Криптографические средства

Лабораторная работа №3

Вариант 7

Выполнили студенты группы 22307

Никаноров Роман и Харичев Евгений

ПетрГУ 2022

Формулировка задания

Реализуйте гибридную криптосистему, включающую:

1) генерацию ключевой пары RSA;

2) шифрование и расшифрование документа симметричным криптоалгоритмом;

3) шифрование и расшифрование сеансового ключа симметричного алгоритма при помощи ключей RSA;

4) формирование и проверку цифровой подписи документа.

Полученный шифротекст, открытые ключи должны сохраняться и передаваться через файлы.

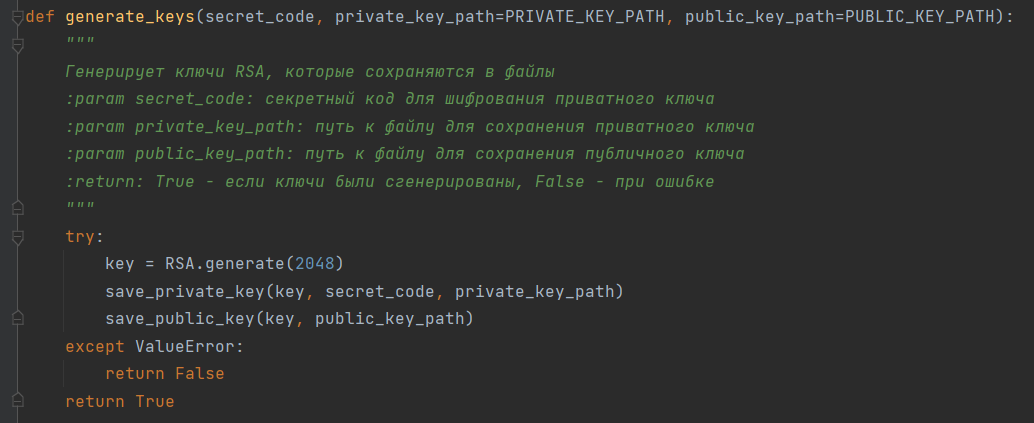
Описание метода решения

Для решения используется Python и библиотека Cryptodome.

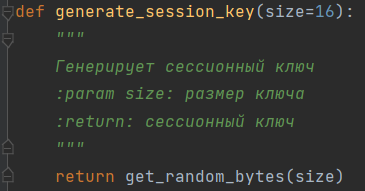
1. Генерируем ключевую пару RSA используя модуль RSA библиотеки Cryptodome для каждой из сторон.
   1. Приватные ключи шифруем, используя секретные фразы сторон, и сохраняем в файлы.
   2. Публичные ключи сохраняем в файлы без шифрования.
   3. Публичные ключи каждой стороны отправляются друг другу.
2. Генерируем рандомный набор байт в качестве сессионного ключа.
   1. Отправляющая сторона шифрует его публичным ключом RSA принимающей стороны и сохраняет в файл.
   2. Принимающая сторона считывает зашифрованный ключ из файла и расшифровывает его своим приватным ключом RSA.
3. Шифруем и расшифровываем файл симметричным алгоритмом AES модуля AES библиотеки Cryptodome, режим шифрования AEAD и сгенерированный симметричный ключ.
4. Формируем и проверяем цифровую подпись, используя модуль Signature библиотеки Cryptodome и алгоритм SHA для получения хэша файла.
   1. Отправляющая сторона получает хэш исходного файла и формирует цифровую подпись для него используя свой приватный ключ RSA, затем шифрует её публичным ключом получателя и сохраняет в файл.
   2. Принимающая сторона получает хэш для расшифрованного файла и расшифровывает полученную цифровую подпись своим приватным ключом RSA, используя их и публичный ключ отправляющей стороны он проверяет цифровую подпись.

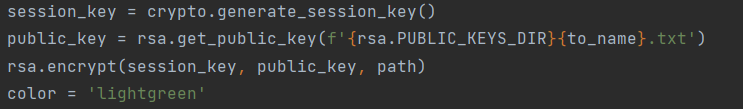
Примеры кода программы

Генерация и сохранение ключей RSA:

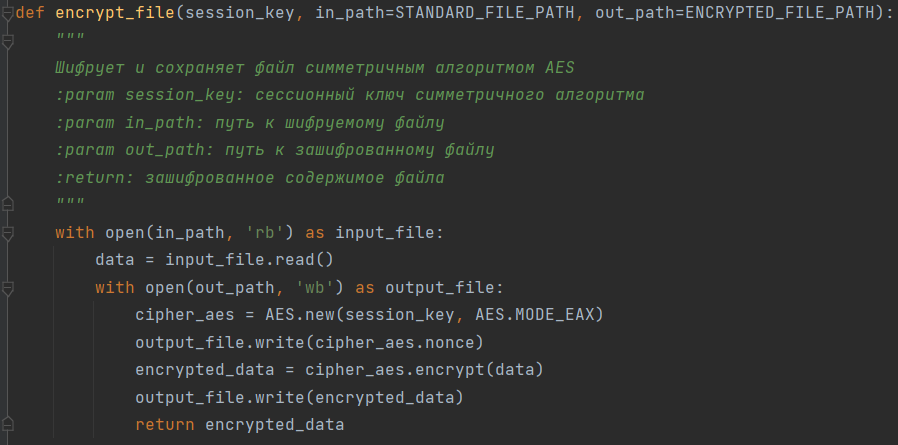


Генерация и шифрование сессионного ключа:

