

# Шифр гаммирования

---

Драммах Мариам Л НФИбд-02-18

15 декабря, 2021, Москва, Россия

Российский Университет Дружбы Народов

# Цели и задачи

---

## Цель лабораторной работы

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

# **Выполнение лабораторной работы**

---

Гаммирование – это наложение (снятие) на открытые (зашифрованные) данные криптографической гаммы, т.е. последовательности элементов данных, вырабатываемых с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных.

Шифротексты обеих телеграмм можно получить по формулам режима однократного гаммирования:

$$C_1 = P_1 \oplus K$$

$$C_2 = P_2 \oplus K$$

Открытый текст можно найти, зная шифротекст двух телеграмм, зашифрованных одним ключом. Для это оба равенства складываются по модулю 2. Тогда с учётом свойства операции XOR получаем:

$$C_1 \oplus C_2 = P_1 \oplus K \oplus P_2 \oplus K = P_1 \oplus P_2$$

Предположим, что одна из телеграмм является шаблоном — т.е. имеет текст фиксированный формат, в который вписываются значения полей. Допустим, что злоумышленнику этот формат известен. Тогда он получает достаточно много пар  $C_1 \oplus C_2$  (известен вид обеих шифровок). Тогда зная  $P_1$  имеем:

$$C_1 \oplus C_2 \oplus P_1 = P_1 \oplus P_2 \oplus P_1 = P_2$$

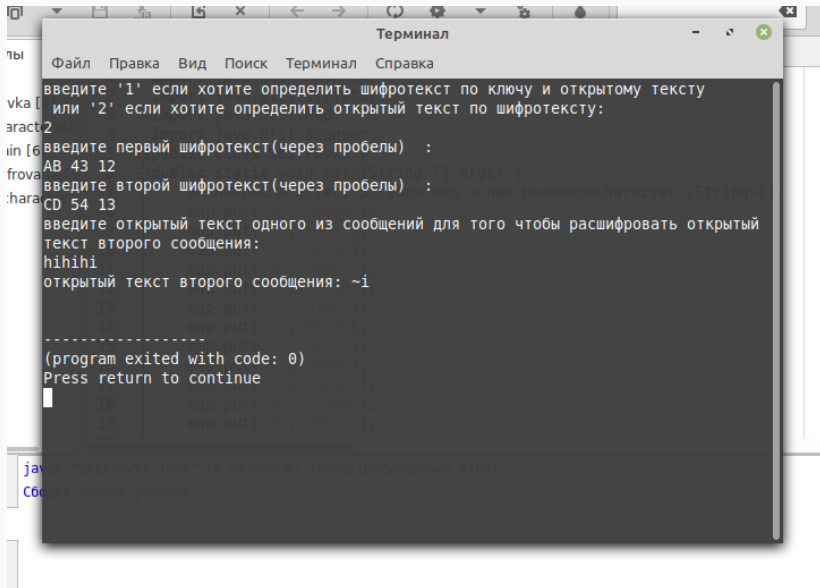


# Схема работы алгоритма



Figure 1: Работа алгоритма гаммирования

# Пример работы программы



```
Терминал
Файл  Правка  Вид  Поиск  Терминал  Справка

введите '1' если хотите определить шифротекст по ключу и открытому тексту
или '2' если хотите определить открытый текст по шифротексту:
2
введите первый шифротекст(через пробелы)  :
AB 43 12
введите второй шифротекст(через пробелы)  :
CD 54 13
введите открытый текст одного из сообщений для того чтобы расшифровать открытый
текст второго сообщения:
hihihi
открытый текст второго сообщения: ~i

-----
(program exited with code: 0)
Press return to continue

```

```
java "Shifrovka.java" (в каталоге: /home/ivan/Рабочий стол)
Сборка прошла успешно.
```

## **Выводы**

---

## Результаты выполнения лабораторной работы

В ходе выполнения лабораторной работы было разработано приложение, позволяющее шифровать тексты в режиме однократного гаммирования.