Информационная безопасность

Презентация к лабораторной работе № 8

Мерич Дорук Каймакджыоглу.

28/10/2023

# Информация

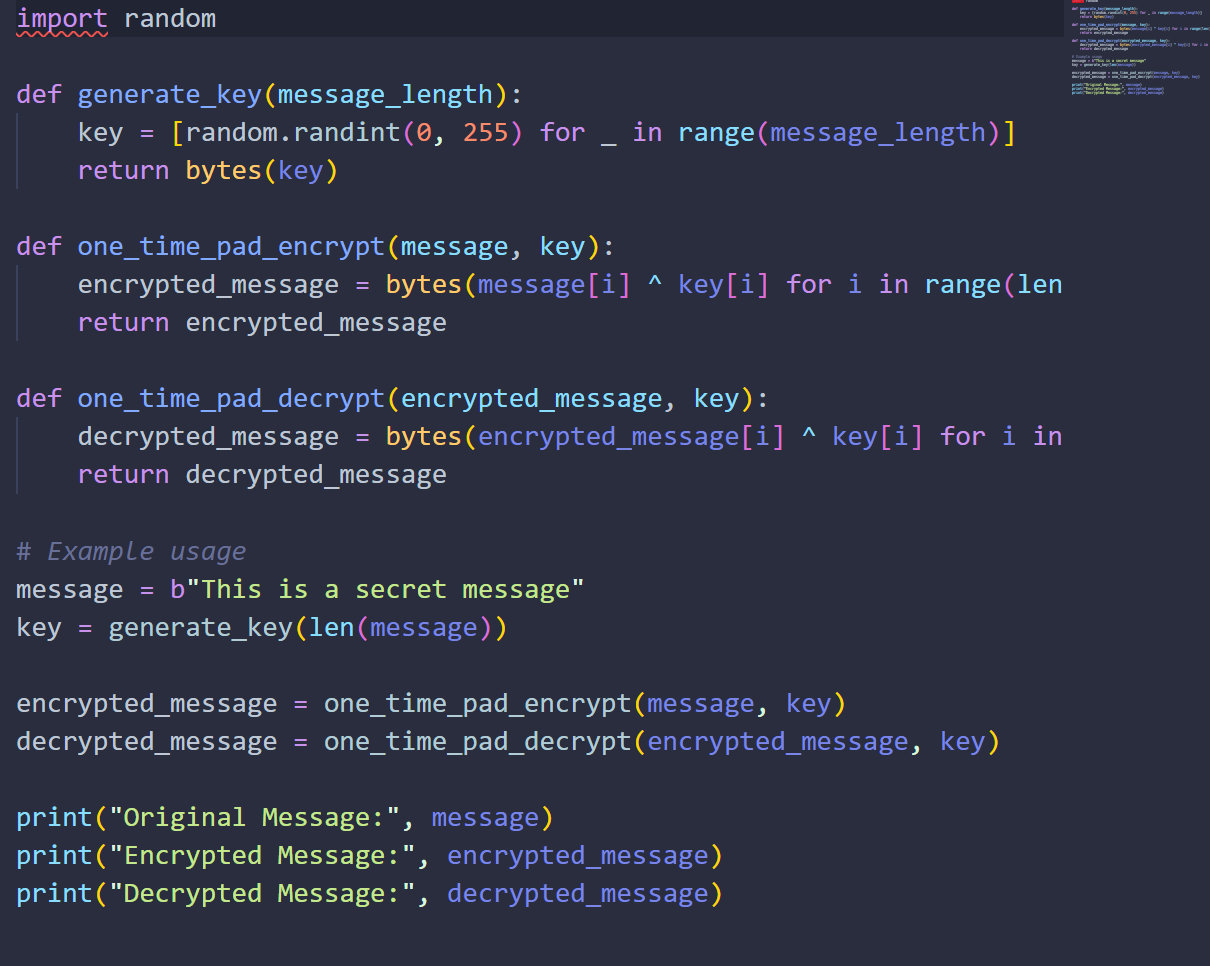
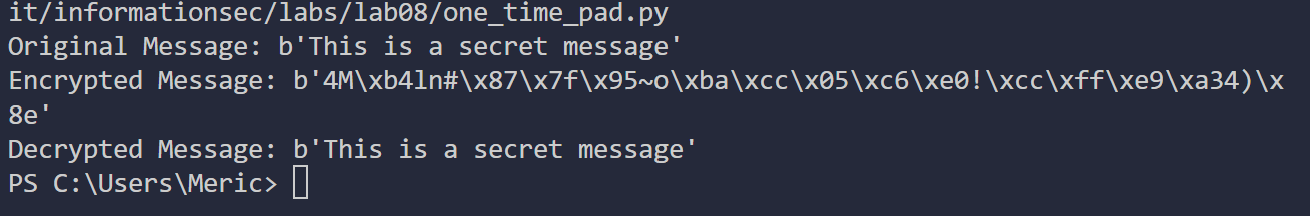
## Докладчик

