

7.2	RSA 算法示例	123
7.2.1	密钥产生	123
7.2.2	加密解密	124

第三部分 PKI 之数字证书与私钥：网络身份证

第 8 章	公/私钥格式	126
8.1	RSA	126
8.2	SM2	128
第 9 章	数字证书格式	130
9.1	基本格式	130
9.1.1	证书域组成 (Certificate)	130
9.1.2	证书内容 (tbsCertificate)	130
9.2	标准扩展项	135
9.2.1	标准扩展项 (Standard Extensions)	135
9.2.2	专用互联网扩展项	145
9.3	国内扩展项	146
9.3.1	卫生系统专用扩展项	146
9.3.2	国内通用扩展项	147
第 10 章	数字证书分类	150
10.1	根据证书持有者分类	150
10.2	根据密钥分类	150
第 11 章	私钥与证书存储方式	152
11.1	证书保存形式	152
11.1.1	DER 文件形式	152
11.1.2	Base64 文件形式	154
11.1.3	PKCS#7 文件形式	154
11.1.4	Windows 证书库形式	155
11.2	私钥保存形式	157
11.2.1	PKCS#8 文件形式	158
11.2.2	PKCS#12 文件形式	158
11.2.3	Java Keystore 文件形式	160
11.2.4	密码设备形式	161
11.2.5	软件系统形式	162
第 12 章	私钥与证书访问方式	164
12.1	CryptoAPI	164

12.1.1	CryptoAPI 简介	164
12.1.2	使用证书	166
12.1.3	使用私钥	168
12.2	PKCS#11	172
12.2.1	PKCS#11 简介	172
12.2.2	使用证书	178
12.2.3	使用私钥	181
12.3	JCA/JCE	183
12.3.1	JCA/JCE 简介	183
12.3.2	使用证书	187
12.3.3	使用私钥	189
12.4	CNG	190
12.4.1	CNG 简介	190
12.4.2	使用证书	195
12.4.3	使用私钥	196
12.5	PC/SC	200
12.5.1	PC/SC 简介	200
12.5.2	使用证书	202
12.5.3	使用私钥	213
12.6	国密接口	213
12.6.1	国密接口简介	213
12.6.2	使用证书	215
12.6.3	使用私钥	217
第 13 章	实验二	222
13.1	RSA 公钥格式编码示例	222
13.1.1	ASN.1 描述与实例	222
13.1.2	DER 编码过程	222
13.2	数字证书格式编码示例	223
13.2.1	ASN.1 描述与实例	223
13.2.2	DER 编码过程	225
13.3	Windows 证书库操作示例	229
13.3.1	查看证书库内容	229
13.3.2	导入证书	230
13.3.3	导出证书	233
 第四部分 PKI 之 CA 与 KMC: 管理网络身份证		
第 14 章	系统结构	236
14.1	国际标准	236

14.2 国内标准	237
14.2.1 证书认证系统 CA	237
14.2.2 密钥管理系统 KMC	239
第 15 章 系统设计	241
15.1 证书认证系统 CA	241
15.1.1 用户注册管理系统 RA	241
15.1.2 证书/CRL 签发系统	242
15.1.3 证书/CRL 存储发布系统	243
15.1.4 证书/CRL 查询系统	244
15.1.5 证书管理系统	245
15.1.6 安全管理系统	245
15.2 密钥管理系统 KMC	246
15.3 企业级 CA 总体设计示例	248
15.3.1 技术路线选择	248
15.3.2 模块设计	250
15.3.3 数据库设计	251
15.3.4 双证书技术流程设计	253
第 16 章 对外在线服务	256
16.1 OCSP/SOCSP 服务	256
16.1.1 OCSP	256
16.1.2 SOCSP	258
16.2 CRL 服务	259
16.2.1 基本域组成 (CertificateList)	259
16.2.2 CRL 内容 (tbsCertList)	260
16.2.3 CRL 扩展项 crlExtensions	262
16.2.4 CRL 条目扩展项 crlEntryExtensions	265
16.3 LDAP 服务	267
16.3.1 发布数字证书到 LDAP	267
16.3.2 访问 LDAP 获取数字证书	268
第 17 章 网络部署结构	270
17.1 运营型 CA	270
17.2 企业级 CA	273
17.2.1 双层标准模式	273
17.2.2 双层简化模式	273
17.2.3 单层单机模式	274
17.2.4 纯硬件模式	274

17.3 按企业管理模式部署 CA	276
17.3.1 单机构	276
17.3.2 集团公司+集中部署+集中发证	276
17.3.3 集团公司+集中部署+分布发证	277
17.3.4 集团公司+两级部署+分布发证	278
第 18 章 实验三	280
18.1 OpenSSL CA 示例	280
18.1.1 简介	280
18.1.2 安装配置	280
18.1.3 申请证书	284
18.1.4 生成并下载 CRL	287
18.1.5 导入 CA 证书到 IE 可信任证书库	290
18.2 EJBCA 示例	291
18.2.1 简介	291
18.2.2 安装配置	292
18.2.3 申请证书	300
18.2.4 下载 CRL	303
第五部分 PKI 之应用：使用网络身份证	
第 19 章 基本应用	308
19.1 身份认证	308
19.2 保密性	310
19.3 完整性	311
19.4 抗抵赖性	312
19.5 证书有效性验证	314
第 20 章 通用应用技术	315
20.1 SSL/TLS (Secure Socket layer/Transport Layer Security)	315
20.1.1 概述	315
20.1.2 记录协议	315
20.1.3 握手协议	316
20.1.4 警告协议	317
20.1.5 改变密码约定协议	318
20.1.6 应用数据协议	318
20.2 IPSec	318
20.3 Kerberos	323
20.4 TSP	326

20.5	SET	331
20.6	3-D Secure	333
20.7	WAP	335
20.8	S/MIMI	338
第 21 章	常见应用	345
21.1	防止假网站与 Web 服务器证书	345
21.1.1	假网站	345
21.1.2	使用 Web 服务器证书预防假网站	346
21.2	防止假软件与代码签名证书	348
21.2.1	Web 技术的发展	348
21.2.2	插件技术与假网银软件	350
21.2.3	使用代码签名证书预防假网银软件	351
21.3	网上银行系统	352
21.3.1	简介	352
21.3.2	应用安全需求	353
21.3.3	应用安全总体架构	354
21.4	网上报税系统	355
21.4.1	简介	355
21.4.2	应用安全需求	356
21.4.3	应用安全总体架构	356
21.5	电子病历系统	357
21.5.1	简介	357
21.5.2	应用安全需求	357
21.5.3	应用安全总体架构	359
21.5.4	网络部署结构	359
21.6	公交 IC 卡在线充值系统	361
21.6.1	简介	361
21.6.2	应用安全需求	361
21.6.3	应用安全总体架构	362
21.6.4	充值交易流程	362
第 22 章	实验四	365
22.1	Windows IIS 服务器证书配置	365
22.1.1	下载并安装服务器证书	366
22.1.2	配置 SSL 策略	373
22.1.3	访问 Web Server	374
22.2	Apache 服务器证书配置	375
22.2.1	下载并安装服务器证书	375