**Отчет по лабораторной работе № 10**

**Блочные шифры**

**Григорович Алина Александровна, 21 группа**

**Вариант 5**

**Теория**

DES (Data Encryption Standard, стандарт шифрования данных) -

федеральный стандарт шифрования США в 1977-2001 годах для

использования во всех несекретных правительственных каналах

связи (FIPS PUB 46 «Data Encryption Standard»). Несмотря на то, что в

настоящий момент федеральным стандартом шифрования США

является Rijndael (AES - Advanced Encryption Standard, расширенный

стандарт шифрования; тип – подстановочно - перестановочная сеть),

рассмотрение DES позволяет понять основные принципы блочного

шифрования.

В алгоритме, лежащем в основе DES, используются методы

замены, перестановки и гаммирования (сложение по модулю 2).

Открытое сообщение разбивается на блоки длиной 64 бита. Если

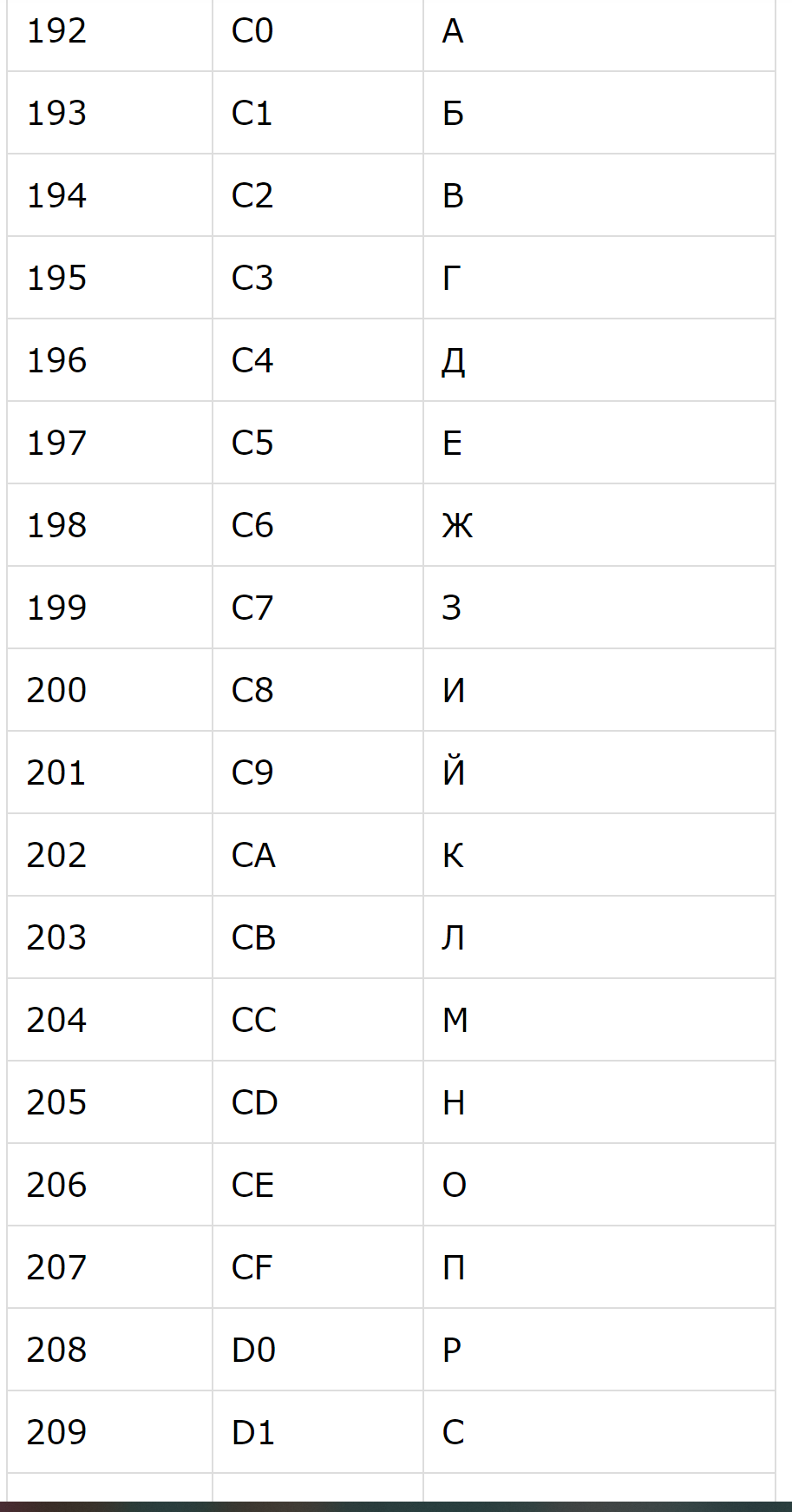
длина сообщения не кратна 64, оно дополняется справа недостающим

