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 режим однократного гаммирования (одноразового шифрования) на примере кодирования двух различных телеграмм одним ключом и продемонстрировать уязвимость повторного использования ключа.

Шифрование и получение шифротекстов

Шифрование и получение шифротекстов

Кодирование двух исходных телеграмм P_1 и P_2 одним ключом K с помощью операции XOR.

Демонстрация уязвимости: получение двух открытых текстов без знания ключа

Повторное использование ключа при шифровании P_1 и P_2 позволяет злоумышленнику, зная C_1 и C_2, получить $P_1 ? P_2$:

Повторное использование ключа при шифровании P_1 и P_2 позволяет злоумышленнику, зная C_1 и C_2, получить $P_1 ? P_2$:

$$C1 \oplus C2 = P1 \oplus K \oplus P2 \oplus K = P1 \oplus P2.$$

Если P_1 известен (например, шаблонный текст), то:

$$P2 = (C1 \oplus C2) \oplus P1.$$

Вычисление $C1 ? C2$ и получение P_2 при известном P_1.

Программы и вывод

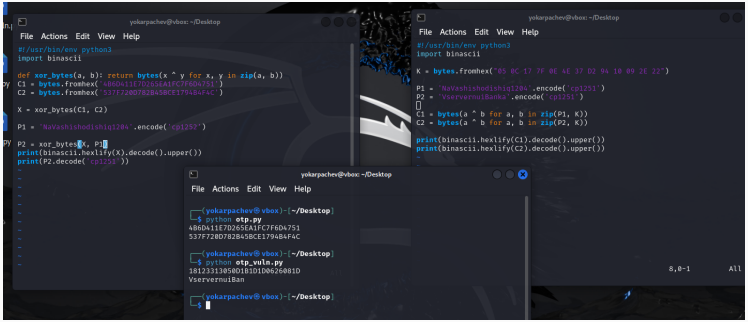

Рис. 1: Программы

Выводы

1. Повторное использование одного и того же ключа при режиме гаммирования приводит к опасной уязвимости: злоумышленник, имея два шифротекста, может получить XOR двух открытых текстов.
2. Зная один из открытых текстов (шаблон), можно полностью восстановить второй без знания ключа.
3. Ключ в режиме одноразовой гаммы должен использоваться лишь один раз; повторное использование делает шифрование небезопасным.