AES Encryption & System Testing

Описание

Этот проект демонстрирует системное тестирование алгоритма шифрования AES (Advanced Encryption Standard). Основное внимание уделяется автоматическому тестированию работы различных режимов шифрования с помощью `unittest`. Помимо тестов, реализовано логирование результатов в консоль и HTML-файл `log.html` с удобным оформлением.

Цель проекта

- Продемонстрировать системное тестирование криптографических алгоритмов, включая их устойчивость к различным входным данным.
- Проверить корректность работы шифрования и расшифрования в разных режимах (CBC, CFB, OFB), используя как валидные, так и невалидные ключи и данные.
- Логировать результаты тестов в удобочитаемом формате с возможностью последующего анализа.
- Визуализировать результаты тестирования в `log.html`, чтобы можно было легко анализировать ошибки и успешные выполнения.

Возможности

- Автоматизированные тесты с использованием `unittest`, охватывающие различные сценарии использования.
- Проверка корректности работы алгоритма AES в различных режимах.
- Проверка обработки ошибок, включая неверные ключи, IV и некорректные входные данные.
- Логирование операций в `log.html` и консоль для наглядного анализа.

Требования

- Python 3.6+
- Установленная библиотека `cryptography`

Установка

1. Клонируйте репозиторий:

   ```
   git clone https://github.com/verlliann/aes-system-testing.git
   cd aes-system-testing
   ```

2. Установите зависимости:

   ```
   pip install cryptography
   ```

Использование

Запуск тестов

Главное предназначение проекта — системное тестирование, поэтому его основной сценарий использования:

```
python aes_script.py test
```

Тесты включают:

- Проверку корректного шифрования и расшифрования в разных режимах AES.
- Обработку неверных ключей и IV, которые не соответствуют стандартам AES.
- Проверку граничных условий, включая минимальные и максимальные размеры входных данных.
- Анализ ошибок и проверку реакции алгоритма на неожиданные ситуации.

Интерактивный режим

Если требуется протестировать алгоритм вручную, можно запустить скрипт без аргументов:

```
python aes_script.py
```

Следуйте инструкциям для ввода ключа, IV и данных для шифрования.

Логирование

Все результаты тестирования и операций шифрования записываются в `log.html`. Этот файл оформлен в современном стиле и содержит:

- Подробные записи о каждом тесте, включая входные и выходные данные.
- Успешные и неуспешные тесты с соответствующими метками.

Почему важны системные тесты?

Системное тестирование играет ключевую роль в обеспечении безопасности и надежности кода. Это помогает:

- Автоматизировать проверку различных сценариев использования.
- Исключить ошибки при изменении кода, обеспечивая его стабильность.
- Быстро находить и исправлять потенциальные уязвимости.

Автор

verlliann prod.