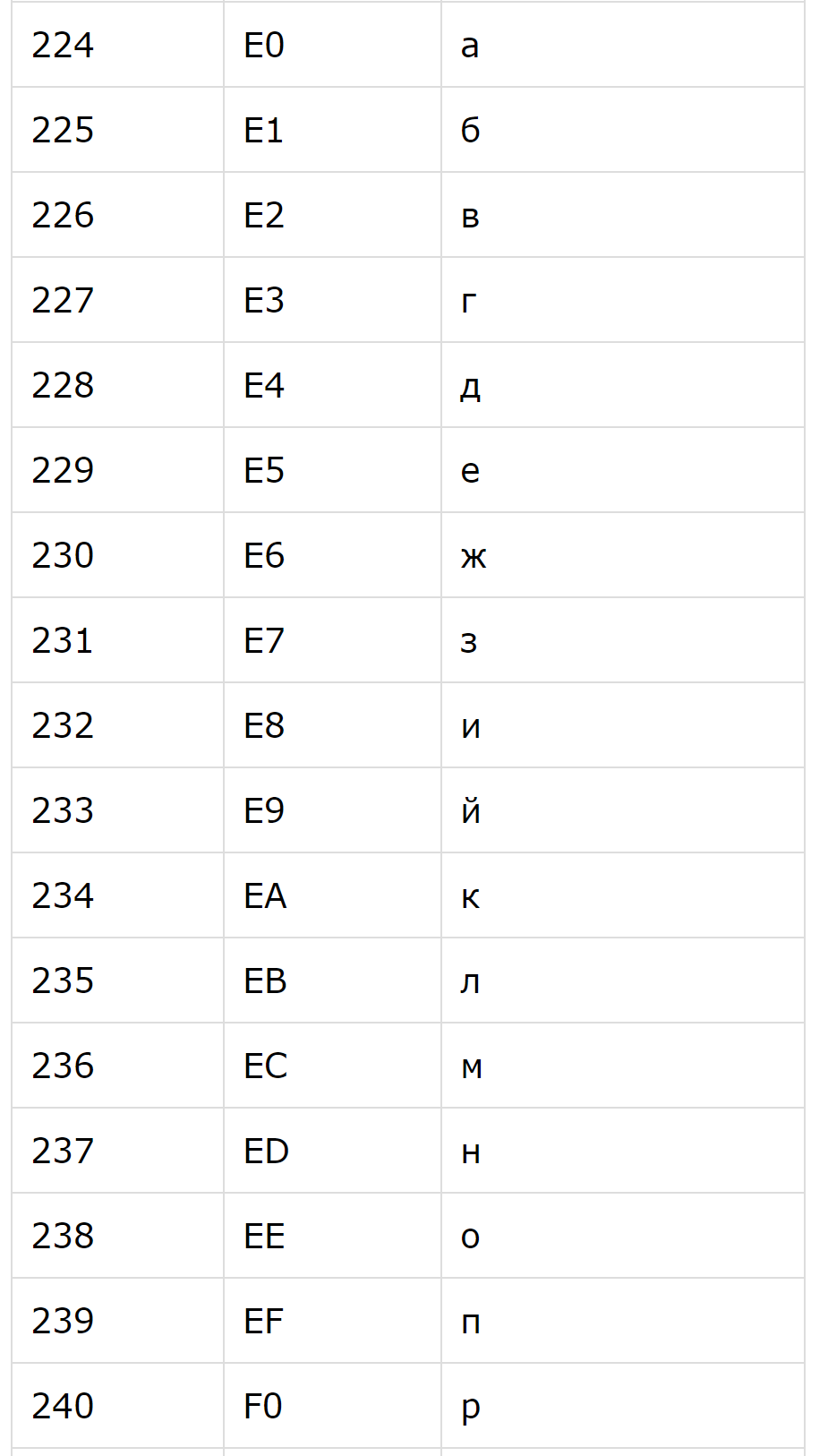
количеством битов.

Данные шифруются ключом длиной 56 бит.

Алгоритм решения, следующий:

**Перекодировка в Windows-1251**





После перекодировки получаем следующее:

195 240 232 227 238 240 238 226 (Григоров)

Перевод в двоичную систему счисления ШИФРА:

11000011 11110000 11101000 11100011 11101110 11110000 11101110 11100010

Перевод в двоичную систему счисления КЛЮЧА:

11000011 11110000 11101000 11100011 11101110 11110000 11101110 (Григоро)

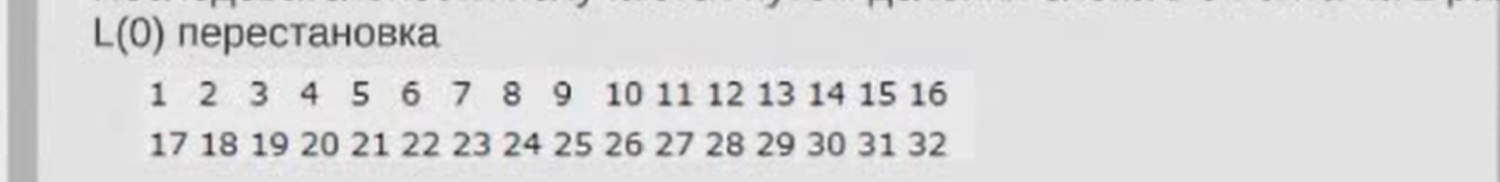
***Шаг 1. Таблица первоначальной перестановки***

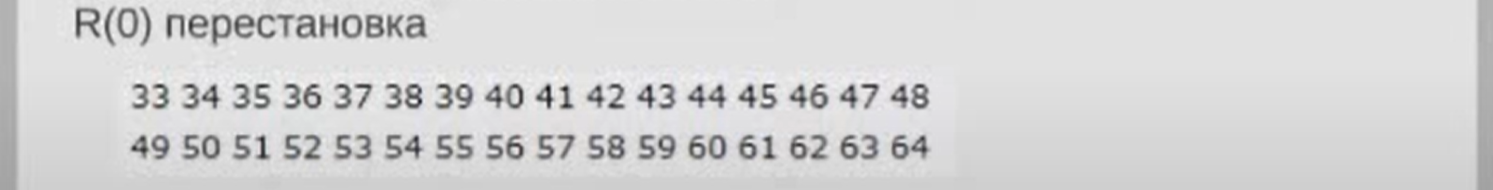
Согласно таблице первоначальной перестановки, получаем следующее:



