

CRYPTOGRAPHY'S  
ROLE  
IN  
SECURING THE  
INFORMATION  
SOCIETY

密码在信息社会里  
的安全保护作用

主编：Kenneth W. Dam 和 Herbert S. Lin

国家研究委员会

物理科学、数学和应用委员会  
计算机科学和电信委员会  
国家密码政策研究委员会

国家科学院出版社  
哥伦比亚特区华盛顿 1996 年

# 目录

执行摘要

本报告的篇章结构

## 第一部分——框定政策问题

- 第1章 信息时代日益严重的脆弱性（漏洞）
  - 1.1 信息时代的技术背景
  - 1.2 向信息社会过渡——不断增加的相互连接和相互依赖
  - 1.3 应对信息脆弱性
  - 1.4 企业和经济方面
    - 1.4.1 保护重要企业信息
    - 1.4.2 确保国家利用全球市场的能力
  - 1.5 个人和个人的隐私利益方面
    - 1.5.1 信息经济中的隐私
    - 1.5.2 公民的隐私权
  - 1.6 政府的特殊需要方面
  - 1.7 小结
- 第2章 密码：角色、市场和基础设施
  - 2.1 具体语境下的密码
  - 2.2 什么是密码？它能干什么？
  - 2.3 密码怎样适应大安全图景
    - 2.3.1 阻碍访问的因素
    - 2.3.2 方便信息访问的因素
  - 2.4 密码的市场
    - 2.4.1 密码市场的需求方
    - 2.4.2 密码市场的供应方
  - 2.5 广泛使用密码的基础设施
    - 2.5.1 密钥管理基础设施
    - 2.5.2 证书基础设施
  - 2.6 小结
- 第3章 访问被加密信息的需要
  - 3.1 词语解释
  - 3.2 执法：调查和起诉
    - 3.2.1 执法访问信息的价值
    - 3.2.2 管辖监视的法律框架
    - 3.2.3 执法监视需要的性质
    - 3.2.4 密码和新介质对执法的影响（存储和传输的数据）
  - 3.3 国家安全和信号情报
    - 3.3.1 信号情报的价值
    - 3.3.2 密码对信号情报的影响
  - 3.4 外交政策/国家安全与执法通信监视需要之间的异同
    - 3.4.1 相同点
    - 3.4.2 差异点

- 3.5 企业和个人对受保护信息的特例访问需要
- 3.6 对受保护信息的其他类型特例访问
- 3.7 小结

## 第二部分——政策手段

### 第4章 出口管制

- 4.1 当前出口管制简述
  - 4.1.1 出口管制的理由
  - 4.1.2 综述
  - 4.1.3 有关当前许可证制度的讨论
- 4.2 密码出口管制的效应
- 4.3 出口管制对美国信息技术供应商的影响
  - 4.3.1 对密码在国内使用的事实限制
  - 4.3.2 与出口管制相关的法规不确定性
  - 4.3.3 受影响的密码市场规模
  - 4.3.4 阻碍供应商响应用户需要
- 4.4 出口管制对美国经济和国家安全利益的影响
  - 4.4.1 对美国企业的直接经济伤害
  - 4.4.2 对美国信息技术领先地位的损害
- 4.5 政府/国家安全部门与供应商之间看法不一
- 4.6 技术数据出口
- 4.7 外交政策因素
- 4.8 技术-政策不匹配
- 4.9 小结

### 第5章 托管加密及相关问题

- 5.1 什么是托管加密?
- 5.2 支持托管加密的政府举措
  - 5.2.1 Clipper方案和托管加密标准
  - 5.2.2 Capstone/Forzezza方案
  - 5.2.3 放宽使用“被适当托管”的64位加密密钥的软件产品的出口管制
  - 5.2.4 其他联邦托管加密方案
- 5.3 托管加密的其他方法
- 5.4 托管加密对信息安全的影响
- 5.5 托管加密对执法的影响
  - 5.5.1 实现犯罪与起诉犯罪之间的平衡
  - 5.5.2 对执法访问信息的影响
- 5.6 强制与自愿使用托管加密
- 5.7 托管加密政策的制定过程
- 5.8 托管代理的隶属关系和数量
- 5.9 托管代理和托管加密用户的责任和义务
  - 5.9.1 分割托管信息
  - 5.9.2 托管代理的操作责任
  - 5.9.3 托管代理要担负的法律责任
- 5.10 保密的确保产品安全角色
  - 5.10.1 算法保密

