

**CryptoBox**  
presentation

# Применение Шифрования



## Связь

- Wpa
- Wpa2



## Интернет

- SSL
- TLS



## Файлы

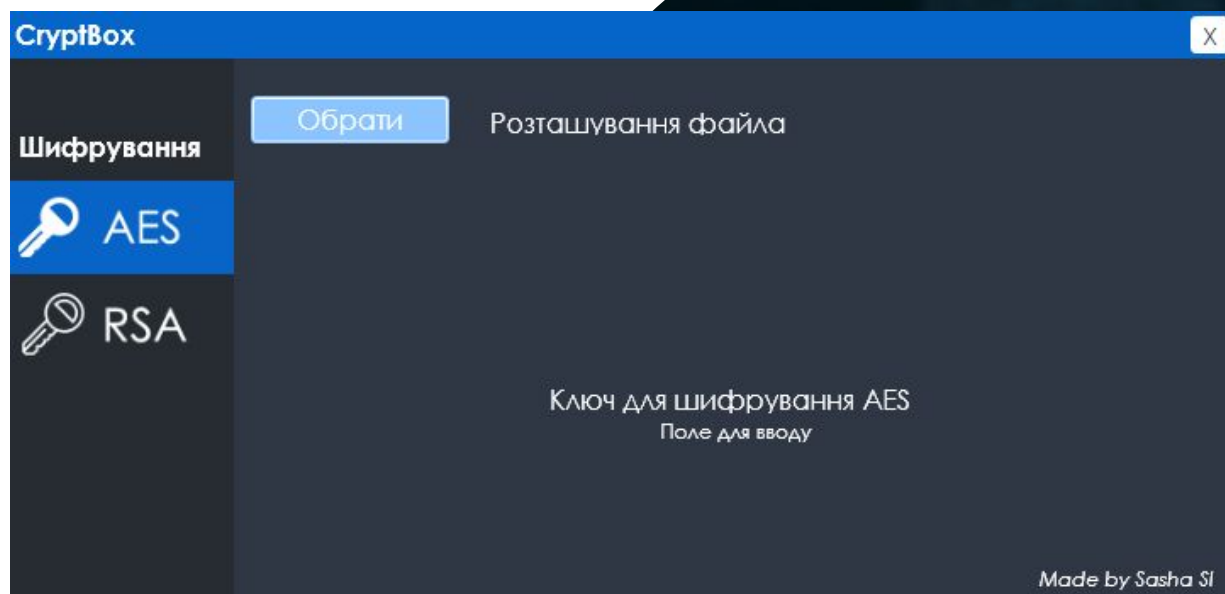
- Bitlocker
- NTFS

# 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

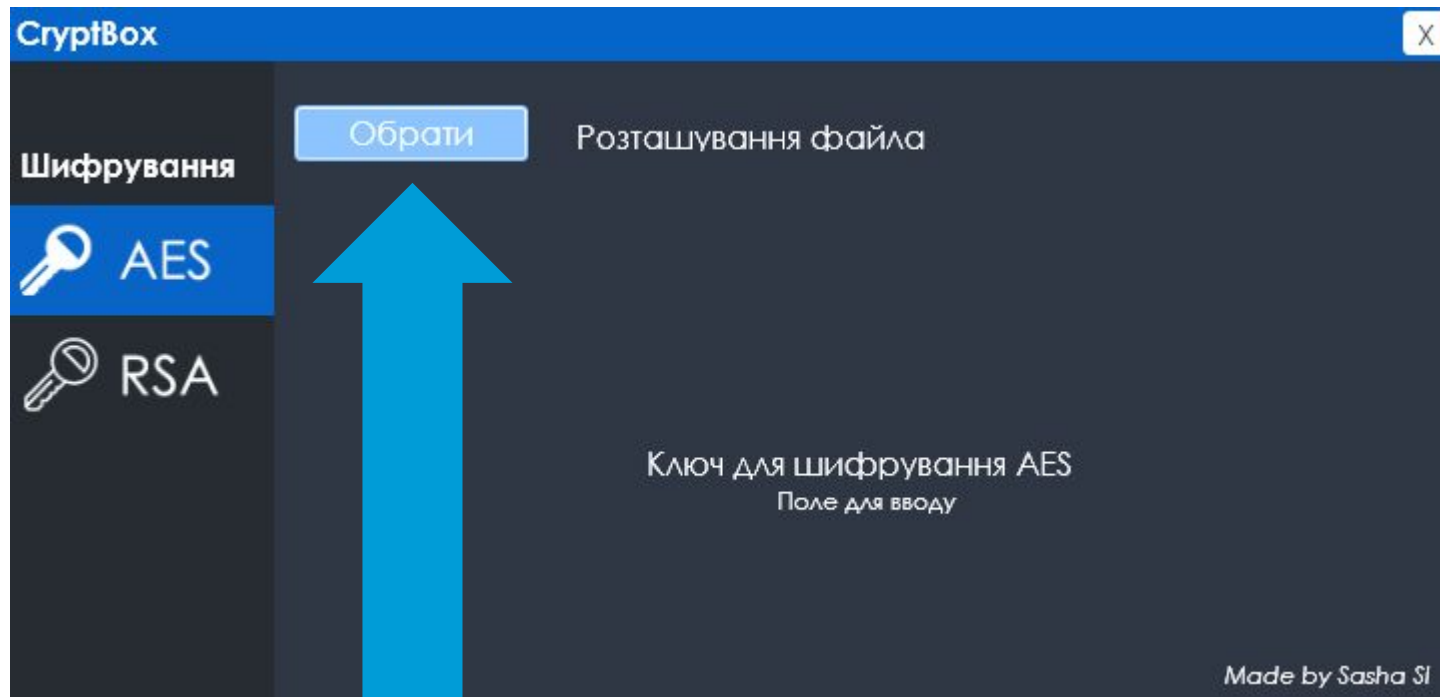
Интерфейс

Пример работы



# AES

симметричное шифрование



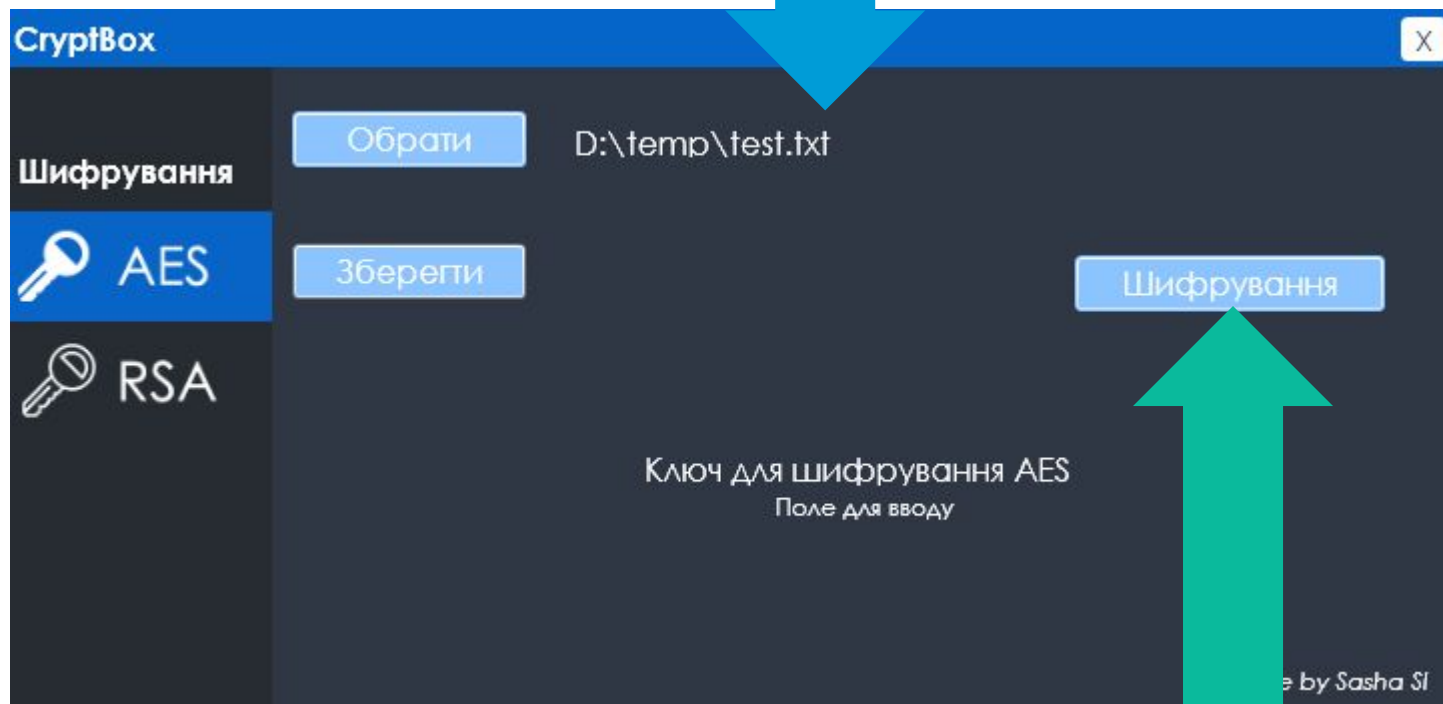