IP: 1111111100100010010100010000100111111111111111100101010011011001

***Шаг 2. Делим полученную последовательность согласно таблицам. Последовательности получаются путем деления блока в 64 бита на две равные части:***

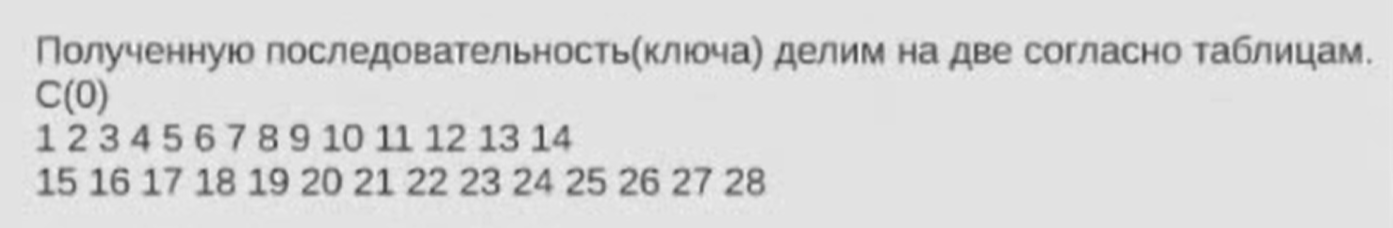


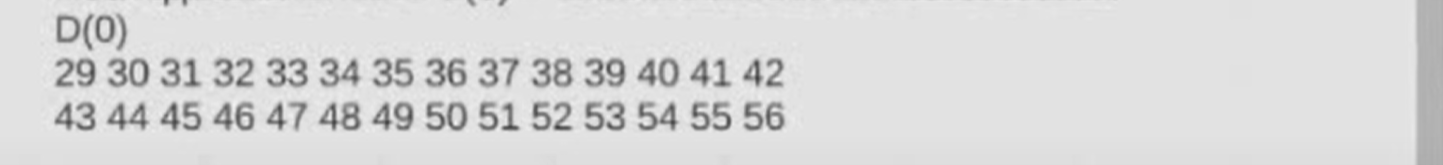


***Шаг 3. Функция выбора и перестановка последовательности (преобразование ключа шифрования)***



***Шаг 4. Получение последовательностей C0 и D0.***





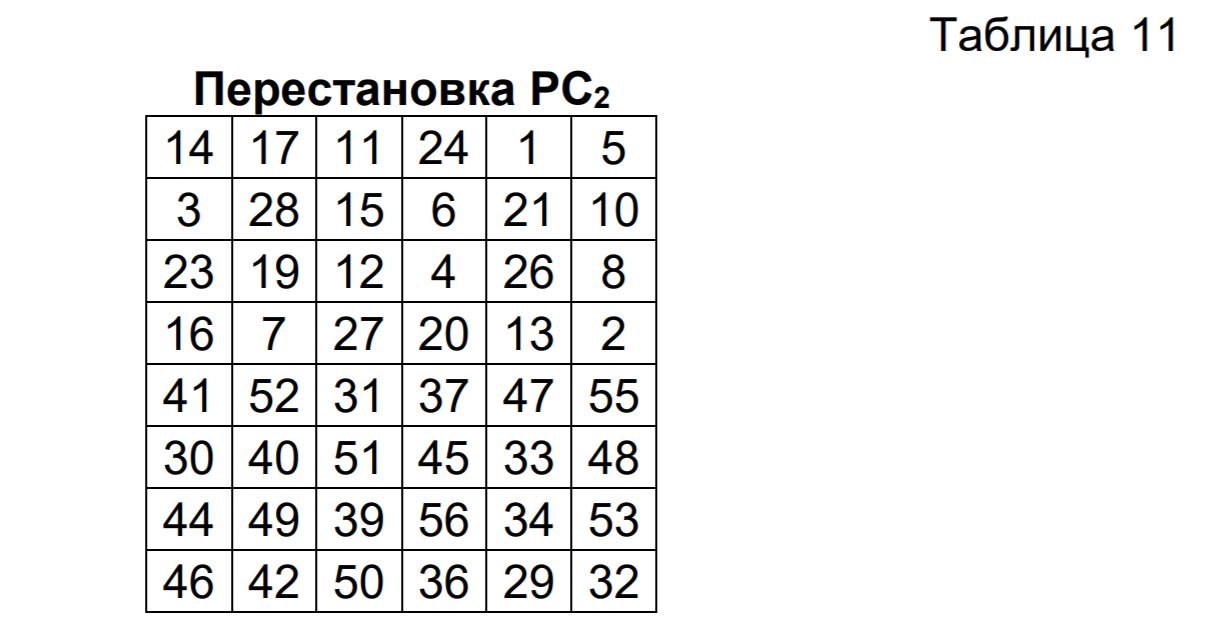
***Шаг 5. Получение последовательности C(i) по следующей таблице:***



***Шаг 6. По той же таблице получаем последовательности D(i)***

***Шаг 7. Получение последовательности K(i)***

Для получения последовательности K(i) проведем конкатенацию последовательностей C(i) и D(i). В полученной последовательности C(i)D(i) переставим биты согласно таблице:



