Структура научной презентации

Простейший шаблон

Карпачев Я. О.

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Карпачев Я. О.
- студент
- Российский университет дружбы народов

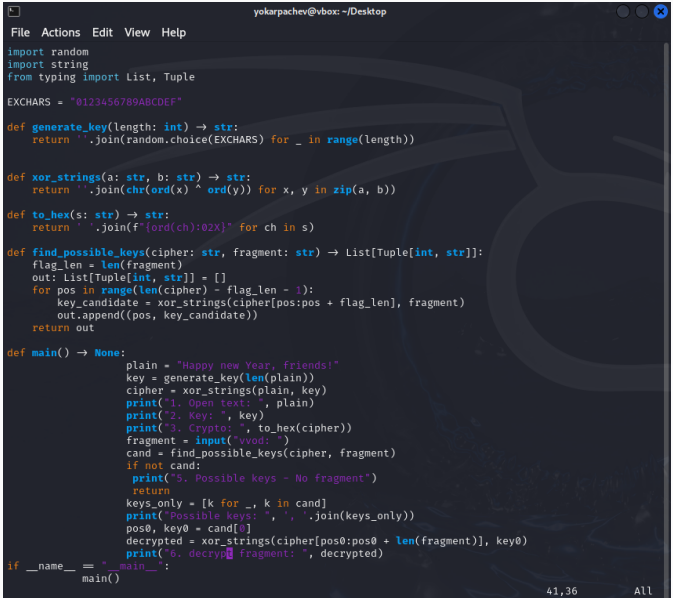
Цель работы

Цель работы

Освоить на практике применение режима однократного гаммирования

Выполнение лабораторной работы

Пишим скрипт



проверяем работу программы

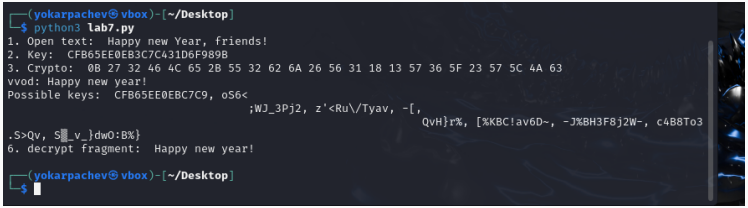


Рис. 2: Работа программы

Контрольные вопросы

1. Смысл однократного гаммирования – сложение (XOR) текста с однократной случайной гаммой той же длины.
2. Недостатки: нужна истинно случайная гамма; ключ хранить/передавать так же долго, как сообщение; ключ нельзя переиспользовать.
3. Преимущества: абсолютная криптостойкость; простота реализации; симметричность (шифр = дешифр).
4. Длины равны, чтобы каждый символ текста «прикрывался» одним символом гаммы; иначе остаётся статистическая избыточность.
5. Операция – XOR (сложение по модулю 2); даёт -– при повторном применении тем же ключом восстанавливается исходник.
6. Шифротекст: C_i = P_i ⊕ K_i.
7. Ключ: K_i = C_i ⊕ P_i.
8. Условия абсолютной стойкости: (a) гамма истинно случайна; (b) длина ключа = длина сообщения; (c) ключ используется лишь однажды.

Выводы

Я освоить на практике применение режима однократного гаммирования