

ЛАБОРАТОРНАЯ РАБОТА №1

“Исследование классических методов шифрования данных”

Цель работы

Изучить и практически освоить классические методы шифрования данных.

Литература

1. Мельников В.В. «Защита информации в компьютерных системах». М.: Финансы и статистика, 1997. - 368 стр.
2. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. «Защита информации в компьютерных системах и сетях» М.: Радио и связь, 1999. - 328 стр.
3. Штребе М., Перкинс Ч., Монкур М. Безопасность сетей NT4 в 2-х томах. Пер. с англ., В.В. Матвеева: под ред. С.О. Шурчкова М.: МИР, 1999. - 367 стр.

Выполнение работы

Часть 1

1. По краткой теории изучить классические методы шифрования данных.
2. Запустить программу **crypt**. Изучить пользовательский интерфейс и практически освоить методы шифрования данных (сообщения и ключи взять по умолчанию).

Часть 2

1. Зашифровать заданные сообщения (таблицы 1 - 7, номер варианта задаётся преподавателем) с помощью методов шифрования, заложенных в программе.
2. Зашифровать те же сообщения “вручную”, применяя таблицы кода ASC II (таблица 5 – упрощённый вариант; таблица 7 – полный вариант).
3. Сравнить полученные по пунктам 1 и 2 результаты и сформулировать выводы.
4. Составить отчёт по работе.
5. Подготовиться к теоретическому зачёту.

Содержание отчёта

1. Цель работы.
2. Результаты выполнения работы.