**Выбираем файл**



# AES

симметричное шифрование

Выбранный файл



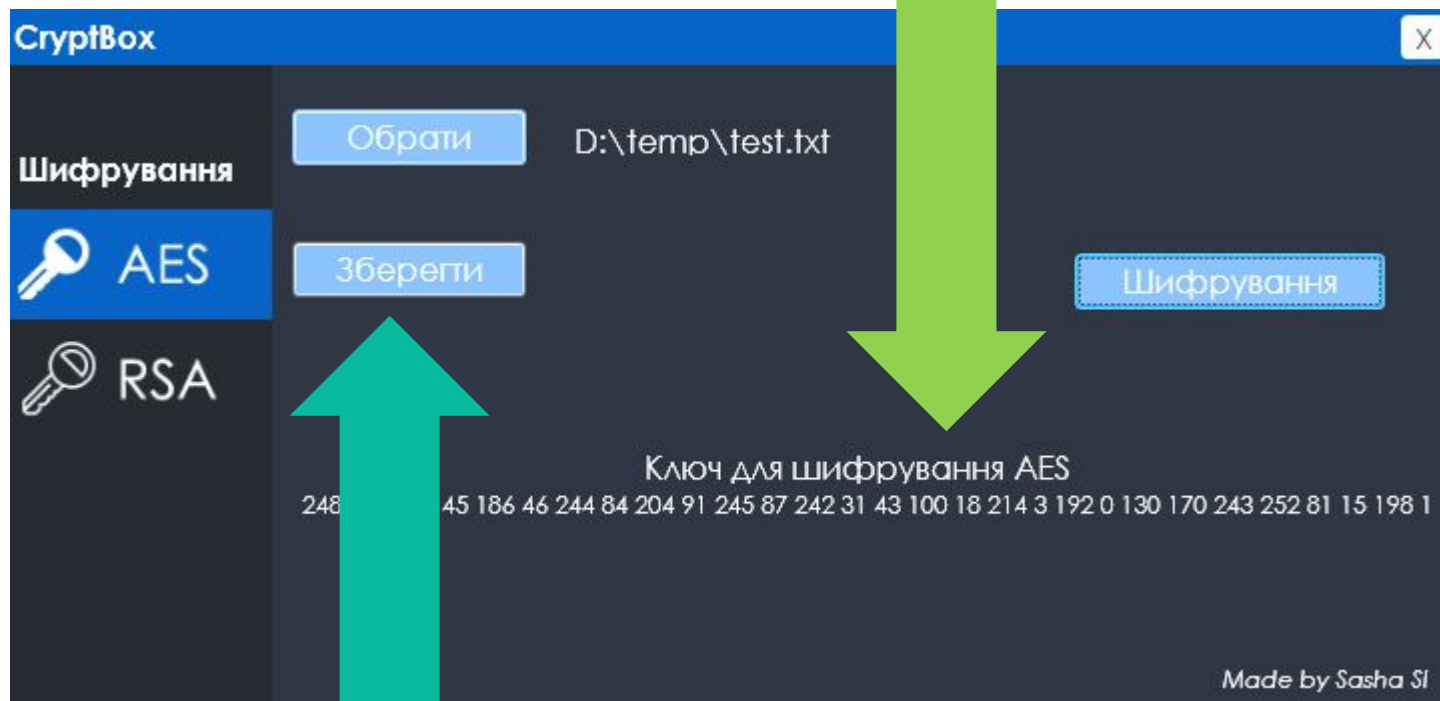
Шифруем файл



# AES

симметричное шифрование

Ключ



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 исходных данных (текста, изображений, аудио и т.д.) в зашифрованную форму с помощью одного и того же ключа. Этот процесс обратим, что позволяет восстановить исходные данные. Симметричные шифры широко используются для защиты конфиденциальной информации в различных приложениях, включая электронную почту, мессенджеры и облачные хранилища. Однако у них есть недостаток: передача ключа должна быть безопасной, иначе шифрование теряет смысл.

**Спасибо**  
За внимание



**Спасибо**  
за внимание