- 5.10.2 产品设计和执行方案保密
  - 5.11 产品执行方案的硬件/软件之选
  - 5.12 生成单元密钥的责任
  - 5.13 与放宽64位托管加密软件出口管制的政府提案相关的问题
    - 5.13.1 “适当托管”的定义
    - 5.13.2 有关把密钥长度限制到64位或更64位以下的提案
  - 5.14 小结
- 第6章 国家密码政策的其他方面
- 6.1 通信执法协助法案
    - 6.1.1 《执法通信协助法案》简述和出台目的
    - 6.1.2 降低监听的资源要求
    - 6.1.3 未来获得数字流访问权
    - 6.1.4 信息服务供应商的《执法通信协助法案》豁免以及语音和数据服务的区别
  - 6.2 国家密码政策使用的其他工具
    - 6.2.1 联邦信息处理标准
    - 6.2.2 政府采购流程
    - 6.2.3 政策的执行：担心、不确定、疑惑、拖延、复杂性
    - 6.2.4 研发资金
    - 6.2.5 专利和知识产权
    - 6.2.6 与他国政府和各种机构的正式和非正式协议
    - 6.2.7 认证和评估
    - 6.2.8 非法定影响
    - 6.2.9 行政分支内的机构间协议
  - 6.3 联邦政府在信息安全方面的组织安排
    - 6.3.1 国家安全在民用信息基础设施中担任的角色
    - 6.3.2 影响信息安全的其他政府实体
  - 6.4 密码政策的国际维度
  - 6.5 小结

### 第三部分——政策选项、发现和建议

- 第7章 未来的政策选项
- 7.1 密码出口管制选项
    - 7.1.1 管制密码出口的选择维度
    - 7.1.2 完全取消密码出口管制
    - 7.1.3 把密码产品全部移交商品管制清单管辖
    - 7.1.4 最终用途审核
    - 7.1.5 根据其他国家的进出口政策逐国放宽管制并协调美国的密码出口管制政策
    - 7.1.6 弱默认模式强密码的自由出口
    - 7.1.7 密码应用编程接口的自由出口
    - 7.1.8 带加密性能可托管产品的自由出口
    - 7.1.9 海外托管代理政府认证的可选方案
    - 7.1.10 差分工作因子在密码中的使用
    - 7.1.11 把密码与美国军火清单上的其他项目分离
  - 7.2 提供被加密信息政府特例访问权的可选方案
    - 7.2.1 缺乏特例访问性能的密码的出售和使用禁令

- 7.2.2 将实施过程中使用密码的犯罪定性为刑事犯罪
  - 7.2.3 访问信息的非托管技术手段
  - 7.2.4 基于网络的加密
  - 7.2.5 在特例访问权上区别对待加密语音与数据通信服务
  - 7.2.6 用于政府特例访问的集中式解密设施
  - 7.3 迫在眉睫的问题
    - 7.3.1 不同加密级别对抗高质量攻击的充分性
    - 7.3.2 在国家层面组织美国政府提升信息安全的工作
  - 7.4 小结
- 第8章 汇总、发现和建议
- 8.1 汇总和发现
    - 8.1.1 信息脆弱性问题
    - 8.1.2 信息脆弱性的密码解决方案
    - 8.1.3 密码带来的政策困境
    - 8.1.4 信息时代的国家密码政策
  - 8.2 建议
  - 8.3 还需开展的额外工作
  - 8.4 结论

