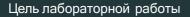
## Лабораторная работа № 7

Элементы криптографии. Однократное гаммирование

Форис Анастасия Дмитриевна

10.2024

Российский университет дружбы народов, Москва, Россия



Освоить на практике применение режима однократного гаммирования.

### Выполнение лабораторной работы 1. Создание программы

Я начала процесс с импорта необходимых библиотек, неотъемлемых для криптографических операций, которые последовали. Впоследствии я разработала специализированную функцию, способную выполнять операции побитового ХОК на двух строках, облегчая процессы шифрования и дешифрования. Исходный текст, служащий оригинальным незашифрованным текстом, играл ключевую роль в последующих шагах. Ключ, тщательно созданный для соответствия длине исходного текста, генерировался для внесения дополнительного уровня безопасности в механизм шифрования.

Применяя ранее разработанную функцию, я легко получила шифротекст, предполагая знание как исходного текста, так и созданного ключа. Этот шифротекст, представляющий собой зашифрованную форму оригинального текста, служил важным посредником в криптографических процедурах. Кроме того, я продемонстрировала обратимость процесса, используя ту же функцию для получения исходного текста при наличии информации как о шифротексте, так и о ключе.

Интригующим образом, криптографический процесс не ограничивался лишь шифрованием и дешифрованием, но также распространялся на восстановление ключа. Снова воспользовавшись той же функцией, я успешно извлекла ключ, обладая информацией как о исходном тексте, так и соответствующем шифротексте. Этот всесторонний подход к криптографическим операциям подчеркивает взаимосвязанную природу шифрования, дешифрования и управления ключами в обеспечении целостности и конфиденциальности чувствительной информации.

### Выполнение лабораторной работы 4



Рис. 1: Приложение, реализующее режим однократного гаммирования

```
the first time the first that
5 4 4 5 5 6 4 4 4 - 8 C C -
                                    Or $117 March 1898a
                                                                           Tree custod migrit cost
                                                                              March 100s
                                 or TTY and classificant has been seen, but
                                                                                                      party time a very party tree and party
                                                                                                   Tight : lette-
                                                                                                the 1.44 timestandensin
                                                                                             The part seed amount to a small to
                                                                                                   man tiple Tall
                                 IN 1812 Start of Telephone States and an extension of the contract of the cont
                                    on the late of
                                                                              Tion In
                                                                              No. 1 to require country.
                                                                              the salestee minimal by sever letters a partial shares.
                                                                              Stilled Heater
                                                                                 Name of the Owner, the
                              in (11) Takes and Condensed Section Seeks and
                                                                           WINE CONTRACT CAMPACINGS
                                                                              paperson manifestation in the
                                 IN 1889 AND DESCRIPTION OF THE PARTY OF THE 
                                                                                 Street, experient feature steel, day of
                              IN THE WORLDOOK, SQUEETERS BROKENING, TORSON THE
                                                                              Own Story budged to be
```

Рис. 2: Код

# Вывод

#### Вывод

В ходе выполнения данной лабораторной работы я освоила на практике применение режима однократного гаммирования.