**Гаммирование**

***Цель работы***: освоить метод шифрования гаммированием.

***Задание:***

* Разработать алгоритм для шифрования сообщений гаммированием;
* Разработать алгоритм для дешифрования сообщений зашифрованных гаммированием;
* Составить приложение для шифрования/дешифрования текстовой строки с использованием метода гаммирования;
* Составить приложение для шифрования/дешифрования отдельного файла с использованием метода гаммирования.

***Выполнение работы***:

Для решения поставленной задачи мною был выбран язык TypeScript

Класс для шифрования содержит в себе одну публичную функцию

/\*\*

     \* Encode function

     \*

     \* @param source data to encode

     \* @param key encryption key

     \*/

    encode(source: Buffer, key: Buffer): Buffer;

Функция encode сдвигает каждый байт по формуле

Bi = (Ai + Ki) mod 2 = Ai ⊕ Ki

где

* Ai - исходный бит;
* Ki - бит ключа;
* Bi - зашифрованный бит.

        const result: Uint8Array = source.map(

            (byte: number, index: number) =>

                byte ^ key[index % key.length]

        );

Декодирование происходит с помощью этой же функции

Полный код класса: <https://github.com/wbydc/ISUCT-data-protection/blob/master/src/encoders/lab3/Encoder.ts>

Как запустить и протестировать: <https://github.com/wbydc/ISUCT-data-protection/blob/master/README.md>