**Полиалфавитный шифр Виженера**

***Цель работы***: освоить шифрования методами замены.

***Задание:***

* Разработать алгоритм для шифрования сообщений полиалфавитным шифром Виженера;
* Разработать алгоритм для дешифрования сообщений зашифрованных полиалфавитным шифром Виженера;
* Составить приложение для шифрования/дешифрования текстовой строки с использованием полиалфавитного шифра Виженера;
* Составить приложение для шифрования/дешифрования отдельного файла с использованием полиалфавитного шифра Виженера.

***Выполнение работы***:

Для решения поставленной задачи мною был выбран язык TypeScript

Класс для шифрования содержит в себе две публичных функции

/\*\*

     \* Encode function

     \*

     \* @param source data to encode

     \* @param key encryption key

     \*/

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

    /\*\*

     \* Decode function

     \*

     \* @param source data to encode

     \* @param key encryption key

     \*/

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

Функция encode сдвигает каждый байт по формуле

Bi = (Ai + Ki) mod 256

где

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

        const result: Uint8Array = source.map(

            (byte: number, index: number) =>

                (byte + key[index % key.length]) % 256

        );

Функция decode сдвигает каждый байт по формуле

Ci = (256 + Bi - Ki) mod 256

* Bi - зашифрованный байт;
* Ki - байт ключа;
* Ci - расшифрованный байт.

        const result: Uint8Array = source.map(

            (byte: number, index: number) =>

                (256 + byte - key[index % key.length]) % 256

        );

Полный код класса: <https://github.com/wbydc/ISUCT-data-protection/blob/master/src/encoders/lab2/Encoder.ts>

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