Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий

Кафедра информационных систем и технологий

**Лабораторная работа № 4**

«Исследование криптографических шифров на основе подстановки (замены) символов»

Выполнил:

Студент: Лысков К.Е.

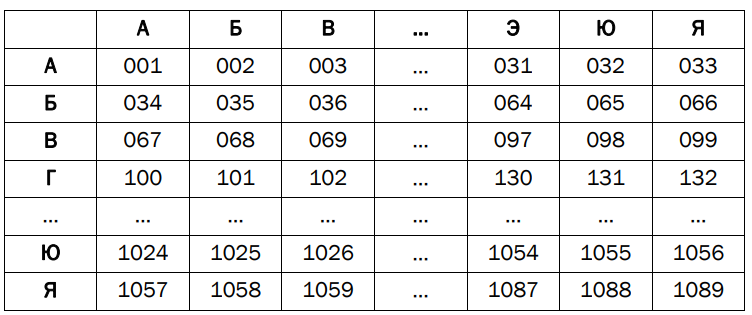
ФИТ 3 курс 4 группа

Преподаватель: Копыток Д.В.

Минск 2023

1) Шифр Порты:

Шифр представляется в виде таблицы. Наверху горизонтально и слева вертикально записывается стандартный алфавит. В ячейках таблицы записываются числа в определенном порядке. Фрагмент таблицы для алфавита русского показан ниже.

****

Шифрование выполняется парами букв исходного сообщения. Перваябуква пары указывает на строку, вторая – на столбец. В случае нечетного количества букв в сообщении Мi к нему добавляется вспомогательный символ, например, «А».

Для процедуры расшифрования используется эта же таблица. Нужно найти ячейку с вашим набором символов и сопоставить ей пару букв. Первая буква пары – строка, вторая – столбец.

Код реализации этого шифра на языке Javascript:





2) Шифр Цезаря с ключевым словом. Является одноалфавитной системой подстановки. Особенностью этой системы является использование ключевого слова (лозунга) для смещения и изменения порядка символов в алфавите подстановки (желательно, чтобы все буквы ключевого слова были различными). Ключевое слово пишется в начале алфавита подстановки.

Код реализации этого шифра на языке Javascript:



