . . 82
5.3 DES . . . 84
5.3.1 初始置换 IP . . . 84
5.3.2 轮结构 f 函数 . . . 86
5.3.3 密钥生成 . . . 88
5.3.3.1 置换选择 1(PC-1) . . . 88
5.3.3.2 置换选择 2(PC-2) . . . 90
5.3.3.3 密钥左循环移位 . . . 90
5.3.4 解密 . . . 90
5.4 2DES . . . 91
5.5 3DES . . . 91
5.6 填充 . . . 92
5.6.1 NoPadding . . . 92
5.6.2 PKCS5Padding . . . 92
5.6.3 ISO 10126 padding . . . 92
5.6.4 Zero padding . . . 92
5.7 分组密码的运行模式 . . . 93

5.7.1 电码本模式 (Electronic Code Book)/ECB 模式 93
5.7.2 密码分组链接模式 (Cipher Block Chain)/CBC 模式 94
5.7.3 密码反馈模式 (Cipher Feedback)/CFB 模式 95
5.7.4 输出反馈模式 (Output Feedback)/OFB 模式 97
5.7.5 计数模式 (Counter Mode)/CTR 模式 97
5.8 ZUC 99
5.9 SM4 101
5.9.1 轮函数 F 101
5.9.2 密钥扩展 102
5.9.3 加密过程 103
5.9.4 解密过程 103
第 5 章 习题 104

6 公钥密码体制 (Public Key Cryptography) 105
6.1 陷门单向函数 (trap-door one-way function) 106
6.2 MH 方法 [3] 109
6.2.1 0-1 背包问题 (0-1 Knapsack Problem) 109
6.2.2 MH 方法 111
6.2.2.1 陷门单向函数构造 111
6.2.2.2 加解密方法 112
6.2.2.3 签名方法 113
6.2.3 背包问题求解的发展 117
6.3 RSA 118
6.3.1 RSA 依赖的困难问题 118
6.3.2 RSA 加密方法 118
6.3.2.1 RSA 解密过程证明 119
6.3.3 RSA 简单示例 120
6.3.3.1 生成公私钥对 120
6.3.3.2 用公钥加密字符串 121
6.3.3.3 用私钥解密密文 121
6.3.3.4 用私钥简单签名字符串 122
6.3.3.5 用公钥验证字符串 122
6.3.4 公私钥对的生成 122
6.4 ECC(Elliptic Curve Cryptography) 123
6.4.1 基本概念 123
6.4.2 有限域上的椭圆曲线 126

6.4.3 构造密码算法 . . . 130
6.4.3.1 消息到椭圆曲线上的映射 . . . 130
6.4.3.2 椭圆曲线上的计算困难问题 . . . 130
6.4.3.3 椭圆曲线上的密码算法 . . . 130
第 6 章 习题 . . . 131

7 密码学哈希函数 (Cryptographic Hash Function) 134
7.1 哈希函数特点 . . . 134
7.2 对哈希函数的攻击 . . . 135
7.2.1 穷举攻击 . . . 135
7.2.2 生日攻击 (birthday attack) . . . 135
7.3 Merkle-Damgård 结构 . . . 137
7.4 MD5(Message-Digest algorithm 5) . . . 137
7.4.1 MD5 算法 . . . 137
7.4.1.1 消息填充 . . . 137
7.4.1.2 附加消息长度 . . . 138
7.4.1.3 缓冲区初始化 . . . 138
7.4.1.4 分组流水处理 . . . 138
7.4.1.5 输出 . . . 139
7.4.1.6 MD5 算法表示 . . . 139
7.4.2 核心算法 H_{MD5} . . . 139
7.4.2.1 H_{MD5} 算法 . . . 139
7.4.2.2 四轮运算 R . . . 139
7.4.2.3 R 中的 $M_i^n, (n = 1, 2, 3, 4)$ . . . 141
7.4.2.4 R 中的 $s_i^n, (n = 1, 2, 3, 4)$ . . . 141
7.4.2.5 R 中的 t_i . . . 141
7.4.2.6 核心运算 . . . 142
7.4.2.7 非线性函数 . . . 142
7.5 MD5 安全性 . . . 142
7.5.1 History and cryptanalysis . . . 142
7.5.2 security . . . 144
7.6 海绵结构 (Sponge Construction) . . . 145
7.7 SHA . . . 146
7.7.1 SHA-1 . . . 146
7.7.1.1 Introduction . . . 146
7.7.1.2 BIT strings and integers . . . 147

