Федеральное государственное бюджетное образовательное учреждение

высшего образования

«Уфимский государственный нефтяной технический университет»

Кафедра вычислительной техники и инженерной кибернетики

Лабораторная работа №5

по дисциплине Информационная безопасность

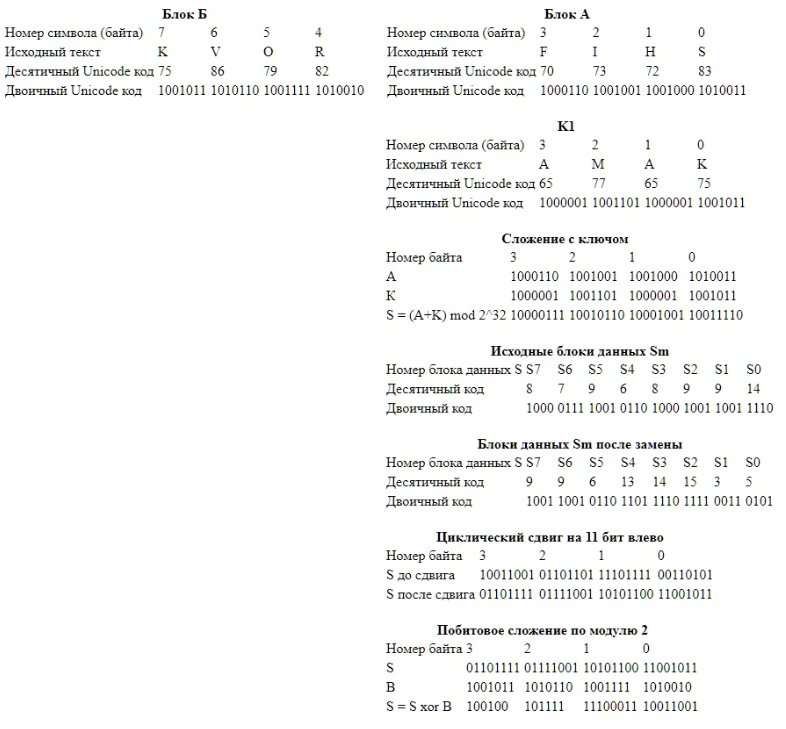
Алгоритм шифрования ГОСТ 28147-89

Выполнил: студент гр. БПОи-16-01 К. И. Камалов

Проверил: кандидат технических наук, доцент Т.Х. Агишев

Уфа, 2019

**Задание.** Для заданных 64 битов данных – в текстовом виде «ШИФРОВКА» (или «D8C8D4D0CEC2 CAC0» в шестнадцатеричном коде), с помощью ключа состоящему из Вашей фамилии (повторенное до размера в 32 символа (256 бит)), произвести один основной шаг (раунд) криптопреобразования по ГОСТ 28147-89. Привести пошаговые расчеты произведенных криптопреобразований в электронной или бумажной форме.

****

**Выводы по работе:**

В ходе выполнения данной лабораторной работы был изучен алгоритм шифрования ГОСТ 28147-89. Также был произведен один основной шаг (раунд) криптопреобразования по ГОСТ 28147-89.