* Мерич Дорук Каймакджыоглу
* Студент
* НКНбд-01-20
* Российский университет дружбы народов
* 1032204917
* <https://github.com/dorukme123>

## Объект и предмет исследования

* выполнил действия, показанные в отчете.

## Цели и задачи

* Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключоm.
* Два текста кодируются одним ключом (однократное гаммирование). Требуется не зная ключа и не стремясь его определить, прочитать оба текста. Необходимо разработать приложение, позволяющее шифровать и дешифровать тексты P1 и P2 в режиме однократного гаммирования. Приложение должно определить вид шифротекстов C1 и C2 обоих текстов P1 и P2 при известном ключе ; Необходимо определить и выразить аналитически способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить.  

## Контрольные вопросы

1. Как, зная один из текстов (P1 или P2), определить другой, не зная при этом ключа? Если вы знаете один из текстов (P1 или P2) и хотите определить другой, не зная ключа, то вам потребуется информация о шифровании, используемом алгоритме и режиме работы. В большинстве случаев, без ключа и без знания алгоритма шифрования или режима, дешифрование второго текста будет практически невозможным
2. Что будет при повторном использовании ключа при шифровании текста? При повторном использовании одного и того же ключа при шифровании текста в большинстве симметричных шифров (например, AES), вы получите одинаковый шифротекст для одного и того же открытого текста. Это означает, что при использовании одного ключа несколько раз шифротекст будет одинаковым, что может привести к утечке информации и понижению безопасности системы.
3. Как реализуется режим шифрования однократного гаммирования одним ключом двух открытых текстов? Режим шифрования однократного гаммирования (One-Time Pad, OTP) использует один ключ для шифрования двух открытых текстов путем применения операции XOR к ключу и каждому открытому тексту. Он работает так: C1 = P1 XOR Key и C2 = P2 XOR Key, где C1 и C2 - шифротексты, P1 и P2 - открытые тексты, и Key - один и тот же случайный ключ.
4. Перечислите недостатки шифрования одним ключом двух открытых текстов. Недостатки шифрования одним ключом двух открытых текстов (OTP) включают в себя: - Требование абсолютно случайного ключа той же длины, что и открытый текст. - Невозможность повторного использования ключа, так как это приведет к потере безопасности. - Затраты на передачу и хранение больших ключей.- Уязвимость к атаке, если ключ повторно используется или не генерируется абсолютно случайным образом.
5. Перечислите преимущества шифрования одним ключом двух открытых текстов. Преимущества шифрования одним ключом двух открытых текстов (OTP) включают в себя: - Математический доказанный уровень безопасности при условии использования абсолютно случайного ключа. - Абсолютно секретное шифрование, если ключ не используется повторно и не разглашается. - Отсутствие возможности криптоанализа, если ключ неизвестен злоумышленнику.

## Материалы и методы

* LaTex
* Процессор **pandoc** для входного формата Markdown
* Результирующие форматы
  + **pdf**
  + **docx**
* Автоматизация процесса создания: **Makefile**

## Результаты

* Освоил на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

## Итог работы

* Получено **pdf** из report.md
* Получено **docx** из report.md
* Получено **html** из presentation.md
* Получено **pdf** из presentation.md
* Получено **docx** из presentation.md
* Запись отчета выложен в youtube.com
* Запись презентация выложен в youtube.com
* Запись отчета выложен в rutube.com
* Запись презентация выложен в rutube.com
* Работа выложена в респоситории в github.com
* CHANGELOG.md создано
* Версия на работе создано