7.7.1.3 Operations on Words 148
7.7.1.4 Message Padding 148
7.7.1.5 Functions Used 150
7.7.1.6 Constants Used 150
7.7.1.7 Computing the Message digest 150
7.7.1.8 Alternate method of computation 151
7.7.2 SHA-1 的破解 152
7.7.2.1 王小云院士的十年一剑 152
7.7.2.2 进一步崩盘 153
第 7 章 习题 154

8 消息认证码 (Message Authentication Code) 156
8.1 MAC 函数要求 157
8.2 基于 DES 的 MAC 158
8.3 基于哈希函数的 MAC(HMAC) 159
8.3.1 HMAC 的安全目标 159
8.3.2 HMAC 方法 160
8.3.2.1 认证密钥 160
8.3.2.2 HMAC 计算过程 160
第 8 章 习题 161

9 密钥管理 (Key Management) 162
9.1 密钥分发 (key distribution) 的基本方法 172
9.1.1 有中心的密码分发 172
9.1.2 无中心的密钥分发 173
9.2 Diffie-Hellman 密钥交换 175
9.2.1 DH 中间人攻击 175
9.3 密钥分割 177
9.3.1 Shamir 门限方案 177
9.3.1.1 拉格朗日插值法 (Lagrange Interpolation Polynomial) 177
9.3.1.2 门限方案 178
9.3.2 CRT 门限方案 180
9.3.2.1 中国剩余定理 [4] 180
9.3.2.2 门限方案 180
第 9 章 习题 182

10 数字签名 (Digital Signatures) 183
10.1 基于对称密钥算法的数字签名 . . . 183
10.2 数字签名的基本概念示例 . . . 184
10.3 证书实例 . . . 188
10.3.1 PKI 标准体系 . . . 189
10.3.2 证书服务公司 . . . 190
10.4 Https 实例 . . . 190
10.5 Https 标准 . . . 192
10.6 签名方案与标准 . . . 193
10.6.1 DSS . . . 193
10.6.1.1 DSA . . . 195
10.6.1.2 RSA ds algorithm . . . 196
第 10 章 习题 . . . 197

11 安全服务和安全机制 (Security Services & Mechanisms) 198
11.1 密码学支撑的安全服务 (Security Services) . . . 199
11.2 密码算法 (Cryptographic Algorithm) . . . 200
11.3 OSI 7 层模型与安全服务与机制 . . . 201
11.3.1 安全服务 (Security Services) . . . 201
11.3.1.1 鉴别 (authentication) . . . 201
11.3.1.2 访问控制 (access control) . . . 202
11.3.1.3 数据机密性 . . . 202
11.3.1.4 数据完整性 . . . 202
11.3.1.5 抗抵赖 . . . 203
11.3.2 特定的安全机制 (Specific security mechanisms) . . . 203
11.3.2.1 加密 . . . 203
11.3.2.2 数字签名机制 . . . 204
11.3.2.3 访问控制机制 . . . 204
11.3.2.4 数据完整性机制 . . . 205
11.3.2.5 鉴别交换机制 . . . 205
11.3.2.6 通信业务填充机制 . . . 206
11.3.2.7 路由选择控制机制 . . . 206
11.3.2.8 公证机制 (Notarization) . . . 206
11.3.3 普遍安全机制 (Pervasive security mechanisms) . . . 206
11.3.3.1 可信功能度 (trusted functionality) . . . 207
11.3.3.2 安全标记 . . . 207

11.3.3.3 事件检测 207
11.3.3.4 安全审计跟踪 208
11.3.3.5 安全恢复 208
11.3.4 安全服务与安全机制间关系的实例 (Illustration of relationship of security services and mechanisms) 209
11.3.5 安全服务与层的关系的实例 (Illustration of the relationship of security services and layers) 209

12 协议 (Protocols) 210
12.1 零知识协议 (Zero-knowledge Protocol) 210
12.1.1 零知识协议的形象例子 [3] 211
12.1.2 Schnorr 识别协议 (Schnorr Identification Protocol) 212
12.2 认证协议 (Authentication protocol) 212
12.2.1 Needham-Schroeder 213
12.2.1.1 基于对称密钥体制的 Needham-Schroeder(Needham-Schroeder Symmetric Key Protocol) 213
12.2.1.2 基于公钥密码体制的 Needham-Schroeder(Needham-Schroeder Public-Key Protocol) 214
12.2.1.3 安全性分析 215
12.3 智力扑克 215
12.3.1 SRA 方案 [3] 215
12.4 kerberos 协议 & 系统 217
12.5 Windows Logon 219
12.6 TLS/SSL 219
12.7 IPv6 220
12.8 5G AKA 220

