

Лабораторная работа №8

Дмитрий К. Федотов - студент группы НКНбд-01-18

16.12.2021

Элементы криптографии.

Шифрование (кодирование)

различных исходных текстов одним
ключом

- Криптография - наука о методах шифрования. Умение шифровать различные исходные тексты одним ключом является необходимым для дальнейшего знакомства с криптографией.

Цель выполнения лабораторной работы

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

- Написать программу, которая должна определять вид шифротекстов при известных открытых текстах и при известном ключе.
- Также эта программа должна определить вид одного из текстов, зная вид другого открытого текста и зашифрованный вид обоих текстов (т.е. не нужно использовать ключ при дешифровке).

- Написал функцию шифрования, которая определяет вид шифротекста при известном ключе и известных открытых текстах.

- Написал функцию дешифровки, которая определяет вид одного из текстов, зная вид другого открытого текста и зашифрованный вид обоих текстов.

- Ответил на вопросы.

Таким образом, я освоил на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.