

Защита информации.

Лабораторная работа 1. Шифры замены.

В лабораторной работе необходимо зашифровать свою фамилию с помощью следующих шифров:

- шифра Цезаря;
- лозунгового шифра;
- полибианского квадрата;
- шифрующей системы Трисемуса;
- шифра Playfair;
- системы омофонов (допускается для каждой буквы алфавита привести всего по две шифрозамены, т.е. принять, что все буквы имеют одинаковую вероятность появления в текстах);
- шифра Виженера.

При оформлении отчета необходимо привести исходное сообщение (фамилию), таблицу шифрозамен, ключ (если таблица шифрозамен не является ключом) и зашифрованное сообщение.

Контрольные вопросы

1. В чем заключается основная идея криптографических преобразований шифров замены?
2. Перечислите основные разновидности шифров замены.
3. Дайте характеристику разновидностям шифров замены.
4. Назовите основной недостаток шифра однозначной замены.