
向使用新的 密码算法和密钥长度过渡

内部资料

翻译：高卓

Elaine Barker

Allen Roginsky

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.800-131Ar2>

2019 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

目录

1. 介绍
 - 1.1 背景和目的
 - 1.2 可帮助理解本建议的有用术语
 - 1.2.1 安全强度
 - 1.2.2 通用定义和缩略语
 - 1.2.3 有关批准状态的词语的定义
 2. 使用块密码算法的加密和解密
 3. 数字签名
 4. 随机位生成
 5. 使用 Diffie-Hellman 和 MQV 的密钥协定
 6. 使用 RSA 的密钥协定和密钥传输
 7. 密钥包装
 8. 从密码密钥派生附加密钥
 9. 散列函数
 10. 消息认证码 (MACS)
- 附录 A 参考文献