Презентация по лабораторной работе №8

Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом

Саргсян А. Г.

21 октября 2023

Российский университет дружбы народов, Москва, Россия

Цель работы

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

Задание

Два текста кодируются одним ключом (однократное гаммирование). Требуется не зная ключа и не стремясь его определить, прочитать оба текста. Необходимо разработать приложение, позволяющее шифровать и дешифровать тексты P1 и P2 в режиме однократного гаммирования. Приложение должно определить вид шифротекстов C1 и C2 обоих текстов P1 и P2 при известном ключе ; Необходимо определить и выразить аналитически способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить.

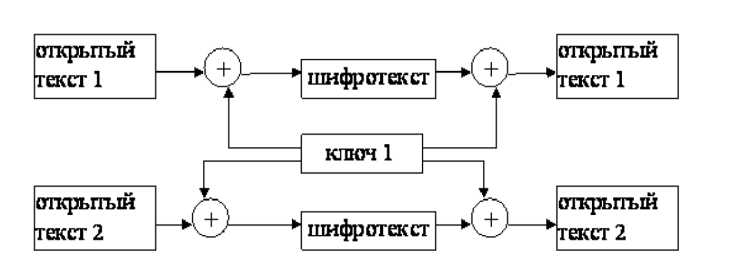

Рис. 1: Общая схема шифрования двух различных текстов одним ключом

Результат

```
C:\Users\User\.jdks\openjdk-19.0.1\bin\java.exe "
[а, б, в, г]
абвг
Числовой вариант текста [0, 0, 0, 0]
Числовой вариант ключа [17, 17, 17, 17]
Числовой вариант шифротекста [17, 17, 17, 17]
Шифротекст cccc
Исходный текст: аааа

Process finished with exit code 0
```

Рис. 2: Результаты программы