

**CryptoBox**  
presentation

# Применение Шифрования



Связь

- Wpa
- Wpa2



Интернет

- SSL
- TLS



Файлы

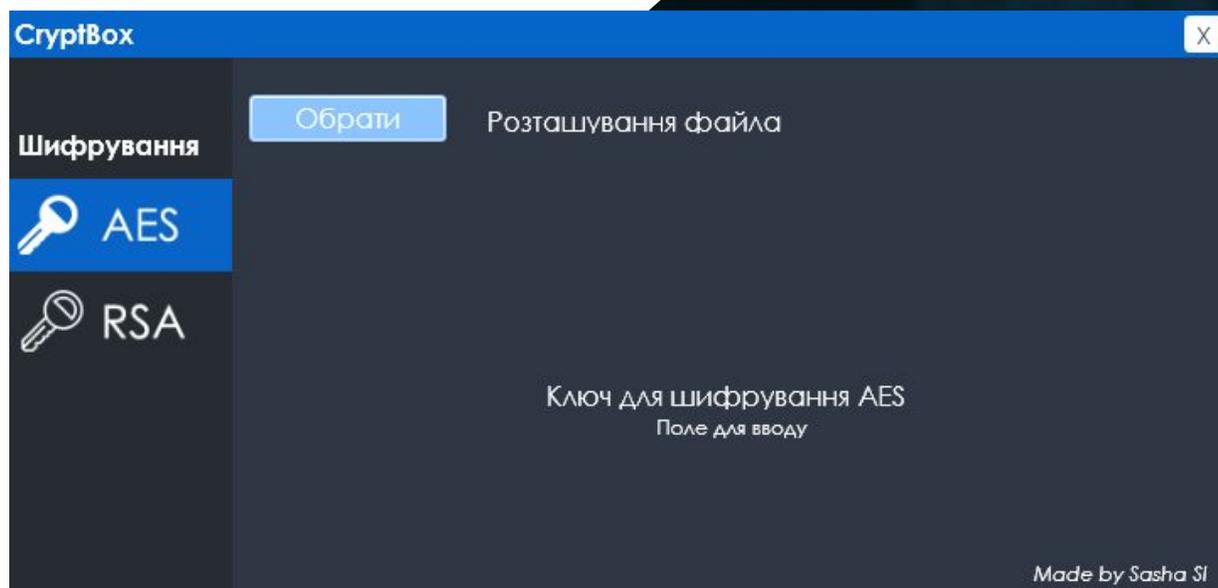
- Bitlocker
- NTFS

# 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

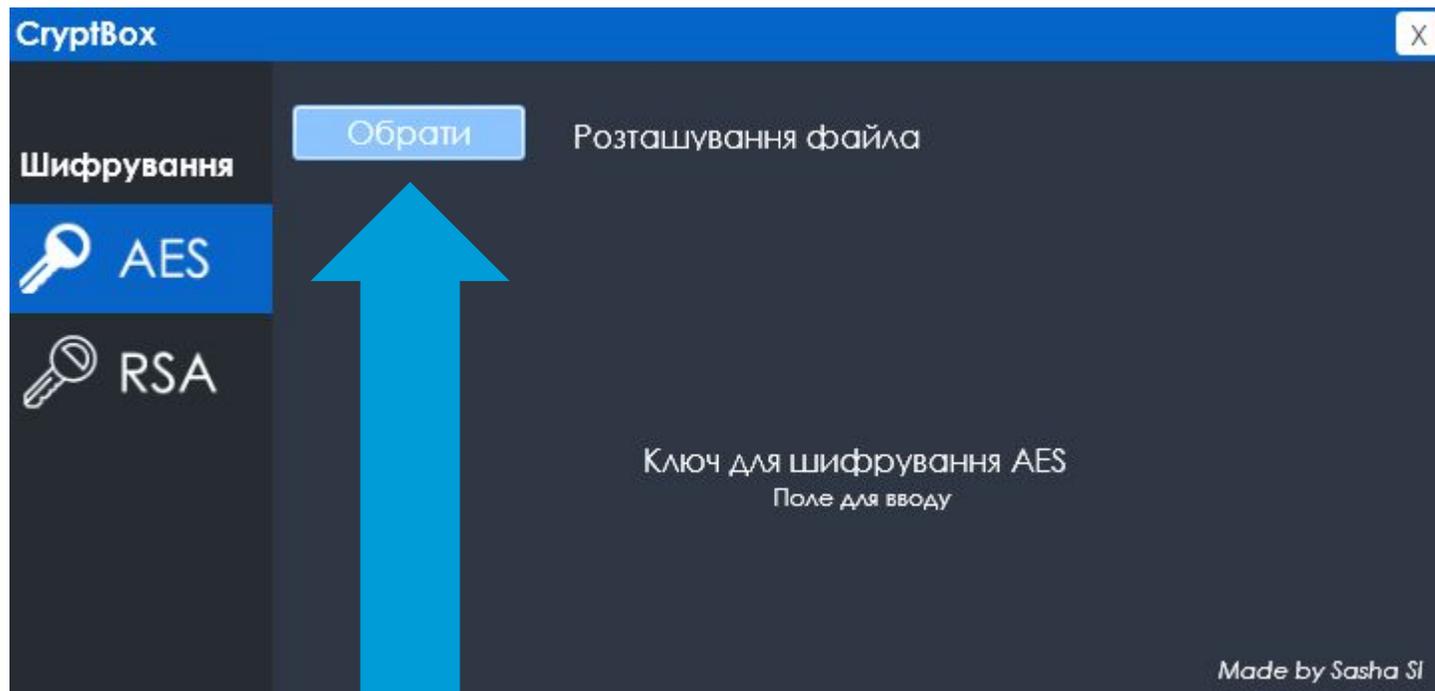
Интерфейс

Пример работы



# AES

симметричное шифрование



