
联邦政府

密码标准使用指南：

密码机制

内部资料

翻译：高卓

Elaine Barker
信息技术实验室计算机安全部

本出版物英文版可从以下网址免费获得：

<https://doi.org/10.6028/NIST.SP.800-175Br1>

2020 年 3 月



美国商务部
Wilbur L. Ross Jr., 部长
国家标准和技术研究所
Walter Copan, 商务部副部长兼 NIST 所长

北京江南天安科技有限公司

目录

第1章 介绍

- 1.1 概述和目的
- 1.2 适用对象
- 1.3 范围
- 1.4 背景
- 1.5 术语和定义
- 1.6 缩略语
- 1.7 篇章结构

第2章 标准和指南

- 2.1 标准的好处
- 2.2 联邦信息处理标准和特别出版物
 - 2.2.1 FIPS 和 SP 的采用
 - 2.2.2 NIST 跨机构或内部报告
 - 2.2.3 FIPS 豁免
- 2.3 其他标准组织
 - 2.3.1 美国国家标准学会 (ANSI)
 - 2.3.2 电气和电子工程师协会 (IEEE) 标准协会
 - 2.3.3 互联网工程任务组 (IETF)
 - 2.3.4 国际标准化组织 (ISO)
 - 2.3.5 可信计算组织 (TCG)

第3章 密码算法

- 3.1 密码散列函数
- 3.2 对称密钥算法
 - 3.2.1 块密码算法
 - 3.2.2 基于散列的对称密钥算法
- 3.3 非对称密钥算法
 - 3.3.1 数字签名算法
 - 3.3.2 密钥建立方案
- 3.4 算法的安全强度
- 3.5 算法的寿命

第4章 密码服务

- 4.1 数据保密性
- 4.2 数据完整性、身份认证和源认证
 - 4.2.1 散列函数
 - 4.2.2 消息认证码算法
 - 4.2.3 数字签名算法
- 4.3 块密码操作模式中保密性和认证的结合
- 4.4 随机位生成
- 4.5 对称密码与非对称密码

第5章 密钥管理

- 5.1 密钥管理通用指南
 - 5.1.1 密钥管理建议
 - 5.1.2 密码模块的安全要求
 - 5.1.3 向新的密码算法和密钥长度转换
- 5.2 密码密钥管理系统
 - 5.2.1 密钥管理框架
 - 5.2.2 密钥管理系统轮廓
 - 5.2.3 公钥基础设施
- 5.3 密钥建立
 - 5.3.1 密钥生成
 - 5.3.2 密钥派生
 - 5.3.3 密钥协定
 - 5.3.4 密钥传输/密钥分发
 - 5.3.5 密钥封装
 - 5.3.6 从口令派生密钥
- 5.4 密钥管理问题
 - 5.4.1 人工密钥建立对自动化密钥建立
 - 5.4.2 挑选和运行 CKMS
 - 5.4.3 保存和保护密钥
 - 5.4.4 密码有效期
 - 5.4.5 使用通过了验证的算法和密码模块
 - 5.4.6 密钥材料控制
 - 5.4.7 破解
 - 5.4.8 问责和存货管理
 - 5.4.9 审计

第 6 章 其他问题

- 6.1 被要求的安全强度
- 6.2 互操作性
- 6.3 当算法不再被批准时

参考文献

- NIST 出版物
- 非 NIST 出版物