***Шаг 8. Функция E (шифрование, перестановка с расширением)***

В каждом раунде i старшая половина Hi-1 блока модифицируется

путем побитового прибавления к ней по модулю 2 () результата

вычисления функции шифрования f, зависящей от младшей половины

блока Li–1 и 48-битового ключевого элемента ki. Ключевой элемент ki

вырабатывается из ключа шифрования. Между раундами старшая и

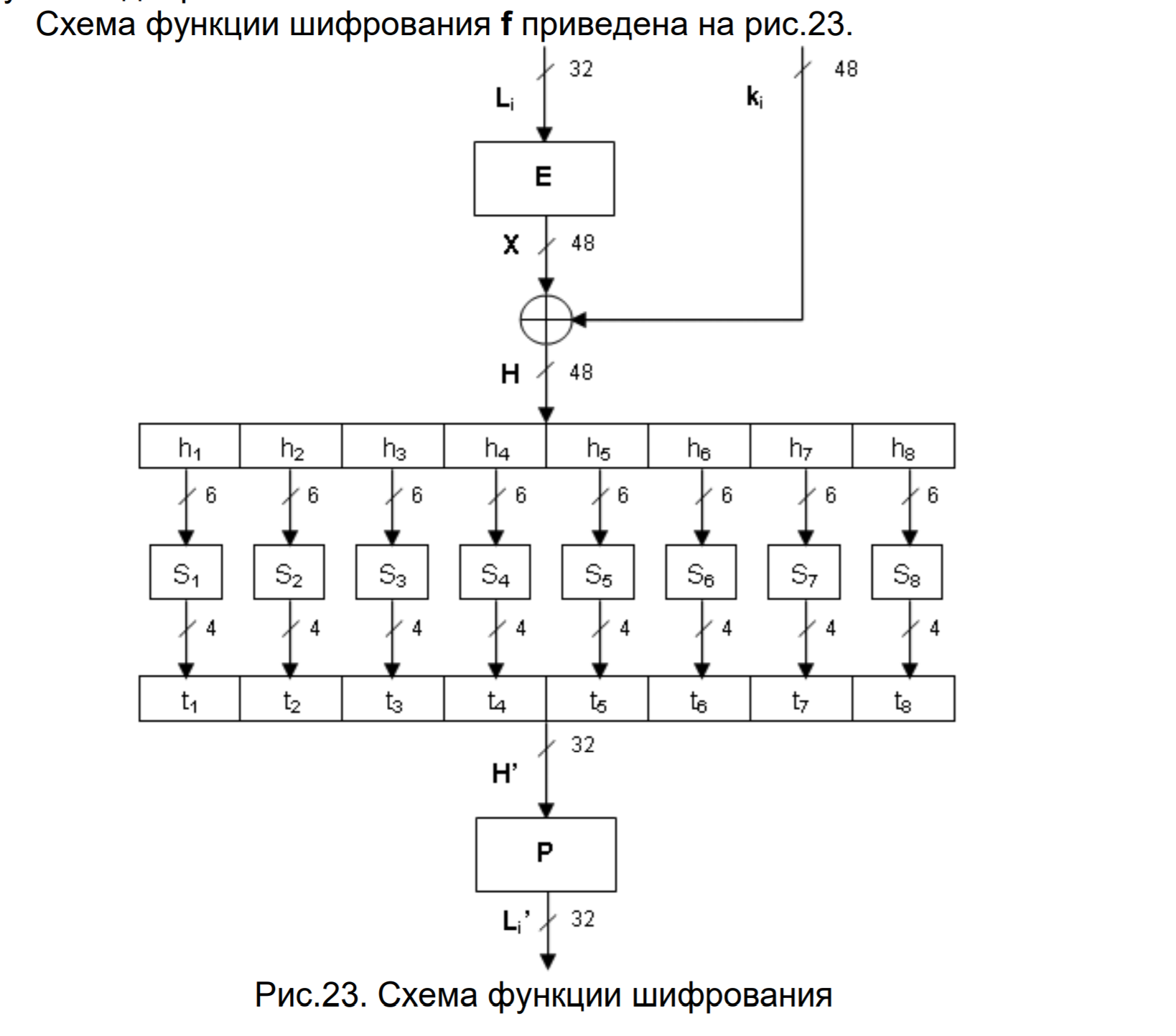
младшая половины блока меняются местами. В последнем раунде

