

Хорев П. Б.

Криптографические интерфейсы и их
использование. -М.: Горячая линия-Телеком, 2007. -
278 с: ил.

Оглавление

Предисловие

Введение

Глава 1. Основы современной криптографии

- 1.1. Симметричная и асимметричная криптография
- 1.2. Электронная цифровая подпись и функции хеширования
- 1.3. Инфраструктура открытых ключей
- 1.4. Принципы построения и использования криптографического интерфейса Windows (CryptoAPI)

Глава 2. Использование базовых криптографических функций. CryptoAPI 1.0

- 2.1. Обзор функций CryptoAPI 1.0
- 2.2. Получение информации о криптопровайдерах
- 2.3. Создание, хранение и распространение криптографических ключей
- 2.4. Шифрование и расшифрование данных
- 2.5. Получение и проверка электронной цифровой подписи
- 2.6. Управление доступом к контейнеру ключей

Глава 3. Использование криптографических функций для работы с сертификатами CryptoAPI 2.0

- 3.1. Обзор функций CryptoAPI 2.0
- 3.2. Работа с хранилищами сертификатов
- 3.3. Получение информации о сертификатах
- 3.4. Шифрование и расшифрование сообщений
- 3.5. Получение и проверка хеш-значений и электронной цифровой подписи

Глава 4. Использование криптографических многокомпонентных объектов CAPICOM

- 4.1. Обзор объектов CAPICOM
- 4.2. Получение информации о криптопровайдерах
- 4.3. Работа с сертификатами и их хранилищами

- 4.4. Шифрование и расшифрование данных
- 4.5. Хеширование данных, получение и проверка электронной цифровой подписи
- 4.6. Запрос и получение сертификатов в удостоверяющем центре.

Глава 5. Системные программы для работы с сертификатами

- 5.1. Создание сертификатов
- 5.2. Создание списка доверенных сертификатов
- 5.3. Вычисление и проверка ЭЦП
- 5.4. Управление сертификатами
- 5.5. Получение сертификата в удостоверяющем центре

Список сокращений

Список литературы