13 协议的安全分析 222
13.1 BAN 逻辑 [3] 222
13.1.1 基本概念 222
13.1.2 逻辑公设 222
13.1.3 推理步骤 224
13.1.4 分析 Needham-Schroeder 协议 224
13.1.4.1 初始假设集合 224
13.1.4.2 理想化协议模型 225
13.1.4.3 建立协议预期目标 225

13.1.4.4 利用初设和逻辑公设推理 225
13.1.4.5 推导出协议最终目标集合 228
13.1.4.6 讨论 228
13.2 逻辑编程和协议分析工具 228

14 安全多方计算 (Secure Multi-Party Computation) 230
14.1 姚的百万富翁方案 232
14.2 混淆电路协议 (Garbled circuit protocol) 234
14.2.1 不经意传输 (Oblivious Transfer (OT)) 237
14.3 同态加密 238
14.4 开源项目 239

15 比特币 (Bitcoin) & 区块链 (Block Chains) 241
15.1 比特币起源 241
15.2 技术发展脉络 241
15.2.1 账本 243
15.2.2 交易 (Transaction) 243
15.2.3 拜占庭协议 243
15.2.3.1 拜占庭将军问题 (The Byzantine Generals Problem) 243
15.2.3.2 拜占庭共识算法之 PBFT 249
15.2.4 挖矿原理 249
15.2.5 钱包 250
15.3 比特币 251
15.4 其他数字货币或虚拟货币 252
15.5 区块链 (block chains) 253
15.5.1 区块链的几种类型 254
15.6 开源系统 256

16 可信计算 (Trusted Computing) 257
16.1 可信平台模块 (TPM:Trusted Platform Module) 258
16.2 相关资源 264

17 量子计算 (Quantum Computing) 266
17.1 量子 (Quantum) 的提出 266
17.2 量子的态叠加 267
17.3 量子比特 267
17.4 量子计算 (Quantum Computing) 268

17.5 量子计算机发展过程 (至 2023 年) 269
17.5.1 量子计算机工作原理及实现模式 271
17.5.1.1 Qbit 的实现方法 271
17.5.1.2 量子计算的实现方法 272
17.5.1.3 量子计算现实中面临的主要问题 272
17.6 量子纠缠 (Quantum Entanglement) 273
17.7 “EPR”佯谬 274
17.8 量子隐形传态 (Quantum Teleportation) 275
17.9 量子通信 276

18 商用密码应用安全性评估简介 277
18.1 密码法中的评估要求 277
18.2 等保、密评与关基 278
18.3 密评的基本内容 279
18.4 密评的应用支撑标准 279
18.5 密评的配套测评文件 280

19 扩展阅读 282
19.1 姚期智——图灵奖的介绍 282
19.2 2021 年理论计算科学和离散数学领域学者获 Abel 奖 287
19.3 ZUC 288
19.3.1 密钥装载 289
19.3.2 初始化阶段 289
19.3.3 工作阶段 289
19.3.4 F 函数 290
19.3.5 ZUC 设计理念及准则 290
19.3.5.1 设计理念 290
19.3.5.2 设计准则 291
19.4 finite field 291
19.5 GF(2) 上的本原多项式 293
19.6 One way function 301
19.7 enigma 302
19.8 Dan Boneh,Cryptography I 302
19.9 各种安全模型 302
19.9.1 Bell-LaPadula model 303
19.9.2 ISO 安全模型 305

19.9.3 IATF 安全模型 (ISSE) 308
19.9.4 BS7799 PDCA 模型 308
19.10课程设计基本概念 308
19.10.1 课程设计的目的 308
19.10.2 课程设计的类型 308
19.10.2.1 学科为中心的课程设计 (subject-centered curriculum design) 308
19.10.2.2 学习者为中心的课程设计 (learner-centered curriculum design) 309
19.10.2.3 问题为中心的课程设计 (problem-centered curriculum design) 309
19.10.2.4 课程设计时的几点注意事项 309
19.11The Vernam Cipher 310
19.12工具 RSA-Tool 2 中的公私钥生成方法 310
19.13PEM, DER, CRT, and CER: X.509 Encodings and Conversions 313
19.13.1 What is OpenSSL? 313
19.13.2 PEM 313
19.13.3 DER 315
19.13.4 Convert PEM certificate with chain of trust to PKCS#7 319
19.13.5 Convert PEM certificate with chain of trust and private key to PKCS#12 319
19.13.6 Convert DER-encoded certificate with chain of trust and private key to PKCS#12 319

A 练习 **322**

B 课程参考分值分配 **323**

C 相关机构 **324**
C.1 国家密码管理局 324
C.2 密码行业标准化技术委员会 324
C.3 商用密码检测中心 325
C.4 中国密码学会 327