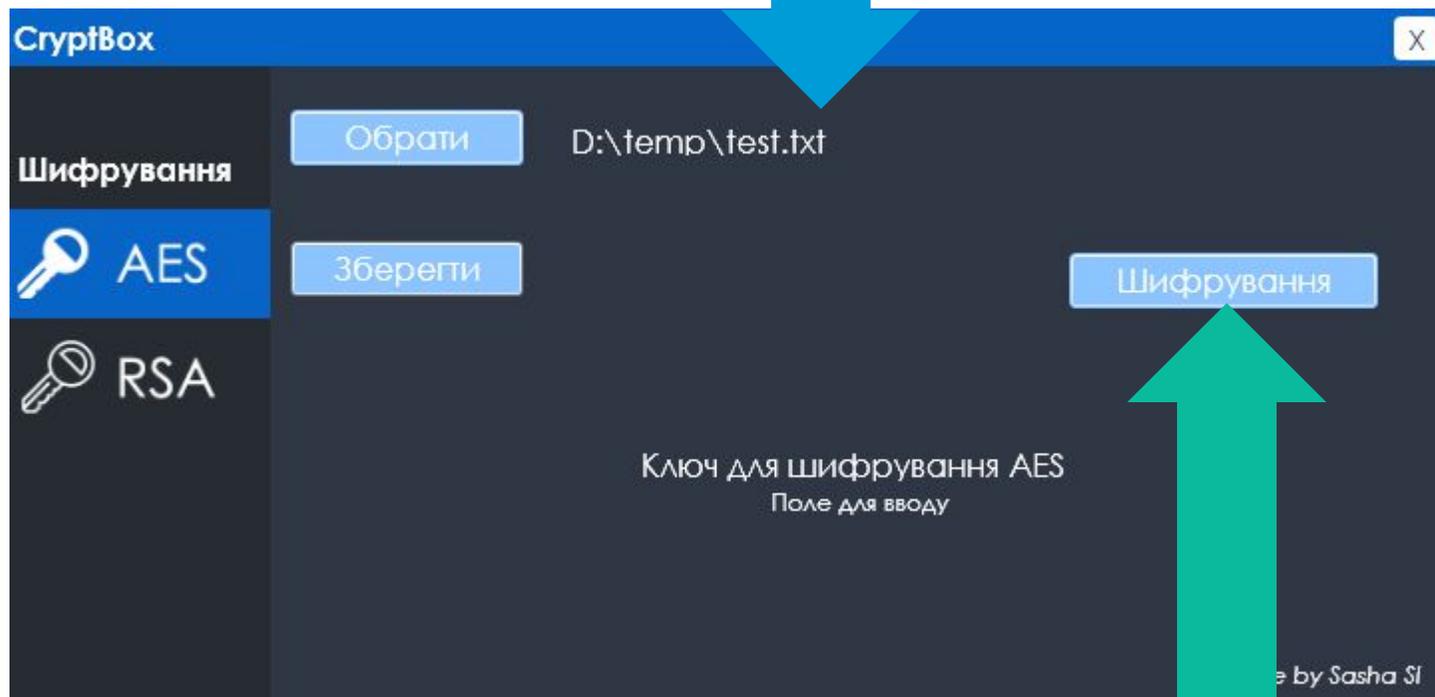
**Выбираем файл**



# AES

симметричное шифрование

Выбранный файл

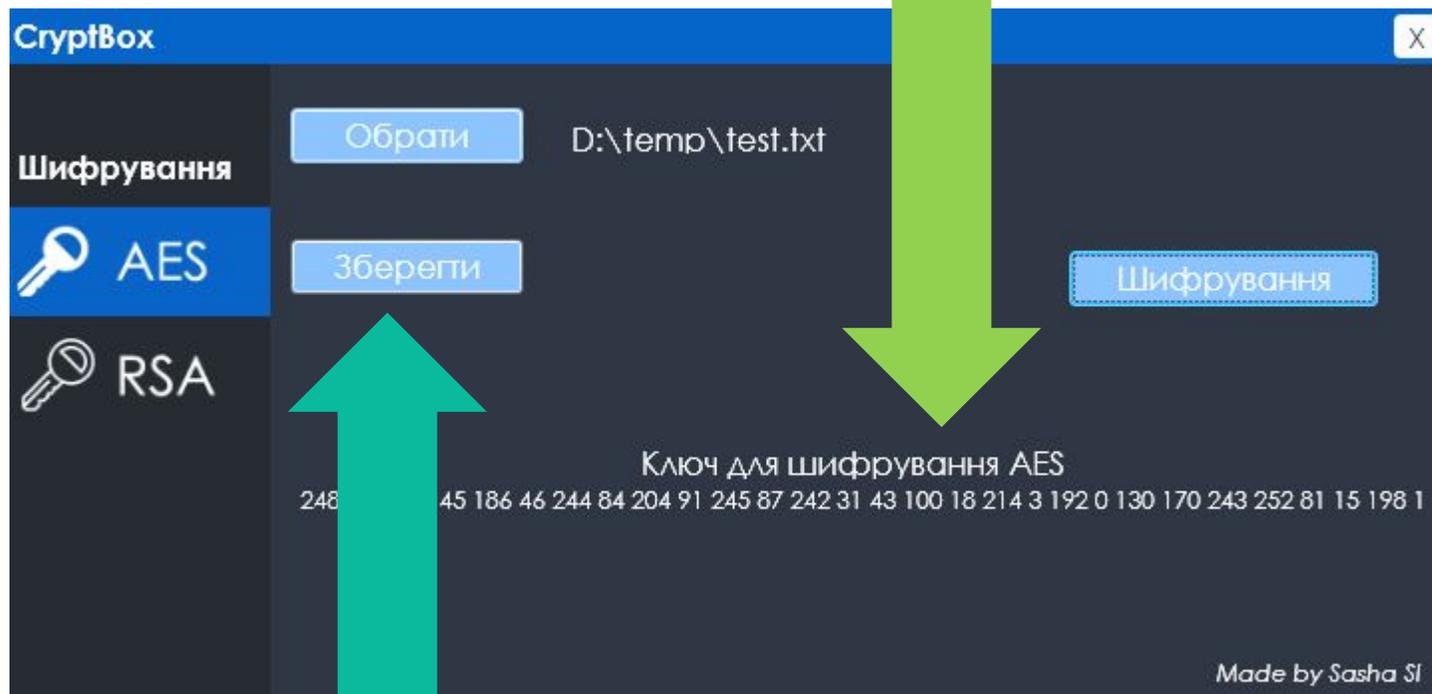


Шифруем файл

# 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 информации в форму, которую невозможно прочитать без специального ключа. В AES используются блочные алгоритмы шифрования, которые работают с данными блоками. Это означает, что каждый блок данных шифруется независимо от других. В результате получается шифрованный текст, который можно прочитать только с помощью правильного ключа. Это обеспечивает высокий уровень безопасности данных.

**Спасибо**  
За внимание



**Спасибо**  
за внимание