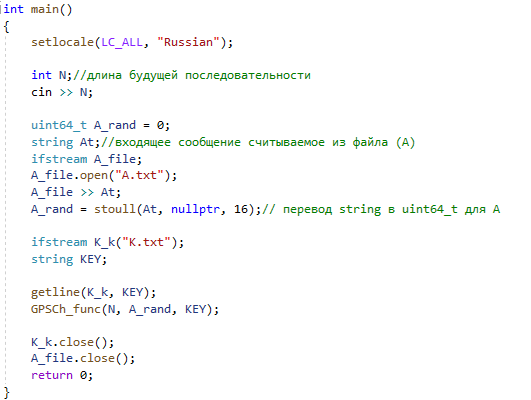
**Инструкция к GSPCh\_MAGMA на языке C++**

(Генератор случайной последовательности чисел на основе ГОСТа 3412-2015 для блочного шифрования с длиной блока n = 64 бит)

# **1.Главная функция**



На вход в переменную N пользователем задается количество блоков преобразования или длина будущей последовательности случайных чисел.

A\_rand-параметр для обращения к методу GPSCh\_func(),в котором хранится 64 битное сообщение для шифрования.

At-64 битное сообщение, поступающее в программу.

A\_file-переменная, в которую считывается из файла сообщение на шифрование.

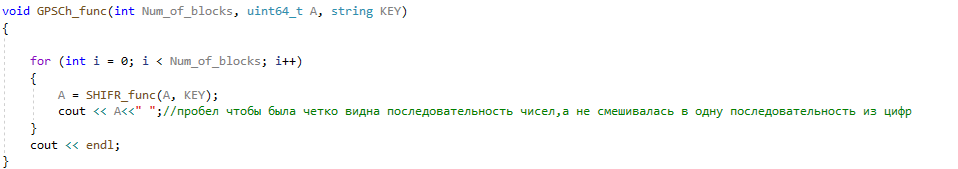
K\_k-переменная, в которую считывается из файла ключ для шифрования.

KEY-переменная, в которой хранится ключ для шифрования.

В целом, в программу требуется передать 3 параметра: N, A\_rand, KEY

Главная функция не обязательна и подлежит изменениям для дальнейшего использования функций.

