Лабораторная работа №7

Элементы криптографии. Однократное гаммирование

Панченко Денис Дмитриевич

Содержание

# 1 Цель работы

Освоить на практике применение режима однократного гаммирования.

# 2 Задачи

* Научиться применять режим однократного гаммирования.

# 3 Выполнение лабораторной работы

1. Создадим файл с программой (рис. 1).

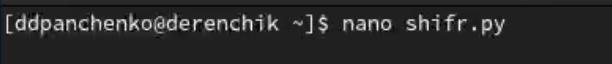


Рис. 1: Файл с программой

1. Напишем саму программу для шифрования (рис. 2).

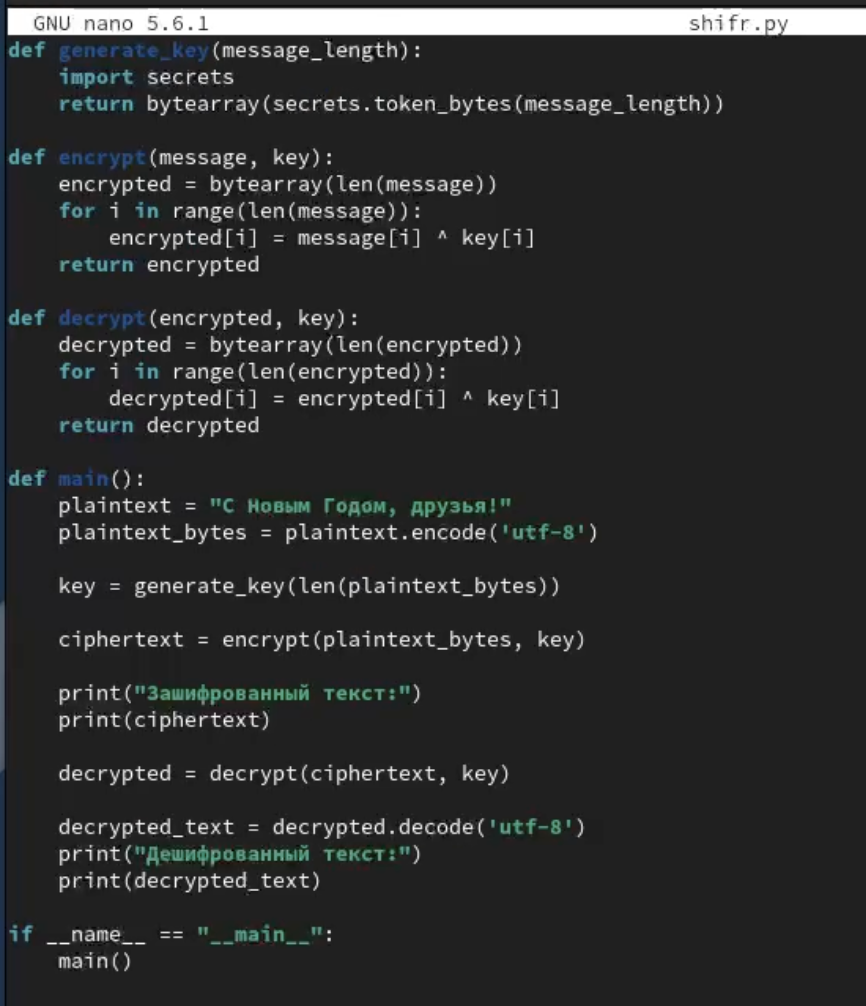


Рис. 2: Программа

1. Выполним эту программу (рис. 3).

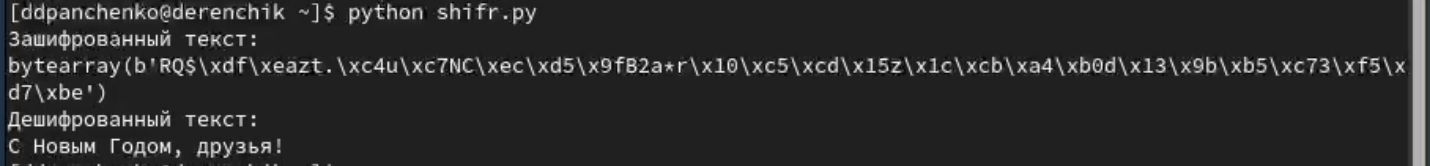


Рис. 3: Выполнение программы

# 4 Контрольные вопросы

1. Поясните смысл однократного гаммирования. Однократное гаммирование - это метод шифрования, при котором каждый символ открытого текста преобразуется путем выполнения операции XOR с соответствующим символом ключа. Этот метод получил свое название потому, что каждый ключ используется только один раз для шифрования определенного сообщения.
2. Перечислите недостатки однократного гаммирования.

* Необходимость в ключе такой же длины, как и открытый текст.
* Необходимость генерации случайного ключа для каждого сообщения.
* Уязвимость к атакам, основанным на повторном использовании ключа.
* Ограничение на размер сообщения из-за необходимости ключа такой же длины.

1. Перечислите преимущества однократного гаммирования.

* При правильной реализации и использовании случайного ключа является абсолютно надежным методом шифрования.
* Нельзя получить информацию о зашифрованном тексте без знания ключа.
* Сложность криптоанализа возрастает с увеличением размера ключа и текста.

1. Почему длина открытого текста должна совпадать с длиной ключа? Поскольку для каждого символа открытого текста используется соответствующий символ ключа при операции XOR, длина ключа должна быть такой же, как и длина открытого текста, чтобы обеспечить правильное шифрование и дешифрование.
2. Какая операция используется в режиме однократного гаммирования, назовите её особенности? В режиме однократного гаммирования используется операция XOR (побитовое сложение по модулю 2). Особенность этой операции заключается в том, что она возвращает true (1), если только один из операндов true (1), и false (0) в противном случае.
3. Как по открытому тексту и ключу получить шифротекст? Шифротекст получается путем выполнения операции XOR между каждым символом открытого текста и соответствующим символом ключа.
4. Как по открытому тексту и шифротексту получить ключ? Ключ получается путем выполнения операции XOR между каждым символом шифротекста и соответствующим символом открытого текста.
5. В чем заключаются необходимые и достаточные условия абсолютной стойкости шифра? Необходимые и достаточные условия абсолютной стойкости шифра включают:

* Полная случайность ключа.
* Равенство длин ключа и открытого текста.
* Однократное использование ключа.

# 5 Вывод

Я освоил на практике применение режима однократного гаммирования.