происходит то же самое за исключением обмена значениями

половинок блока



Расширение

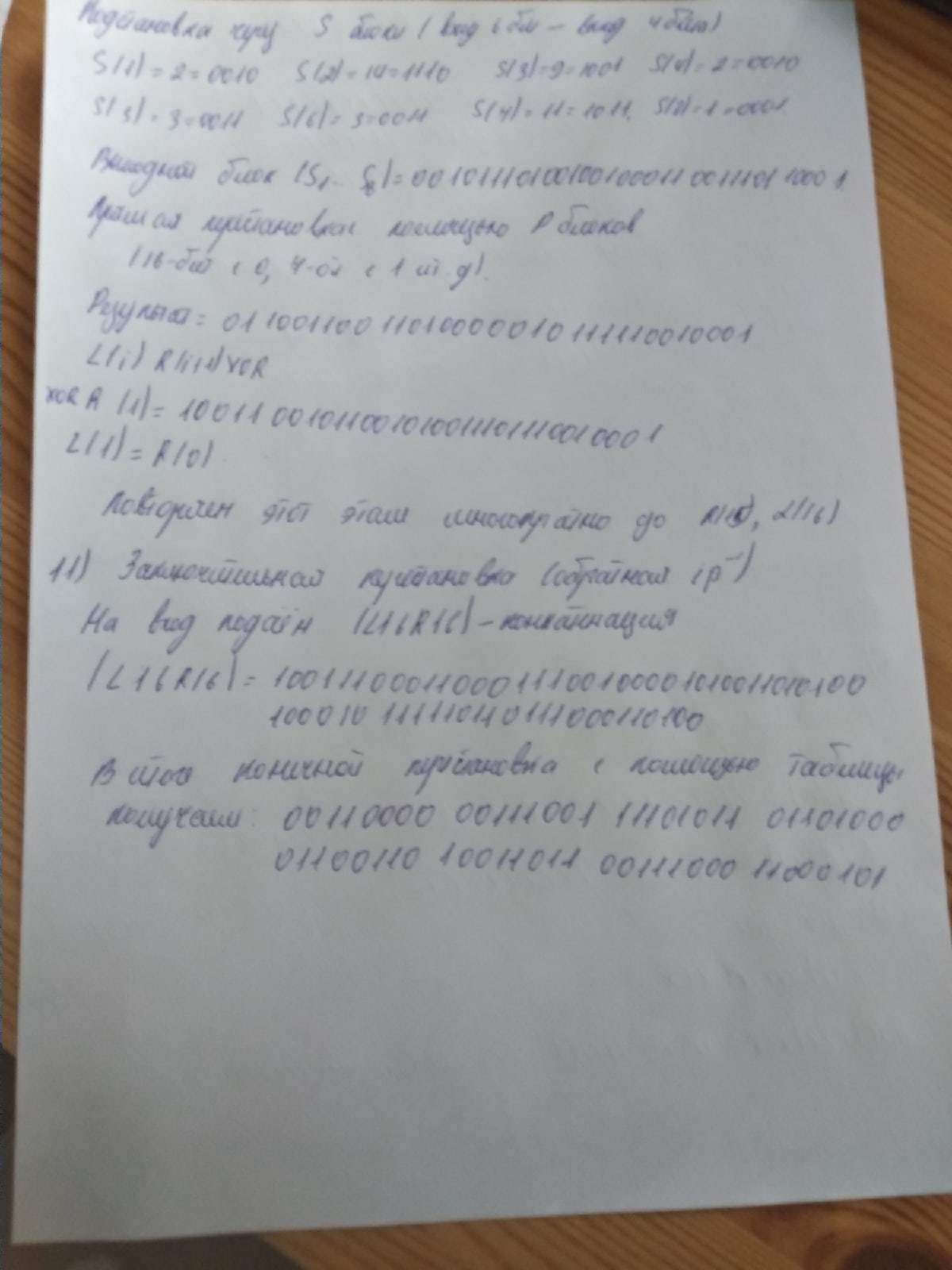
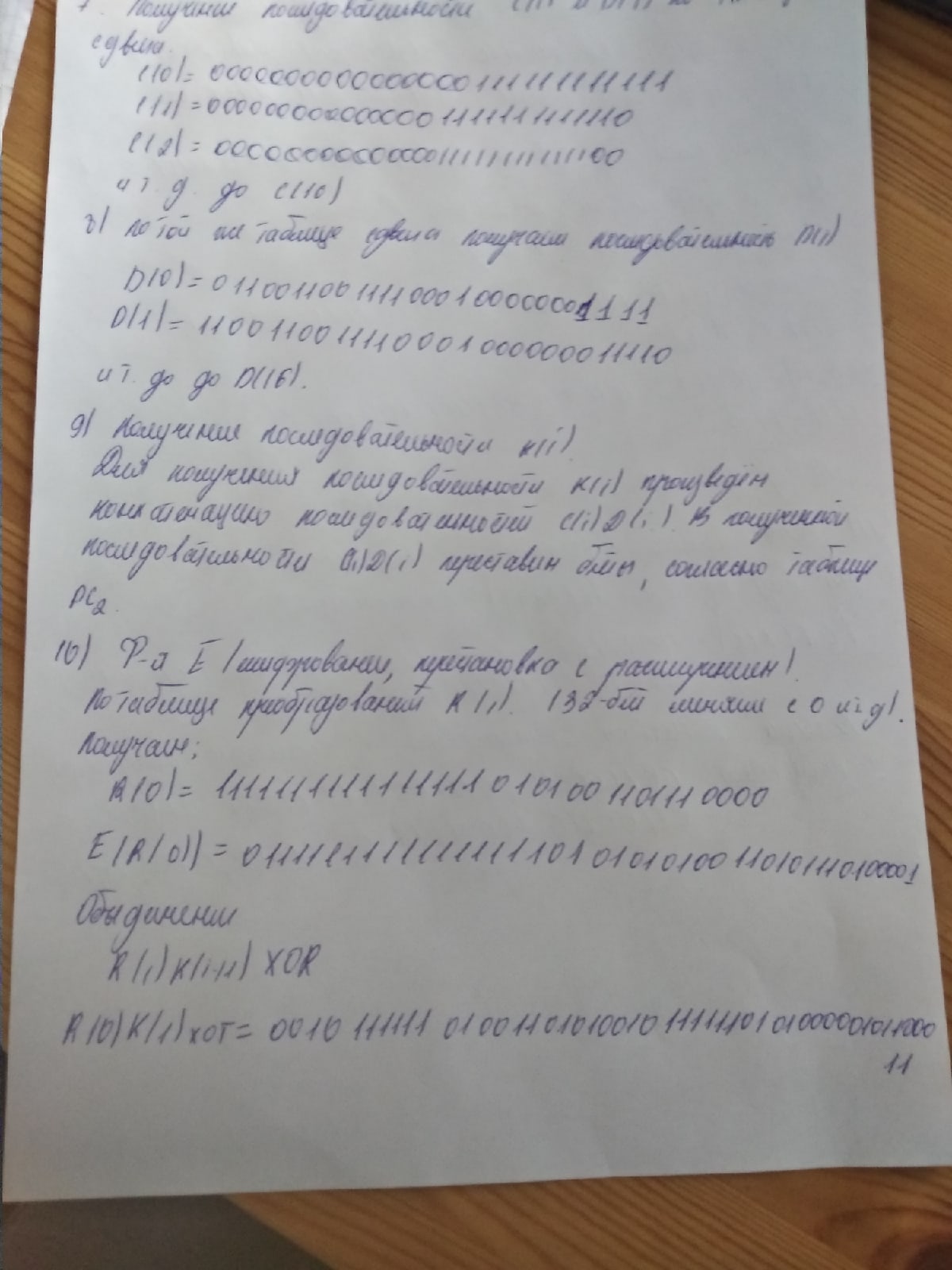