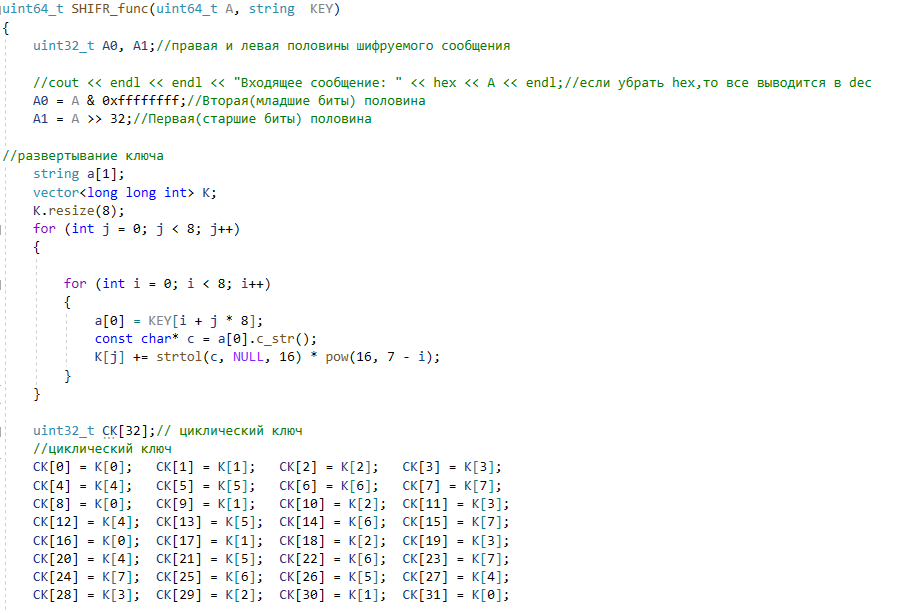
# **2.Метод GPSCh\_func()**

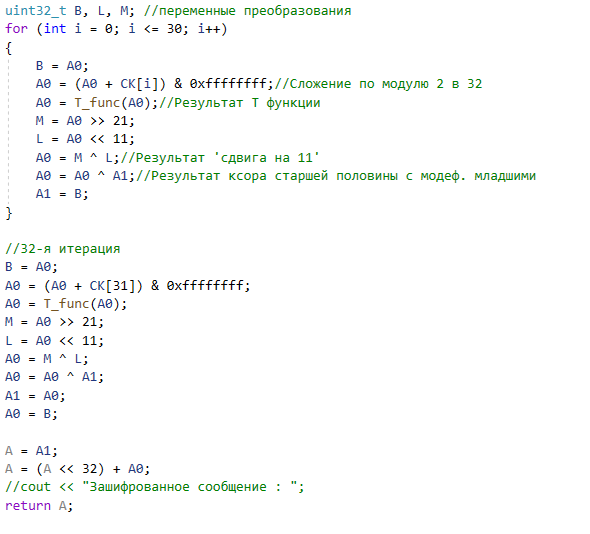


На вход поступают три параметра Num\_of\_blocks, A, KEY имеют соответственные значения, как переменные N, A\_rand, KEY, указанные выше.

В данном методе происходит циклическиое обращение к методу SHIFR\_func() , которое будет повторяться N раз.

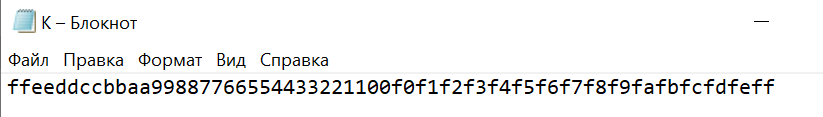
# **3.Метод SHIFR\_func()**





Данный метод используется для реализации алгоритма шифрования МАГМА. На вход в метод поступает изменяемая переменная А (изначально открытый текст),которая в последствии разделится на 2 равные части(A0 и A1).

В методе также происходит считывание ключа(переменная К) из файла с фиксированной длиной - 256 бит. Далее он делится на 8 частей по 32 бита и переносится в массив K[8] для дальнейшей работы(согласно ГОСТу)

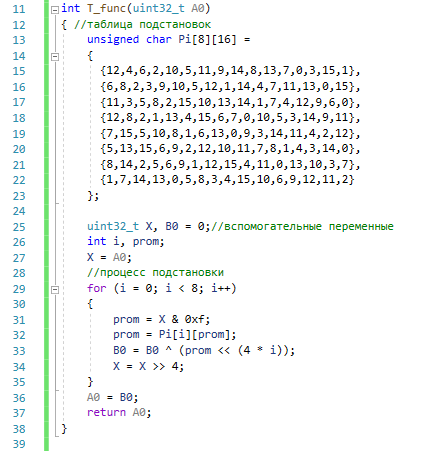


CK-циклический ключ,который повторяет значения K каждые 8 раз по циклу.

Далее согласно ГОСТу проводятся преобразования с половинками шифруемого текста, после чего A0 и A1 “склеиваются” и в метод GPSCh\_func() возвращается уже зашифрованный текст.

# **4. Функция T\_func()**

Метод SHIFR\_func() в двух местах(85 и 96 строки) обращается к функции T\_func()



Данная функция осуществляет некую подстановку новых значений на “старые места” в одной из половинок шифруемого текста(A0)(согласно ГОСТу).

А затем возвращает уже измененную половинку в метод шифрования для дальнейшей работы.

# **5. Получение результата**

Вводим нужное количество блоков преобразования.

Программа выводит случайно сгенерированную последовательность.