## 附录

- 附录A 国家研究委员会国家密码政策项目的贡献者（略）
  - A.1 委员会成员
  - A.2 项目的其他贡献者
- 附录B 词汇表
- 附录C 密码学简介
  - C.1 密码学的简短现代史
  - C.2 密码具备的能力
    - C.2.1 确保数据完整性
    - C.2.2 认证用户身份
    - C.2.3 不可否认性
    - C.2.4 保持保密性
  - C.3 密码的基本体系
  - C.4 针对密码系统的攻击
  - C.5 密码安全的元素
  - C.6 密码系统的预期寿命
    - C.6.1 背景
    - C.6.2 非对称密码系统
    - C.6.3 常规密码系统
    - C.6.4 计时攻击
    - C.6.5 Skipjack/Clipper/EES
    - C.6.6 警示
    - C.6.7 量子与DNA计算
    - C.6.8 椭圆曲线密码系统
    - C.6.9 量子密码
- 附录D 电子监视概述：历史和现状

- D.1 国内执法监视的法律框架
  - D.1.1 全面禁止电子监视
  - D.1.2 1968 年综合犯罪控制和安全街区法案（第 III 篇）和 1986 年电子通信隐私法案
  - D.1.3 外国情报监视法案
- D.2 电子监视历史回顾
- 附录E 密码政策简史
  - E.1 出口管制
  - E.2 学术研究和密码信息控制
  - E.3 商用密码
  - E.4 最近的发展
- 附录F 情报入门知识
  - F.1 情报的任务
  - F.2 情报的周期
    - F.2.1 规划
    - F.2.2 收集
    - F.2.3 处理
    - F.2.4 分析
    - F.2.5 传播
- 附录G 密码政策的国际范围
  - G.1 密码政策的国际维度
  - G.2 美国与其他国家的密码政策异同
  - G.3 对外出口管制制度
  - G.4 进口管制和使用控制
  - G.5 国际现状
  - G.6 争取安全通信政策方面的国际合作
  - G.7 国际密码政策的基本问题
    - G.7.1 密钥由谁持有？
    - G.7.2 密钥持有者在什么情况下可以把密钥发放给其他方？
    - G.7.3 各国怎样才能就密码的出口和使用达成一致的國際政策？
- 附录H 公钥基础设施重要要求汇总
- 附录I 不同行业的特有安全维度
  - I.1 银行和金融服务
  - I.2 医疗咨询和卫生保健
  - I.3 制造业
  - I.4 石油业
  - I.5 制药和化工业
  - I.6 娱乐业
  - I.7 政府
- 附录J 无保护信息风险举例
  - J.1 密码化解认证风险
  - J.2 密码化解保密性风险
  - J.3 密码化解认证和保密性两方面风险
  - J.4 密码化解数据完整性风险

附录K 密码应用编程接口

附录L 与密码政策相关的其他迫近的问题

L.1 数字现金

L.1.1 匿名和犯罪活动

L.1.2 公众的信任

L.1.3 征税

L.1.4 资金跨境流动

L.2 密码保护知识产权

附录M 联邦信息处理标准

附录N 与密码相关的法律、文件和条例

N.1.1 法律

N.1.1 有线和电子通信监听及口头通信监听  
(美国法典第18篇第119章)

N.1.2 外国情报监视  
(美国法典第50篇第36章)

N.1.3 笔式记录器和通信流分析  
(美国法典第18篇第121和206章)

N.1.4 1995年通信执法协助法案

N.1.5 1987年计算机安全法案

N.1.6 武器出口管制法案  
(美国法典第22篇第39章)

N.2 行政命令

N.2.1 第12333号行政命令(美国的情报活动)

N.2.2 第12958号行政命令(涉密国家安全信息)

N.2.3 第12472号行政命令(国家安全和应急防范职能的分配)

N.2.4 第42号国家安全指示令(国家安全电信和信息系统安全国家政策)

N.3 谅解备忘录和协议

N.3.1 国家安全局/国家标准和技术研究所谅解备忘录

N.3.2 国家安全局/联邦调查局谅解备忘录

N.3.3 国家安全局/高级研究项目局/国防信息系统局谅解备忘录

N.4 条例

N.4.1 国际武器贸易条例  
(《联邦法规》第22篇, 摘自第120-123、125、126部分)

N.4.2 出口管理条例

索引(略)

