

CryptoBox
presentation

Применение Шифрования



Связь

- Wpa
- Wpa2



Интернет

- SSL
- TLS



Файлы

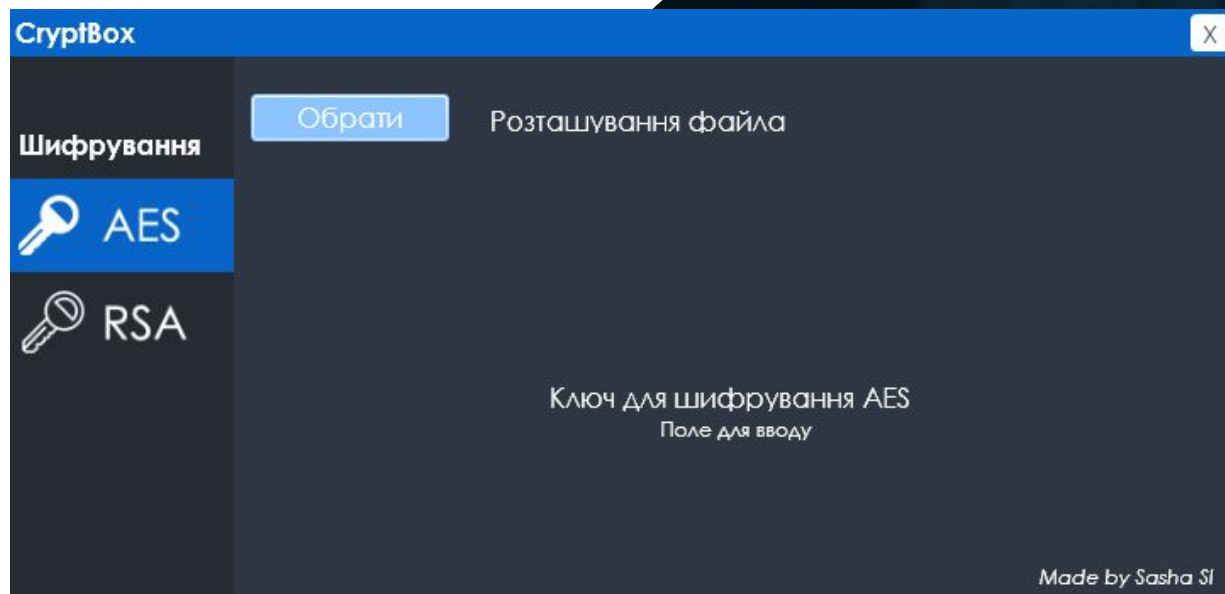
- Bitlocker
- NTFS

Возможности CryptoBox

Симметричное
шифрование

AES

Скорость



Асимметричное
Шифрование
RSA

**Возможность работы
с открытым каналом**



AES

симметричное шифрование

- В июне 2003 года Агентство национальной безопасности США постановило, что шифр AES является достаточно надёжным, чтобы *использовать его для защиты сведений, составляющих государственную тайну.*

RSA



Из-за *низкой скорости шифрования* сообщения обычно шифруют с помощью более производительных симметричных алгоритмов, а с помощью RSA *шифруют лишь этот ключ*, таким образом реализуется гибридная криптосистема.



