CryptoBox

Приложение Windows Store для Windows 8

Приложение позволяет шифровать пользовательский текст с использованием симметричных алгоритмов шифрования.

Шифрование реализовано с использованием классов доступных в пространстве имен Windows.Security.Cryptography. Логика работы приложения реализована в классе Cryptobox в файле Cryptobox.cs, также в файле MainPage.xaml.cs

Возможность шифрования пользовательских файлов и интеграции со SkyDrive (в разработке)

Возможность хеширования пользовательской информации с использованием алгоритмов (в разработке):

- MD5

- SHA1

- SHA256

- SHA384

- SHA512

- ГОСТ Р 34.11-94 (возможно)

На данный момент реализована поддержка алгоритмов симметричного шифрования:

- AES

- DES

- TripleDES

- RC2

- RC4

В планах поддержка алгоритмов:

- ГОСТ 28147-89

- Threefish

- др.

Шифрование доступно в режимах:

- CBC (кроме RC4)

- ECB (кроме RC4)

Для блочных алгоритмов шифрования происходит дополнение блоков открытого текста по стандарту PKCS7

Возможная длина ключа шифрования:

- 64

- 128

- 256

- 512

В приложении существует возможность ввода пользовательского ключа шифрования. Длина пользовательского ключа шифрования увеличивается до длины соответствующей стандарту шифрования путем конкатенации ключа с самим собой. (в разработке)

Реализована возможность автоматической генерации ключа шифрования

Предусмотрена возможность ввода пользовательского вектора инициализации (IV) для шифровании в режиме CBC (в разработке), возможность автоматической генерации вектора инициализации (IV) (в настоящий момент используется только этот режим)

Доступ к справочной информации по криптографии и алгоритмам шифрования реализован через панель application bar (в разработке)

Поиск по приложению реализован через контракт "Поиск" (в разработке), общий доступ к содержимому реализован через контракт "Общий доступ" (в разработке)

В планах реализация ассиметричных алгоритмов шифрования, ЭЦП.

Последняя правка 11.04.2013