Лабораторная работа №2

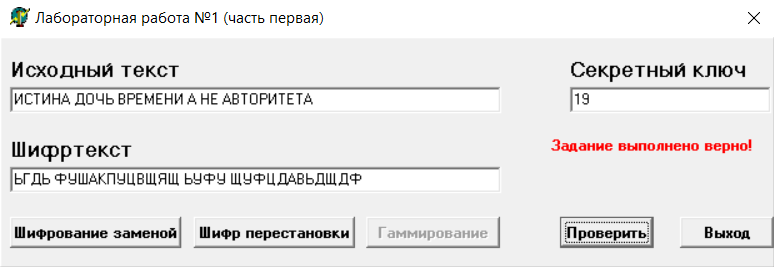
Шифрование в ручном режиме

Работу выполнили:

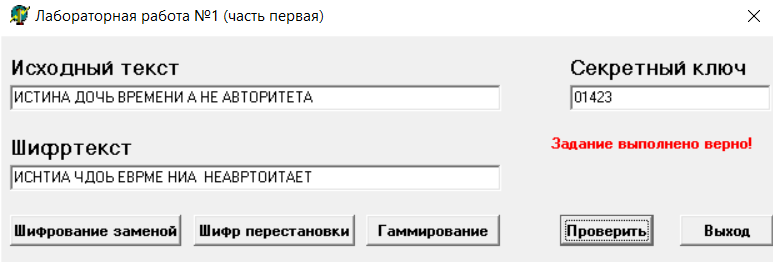
Орехва В. Э.

Балан К. А.

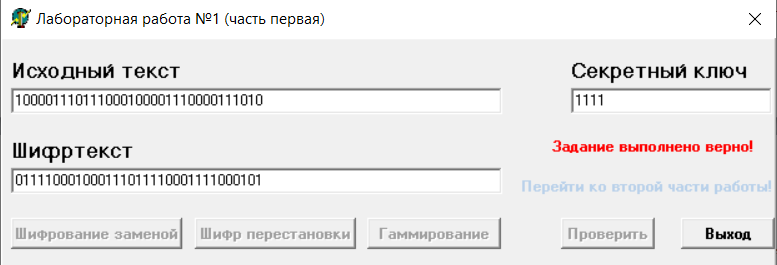
Задание №1



Задание №2



Задание №3



Ответы на вопросы

**1). Перечислить задачи, решаемые криптографическими системами**

1). Шифрование данных: криптографические системы используются для защиты конфиденциальности данных путем их преобразования в шифрованный вид.

2). Цифровая подпись: криптографические системы позволяют проверять подлинность и целостность документов или сообщений с помощью цифровой подписи.

3). Аутентификация: криптографические протоколы используются для проверки подлинности пользователей и устройств, обеспечивая защиту от несанкционированного доступа.

4). Анонимность: криптографические системы могут обеспечивать анонимность при передаче данных или проведении транзакций.

5). Контроль целостности: криптографические методы обеспечивают возможность проверки целостности данных, чтобы обнаружить любые изменения или подделки.

**2). Перечислить классы шифров по стойкости**

1). Симметричные шрифты

2). Ассиметричные шрифты

3). Хеш-функции

4). Криптографические протоколы

**3). Дать определение безусловно стойкого шифра**

Безусловно стойкий шифр - это шифр который не может быть взломан путем анализа шифротекста или криптоанализа, независимо от доступных ресурсов, времени или вычислительных возможностей злоумышленника

**4). Дать определение вычислительно стойкого шифра**

Вычислительно стойкий шифр - это криптографический алгоритм, который обладает свойством устойчивости к различным методам взлома, включая атаки перебором, статистический анализ и другие вычислительные методы.