UI

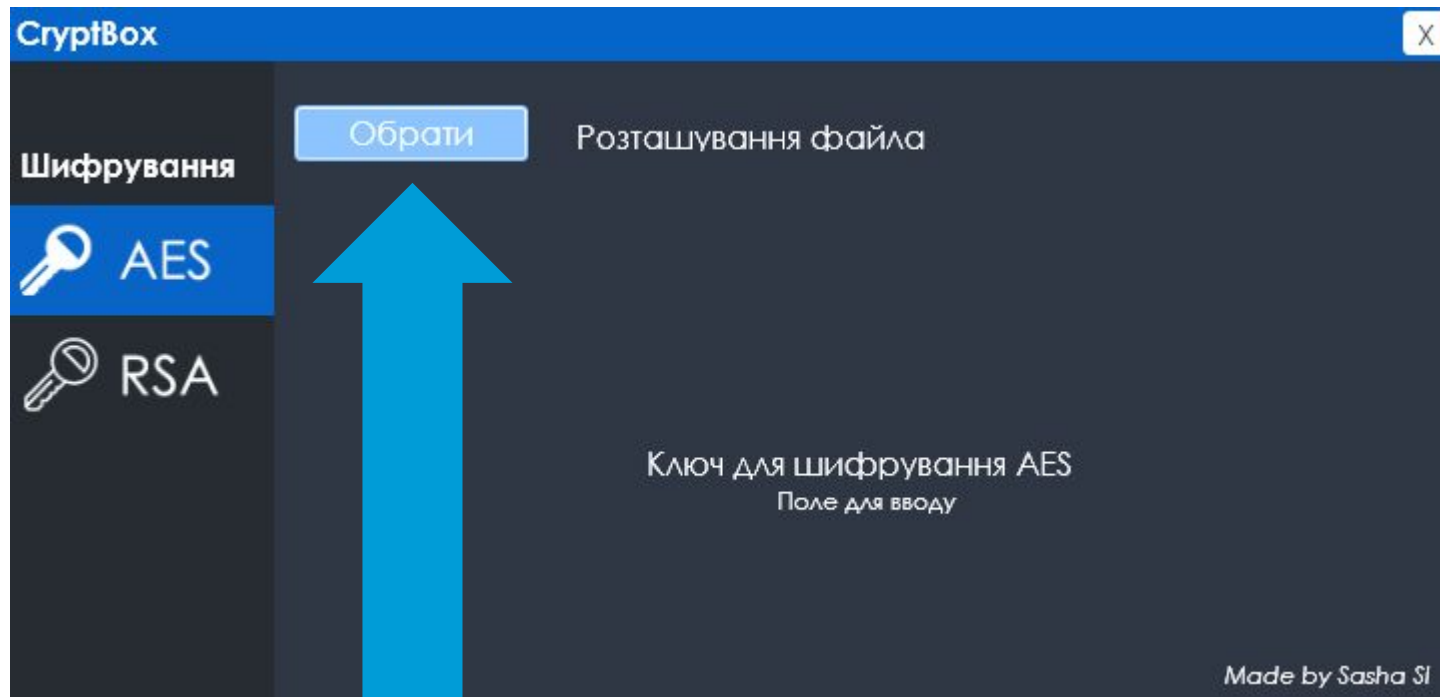
Интерфейс

Пример работы



AES

симметричное шифрование



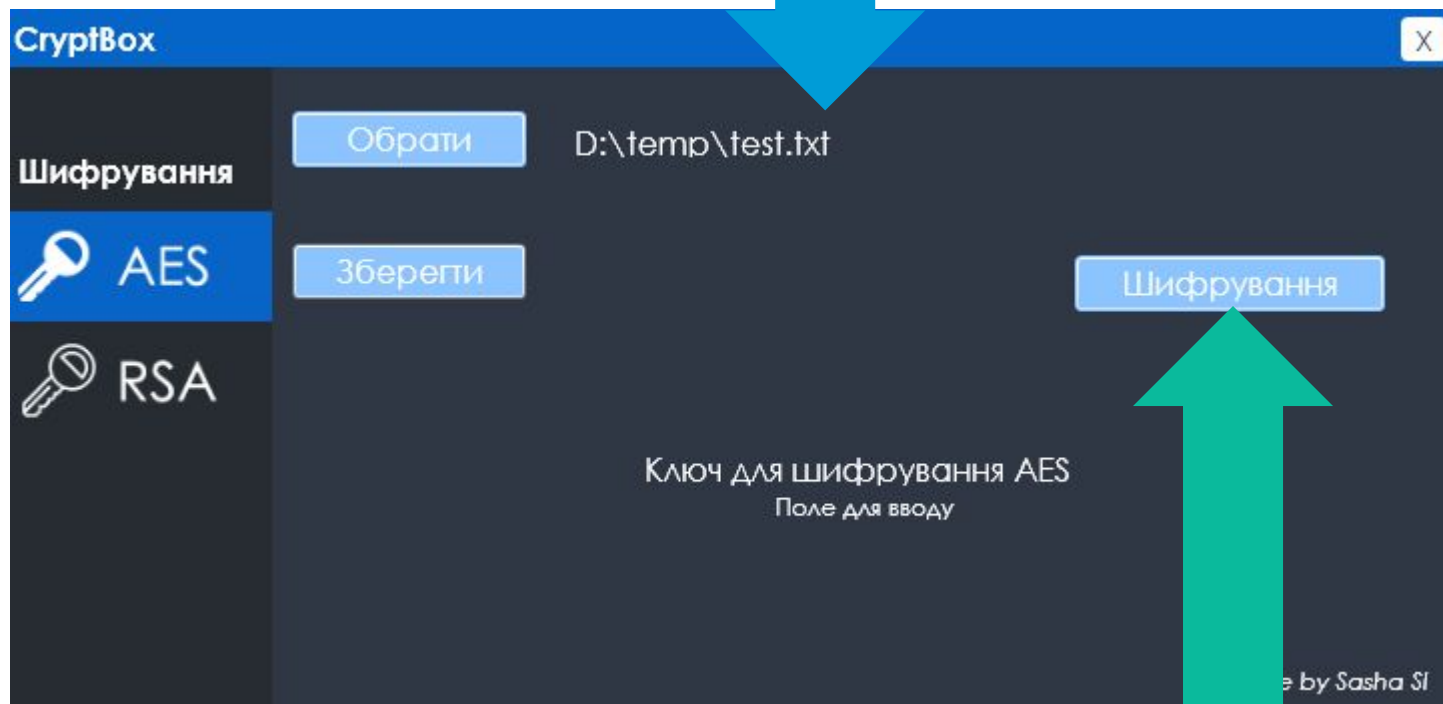
Выбираем файл



AES

симметричное шифрование

Выбранный файл



Шифруем файл



AES

симметричное шифрование

Ключ

The screenshot shows the 'СупрВох' application window. On the left, there is a sidebar with 'Шифрування' (Encryption) and two options: 'AES' (selected) and 'RSA'. The main area contains a file path 'D:\temp\test.txt', buttons for 'Обрати' (Cancel) and 'Зберегти' (Save), and a 'Шифрування' (Encryption) button. Below these, the text 'Ключ для шифрування AES' (AES encryption key) is displayed above a 248-bit hexadecimal key: 248 45 186 46 244 84 204 91 245 87 242 31 43 100 18 214 3 192 0 130 170 243 252 81 15 198 1. The bottom right corner of the window has the text 'Made by Sasha SI'.



Сохраняем зашифрованный файл



AES

симметричное шифрование

До

If you decide to home educate your child you do not have to follow formal rules about how you teach or when you teach. You decide the time and the number of classes for your child per day. You decide the pace of study. You choose the material for your child following his natural abilities and inclinations.

После

Симметричное шифрование — это процесс преобразования информации в форму, которую невозможно прочитать без специального ключа. В AES используются два ключа: открытый и закрытый. Открытый ключ используется для шифрования информации, а закрытый — для ее расшифровки. Этот процесс происходит в несколько этапов: сначала информация делится на блоки, которые затем обрабатываются с помощью сложной математической функции. Результатом является зашифрованная информация, которую можно безопасно передать по каналам связи. Для расшифровки информации необходимо использовать тот же закрытый ключ, который использовался для шифрования. Этот процесс происходит в обратном порядке, и результатом является исходная информация.

Спасибо
За внимание



Спасибо
за внимание