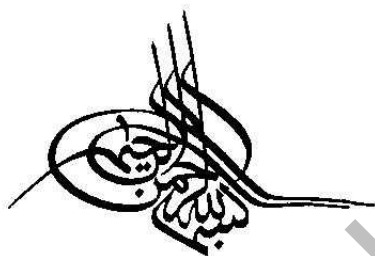


۱۵۷۰۴۳۱



تکنیکهای رمزنگاری

نویسندگان:

مهندس محمدتقی فرامرزی - رضا فتاحی

فهرست مطالب

۱. رمزنگاری و رمزگشایی / ۵
۲. رمزنگاری متقارن / ۶
۳. استاندارد رمزنگاری داده (DES) / ۷
 - ۱-۱. الگوریتم / ۷
 - ۲-۲. حالت بازخورد رمز (CFB) / ۹
 - ۳-۳. DES و محدودیت‌های صادراتی ایالات متحده / ۱۰
 - ۲-۲. DES، فایده / ۱۱
 - ۲-۲. IDEA / ۱۳
 - ۳-۳. IDEA، فایده / ۱۴
 - ۲-۴. استاندارد رمزنگاری داده (AES) / ۱۵
 - ۲-۴. Rijndael / ۱۶
 - ۲-۴. تبدیل‌های دور / ۱۶
 - ۲-۵. RC2, RC4 و RC5 / ۱۷
 - ۲-۵. RC6 / ۱۸
 - ۲-۵. رمزنگاری و رمزگشایی / ۱۹
۳. فشرده کردن پیام یا هش کردن / ۲۰
 - ۱-۲۳. MD5 / ۲۳
 - ۲-۲۳. الگوریتم هش امن (SHA) / ۲۳
 ۴. Kerberos / ۲۳
۴. بررسی اجمالی مدل Kerberos / ۲۴
 - ۲-۴. به دست آوردن بلیط / ۲۶
 - ۳-۴. درخواست سرویس / ۲۶
 ۵. رمزنگاری کلید عمومی یا نامتقارن / ۲۷

- ۵-۱. ویژگی‌های سیستم رمزنگاری کلید عمومی / ۲۸
- ۵-۲. توابع یک طرفه در بچه‌ای / ۲۹
- ۵-۳. استفاده از سیستم‌های رمزنگاری کلید عمومی برای احراز هویت / ۲۹
۶. امضای دیجیتال و بسته بندی / ۳۰
۷. RSA / ۳۲
۸. رمزنگاری منحنی بیضوی / ۳۴
۹. زیرساخت کلید عمومی (PKI) / ۳۵
- ۹-۱. گواهی‌ها / ۳۵
- ۹-۲. مراجع صدور گواهی / ۳۶
- ۹-۳. گواهی‌های اختیاری / ۳۸
۱۰. اطلاعات امنیتی / ۴۰
- ۱۰-۱. تبادل نحوی انتزاعی (ASN.1) / ۴۰
- ۱۰-۲. احراز هویت دایرکتوری X.509 / ۴۳
- ۱۰-۳. گواهی‌های X.509 / ۴۴
- ۱۰-۳. قواعد نحوی رمزنگاری پیام PKCS / ۴۶
۱۱. امضاهای دوگانه / ۴۷
۱۲. شماره‌ی یکبار مصرف / ۴۹
۱۳. امضای کور / ۵۰
۱۴. کارت‌های تراشه دار / کارت‌های هوشمند / ۵۱
- ۱۴-۱. انواع کارت / ۵۴
- ۱۴-۲. انواع حافظه و ظرفیت آن‌ها / ۵۵
- ۱۴-۳. مشخصات فیزیکی / ۵۷
- ۱۴-۴. امنیت / ۵۷
- ۱۴-۵. قابلیت‌های پردازش کلید عمومی / ۵۸
- ۱۴-۶. کارت‌های چند منظوره / ۵۹
- ۱۴-۷. جاوا کارت / ۵۹
- ۱۴-۸. MULTOS / ۶۱
- ۱۴-۹. ناظران / ۶۳
- مراجع / ۶۵