

Лабораторная работа №8

Силкина Мария Александровна

16.12.2021

Элементы криптографии.

Шифрование (кодирование)

различных исходных текстов одним
ключом

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

1. 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 без использования ключа.
2. Ответить на контрольные вопросы

- Первым шагом написала функцию шифрования, которая определяет вид шифротекстов при известном ключе и известном открытом тексте. В выводе я получила наши изначальные тексты, их представление в шестнадцатеричной системе, рандомный ключ и зашифрованные тексты.
- Далее я создала функцию для дешифрования, которая при знании зашифрованных текстов и одного изначального, может найти второй (неизвестный) текст.

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