D 相关法律、条例、标准 **328**
D.1 基本概念 328
D.2 中华人民共和国网络安全法 328

D.3 中华人民共和国密码法 329
D.4 中华人民共和国反恐怖主义法 330
D.5 中华人民共和国电子签名法 331
D.6 国家商用密码管理条例 331
D.7 《GB/T 39786-2021 信息安全技术信息系统密码应用基本要求》国家标准 332
D.8 数据安全法 333
D.9 关键信息基础设施安全保护条例 333

E 代数基础 (Algrbra) 335
E.1 群、环、域 335
E.2 有限域的结构 335
E.2.1 有素数元素的有限域 335
E.2.2 有限域模不可约多项式 336
E.2.2.1 一个代数机构的多项式 336
E.2.2.2 用不可约多项式构造域 336
E.2.3 用多项式基构造有限域 336

F 概率的几个概念 337
F.1 古典概率 (Classical Probability) 337
F.2 条件概率 (Conditional Probability) 339
F.3 随机变量 (Random Variable) 340
F.3.1 离散随机变量 341

G 信息论的几个基本概念 343
G.1 基本概念 343
G.2 哈夫曼编码 (Huffman Coding) 344
G.3 熵的几个性质 345

术语表

中间人攻击 man-in-the-middle attack 一种拦截并有选择地修改通信数据以冒充通信中实体的攻击方法。

假冒攻击 masquerade attack 攻击者假冒用户，欺骗验证者的攻击方法。

假冒验证者攻击 verifier impersonation attack 攻击者假冒验证者，欺骗被验证者的攻击方法。

公钥 public key 非对称密码算法中可以公开的密钥。

分组密码算法 block cipher algorithm 将输入数据划分成固定长度的分组进行加解密的一类对称密码算法。

分组密码算法工作模式 block cipher operation mode 分组密码算法的使用方式，主要包括电码本工作模式（ECB）、密码分组链接工作模式（CBC）、密码反馈工作模式（CFB）、输出反馈工作模式（OFB）、计数器工作模式（CTR）等。

可认证 Authentication 提供某个实体（人或系统）的身份的保证。

唯密文攻击 ciphertext-only attack 一种密码分析者只拥有密文进行密码攻击的方法。

在线攻击 on-line attack 一种在协议进行过程中对交互数据进行窃听、篡改、替换、插入等的攻击方法。

字典攻击 dictionary attack 一种由可能的密钥或口令组成字典，遍历字典中的所有条目以猜测密钥或口令的攻击方法。

密文 ciphertext 加密后的数据。

密钥 key 控制密码算法运算的关键信息或参数。

密钥空间 key space 所有可能的密钥组成的集合。

对称密码算法 symmetric cryptographic algorithm 加密和解密使用相同密钥的密码算法。

差分密码分析 differential cryptanalysis 一种选择明文攻击，通过分析特定明文差分对相应的密文差分的影响，以获得可能性最大的密钥。

差分能量分析 differential power analysis（DPA） 一种密码分析方法，使用统计方法和纠错技术等对密码设备功耗的变化进行分析，以提取密钥的有关信息。

已知明文攻击 known-plaintext attack 一种利用大量互相对应的明文和密文进行分析的密码攻击方法。

序列密码算法 stream cipher algorithm 将明文逐比特/字符运算的一种对称密码算法。

抗抵赖性 non-repudiation 也称不可否认性，证明一个已经发生的操作行为无法否认的性质。

数字签名 digital signature 签名者使用私钥对待签名数据的杂凑值做密码运算得到的结果，该结果只能用签名者的公钥进行验证，用于确认待签名数据的完整性、签名者身份的真实性和签名行为的抗抵赖性。

数字证书 digital certificate 也称公钥证书，由证书认证机构（CA）签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及扩展信息的一种数据结构。按类别可分为个人证书、机构证书和设备证书，按用途可分为签名证书和加密证书。

数据完整性 data integrity 数据没有遭受以非授权方式所作的篡改或破坏的性质。

明文 plaintext 未加密的数据或解密还原后的数据。

机密性 confidentiality 保证信息不被泄露给非授权的个人、进程等实体的性质。

生日攻击 birthday attack 一种主要针对密码杂凑算法的攻击方法，试图找出两个具有相同杂凑值的消息（即找到一个碰撞）。

离线攻击 off-line attack 一种利用已经获取的数据进行分析的密码攻击方法。

私钥 private key 非对称密码算法中只能由拥有者使用的不公开密钥。

穷举攻击 exhaustive attack 通过尝试口令或密钥所有的可能值以获得真实口令或密钥的攻击方法。

线性密码分析 linear cryptanalysis 一种分析明文、密文和密钥之间的若干比特的线性关系进行密码攻击的方法。