**Лабораторные работы**

**1. Шифрование файлов**

Изучите теоретические сведения

Реализуйте программное средство шифрования и дешифрования текстовых файлов при помощи **Шифра Цезаря**, (шифра сдвига, **кода Цезаря).**

**2. Алгоритм DES**

Изучите теоретические сведения, содержащие требования к реализации алгоритма DES.

Реализуйте алгоритм шифрования DES следующих видов:

1. **Классический DES;**
2. **Тройной DES;**
3. **Тройной DES с двумя ключами;**
4. **Алгоритм ГОСТ 28147**

*Режим ECB*

*Режим CBC*

*Режим CFB*

*Режим OFB*

**3. Блочные шифры. AES.**

Изучите теоретические сведения, содержащие требования к реализации блочных шифров.

Реализуйте алгоритм блочного шифрования AES.

**4. Компьютерная реализация криптографии с открытым ключом на примере RSA.**

Изучите теоретические сведения, содержащие требования к реализация хэш-функций.

Реализуйте криптографическую систему шифрования на основе алгоритма RSA.

**5 Компьютерная реализация хэш-функций на примере MD5.**

Изучите теоретические сведения, содержащие требования к реализация хэш-функций.

Програмно реализуйте **хэш-функцию MD5**.

**6. Цифровая подпись**

Изучите теоретические сведения, содержащие требования к цифровой подписи

Програмно реализуйте отечественный стандарт цифровой подписи ГОСТ 3410.

**7. Криптография с использованием эллиптических кривых.**

Изучите теоретические сведения:

Аналог алгоритма Диффи-Хеллмана обмена ключами;

Алгоритм цифровой подписи на основе эллиптических кривых ECDSA;

Шифрование/дешифрование с использованием эллиптических кривых.

Реализуйте алгоритм шифрования/дешифрования на основе эллиптических кривых.