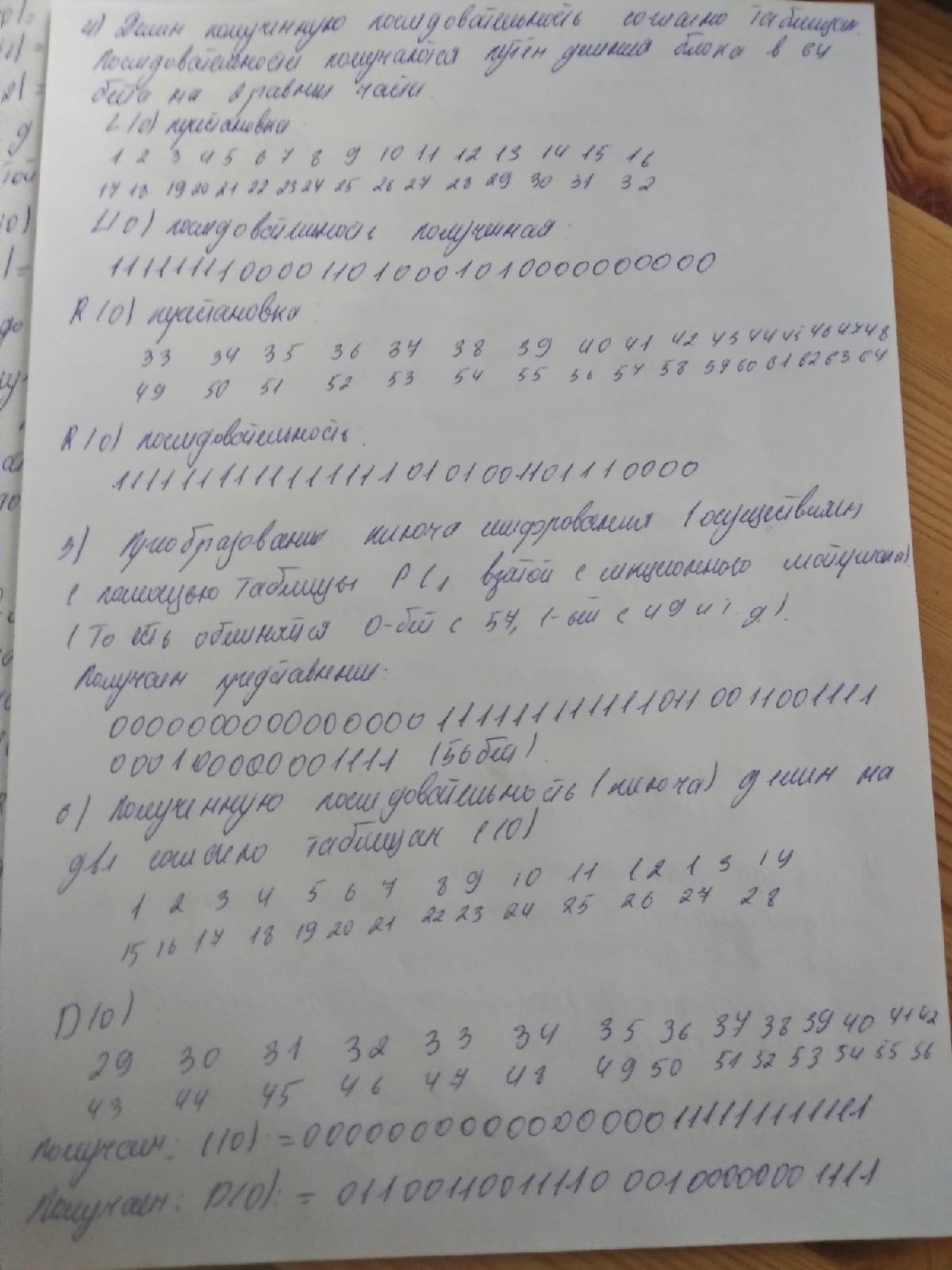
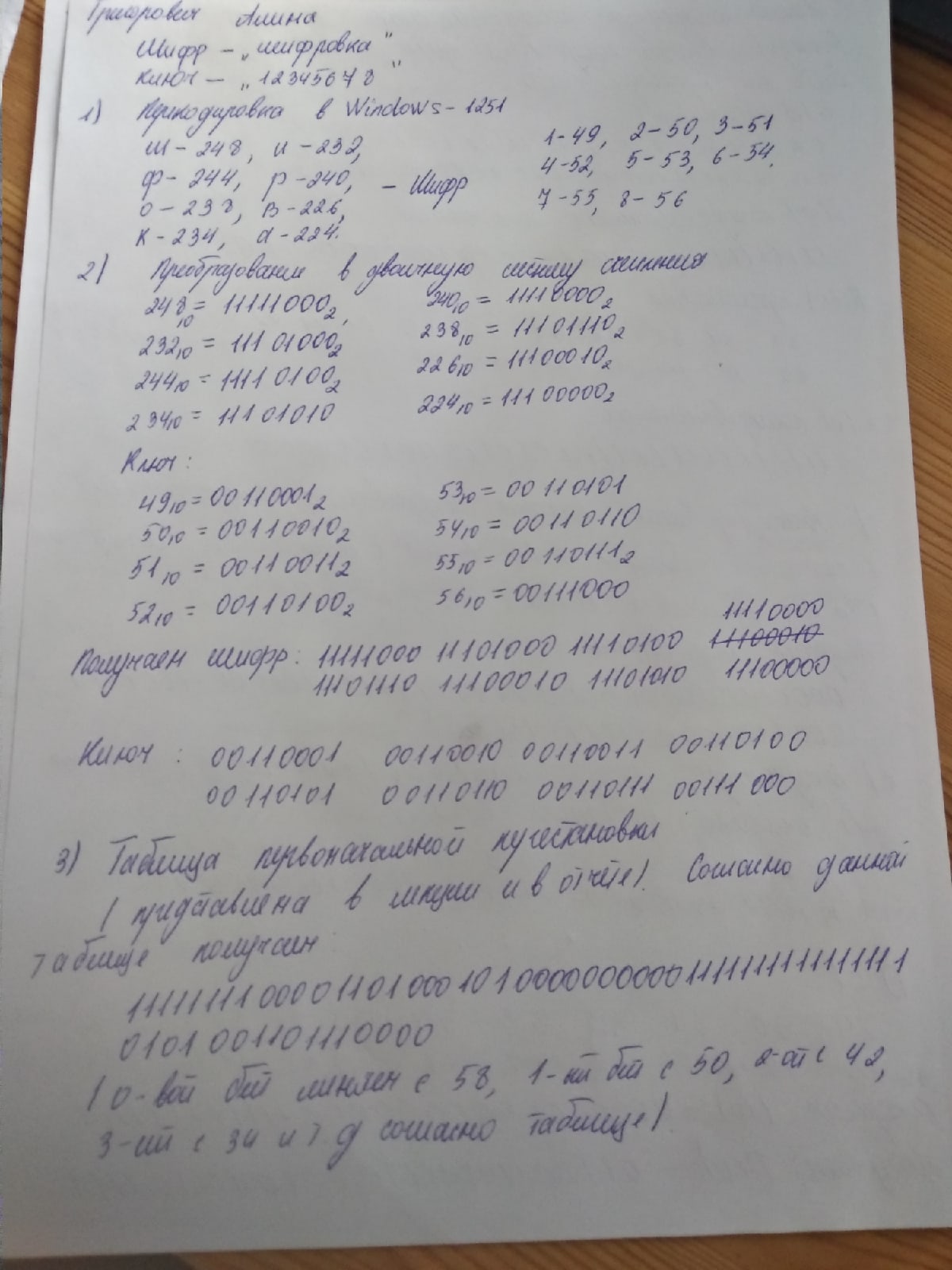