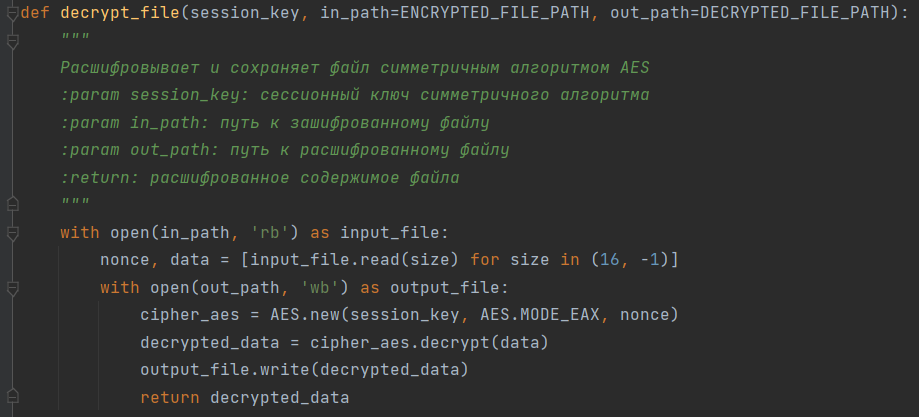




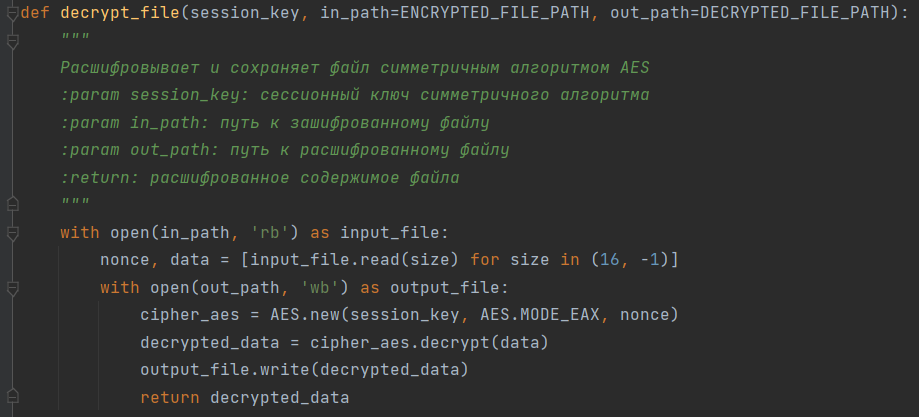
Шифрование файла:



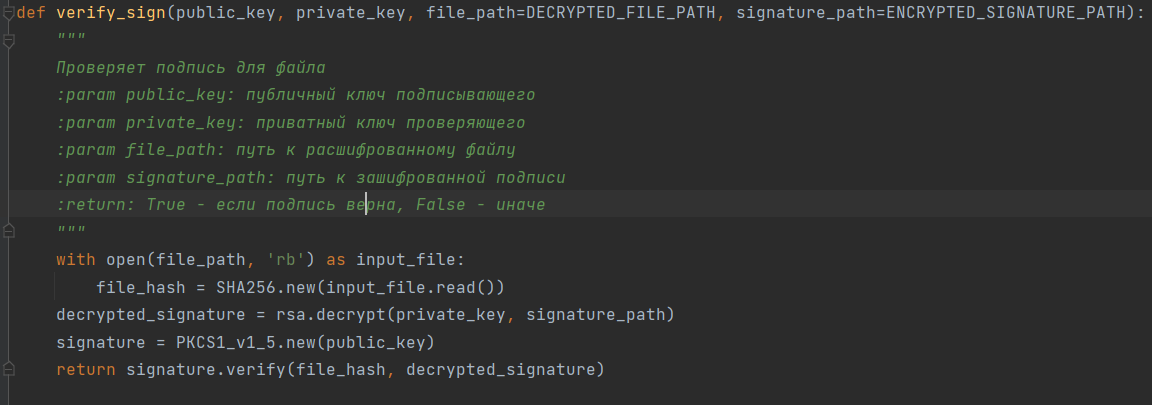
Расшифрование файла:



Подписывание файла:



Проверка цифровой подписи:



Тестовые данные

Сессионный ключ имеет размер 128 бит, в алгоритме RSA равна + 1.Режим шифрование симметричного алгоритма AES – AEAD. Размер nonce равен 128 бит.