***Шаг 9. Заключительная перестановка***

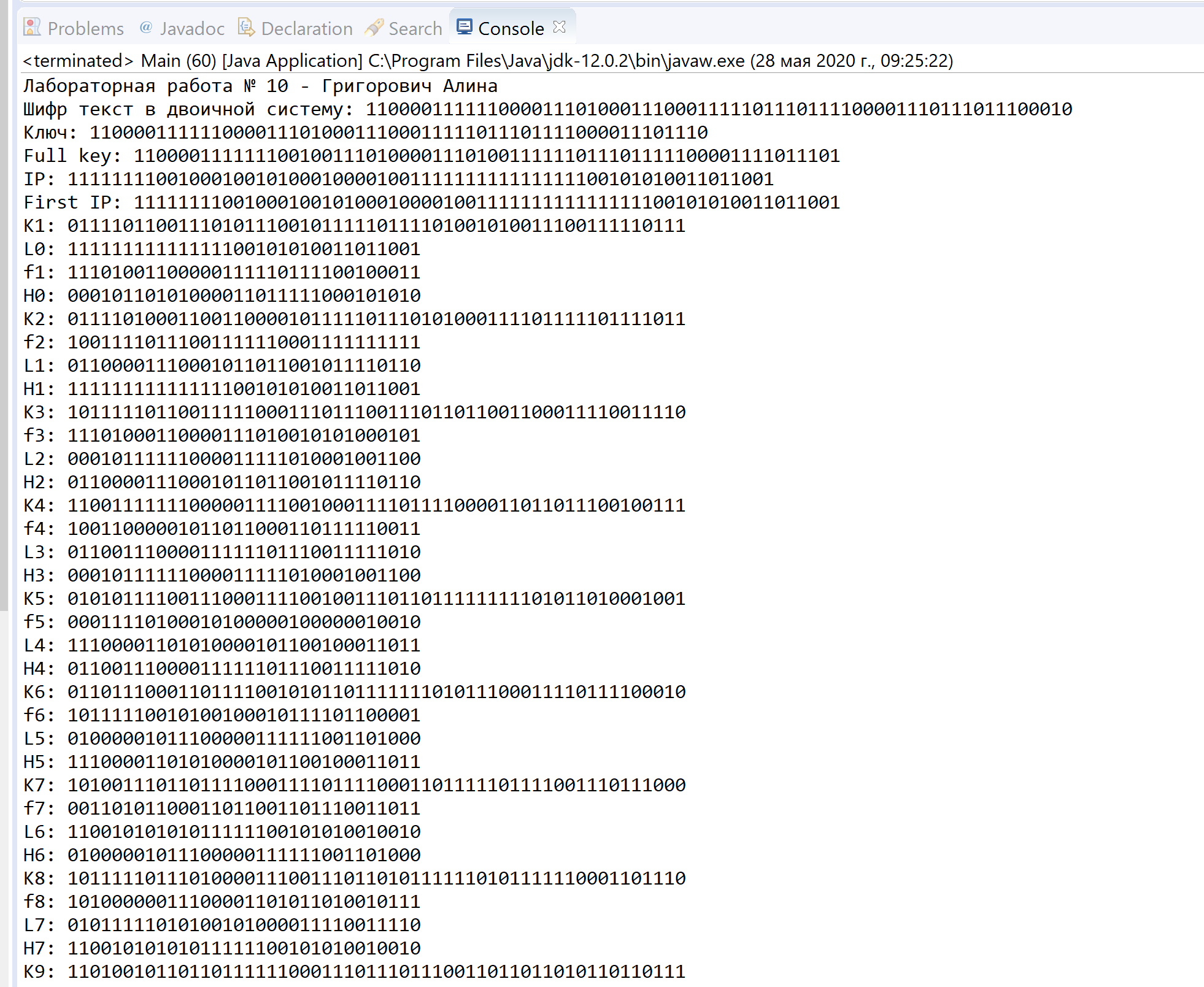


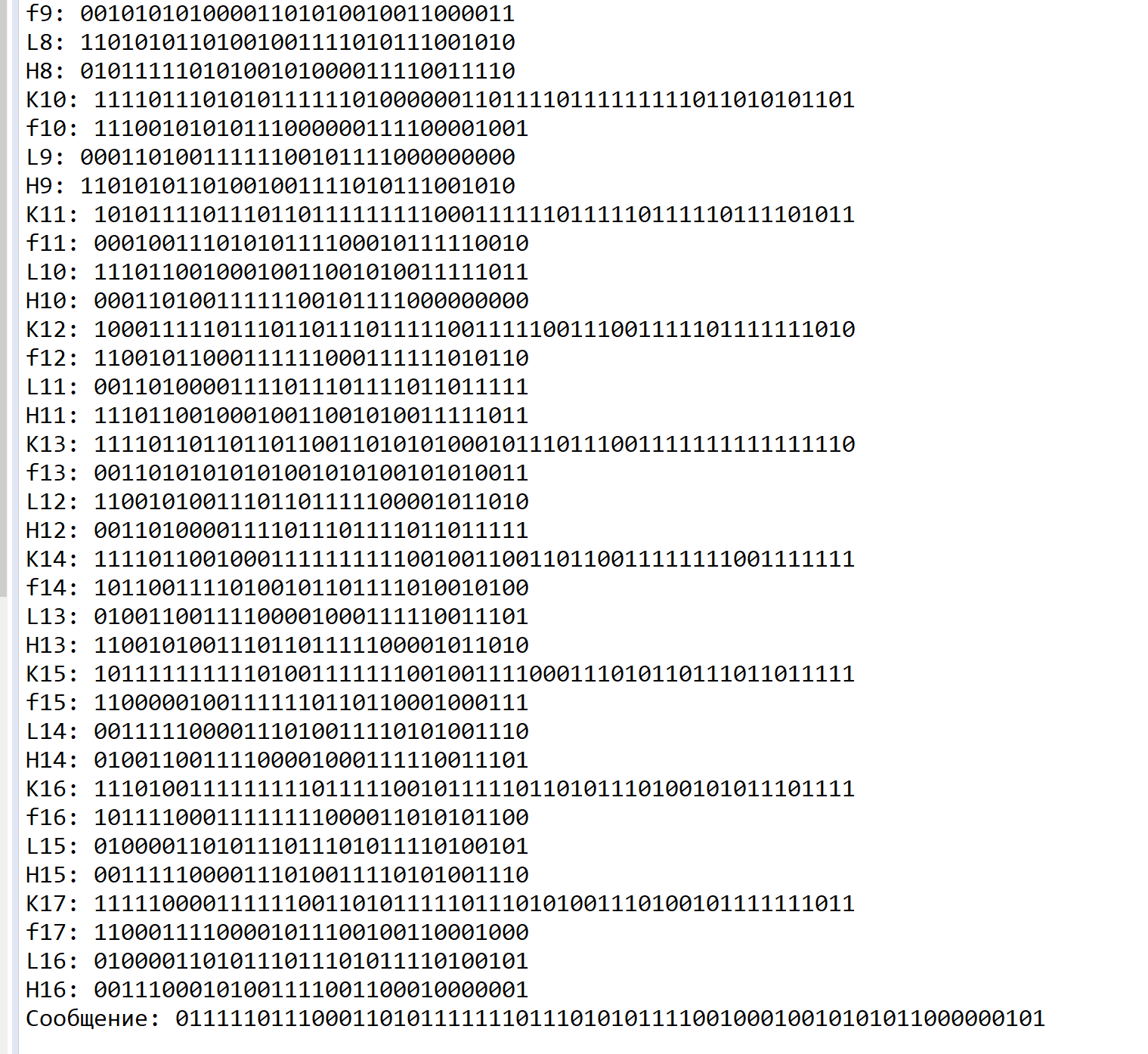
Для того, чтобы убедиться в работоспособности, рассмотрим два примера (один – произвольный, один – из условий лабораторной работы)

Для примера возьмем шифр-тест «шифровка», а в качества ключа последовательность: «12345678».



***Листинг работы программы (Пример № 1 – шифр-текст 8 букв фамилии – из условия лабораторной):***





***Листинг реализации вручную (примера из лабораторной)***:

