**Гончаренко Андрей Дмитриевич, 15 гр. 5 вариант**

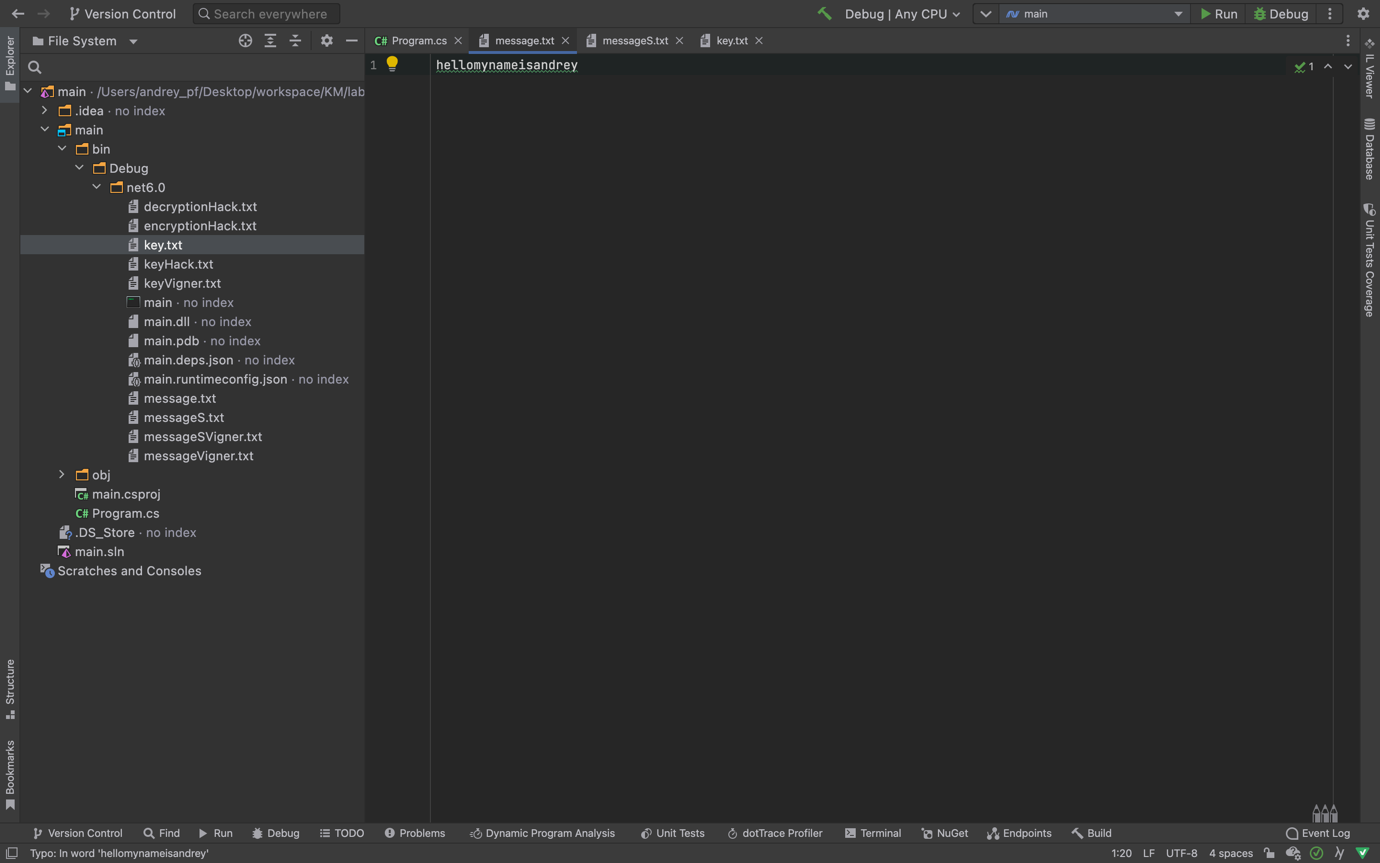
**Шифр сдвига** - это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется символом, находящимся на некотором постоянном числе позиций левее или правее него в алфавите. Например, в шифре со сдвигом вправо на 3, А была бы заменена на Г, Б станет Д, и так далее.

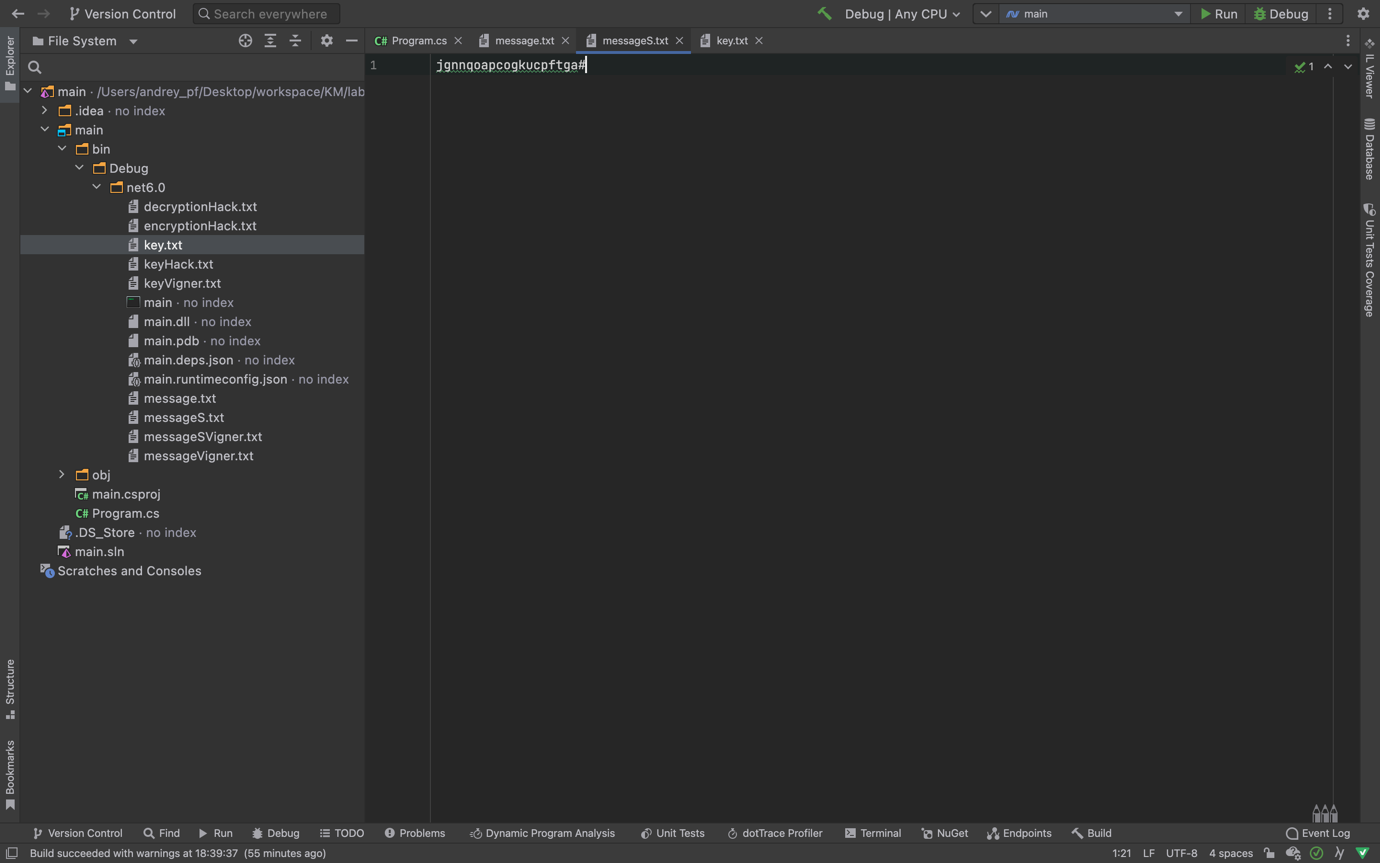
**Математическая модель**

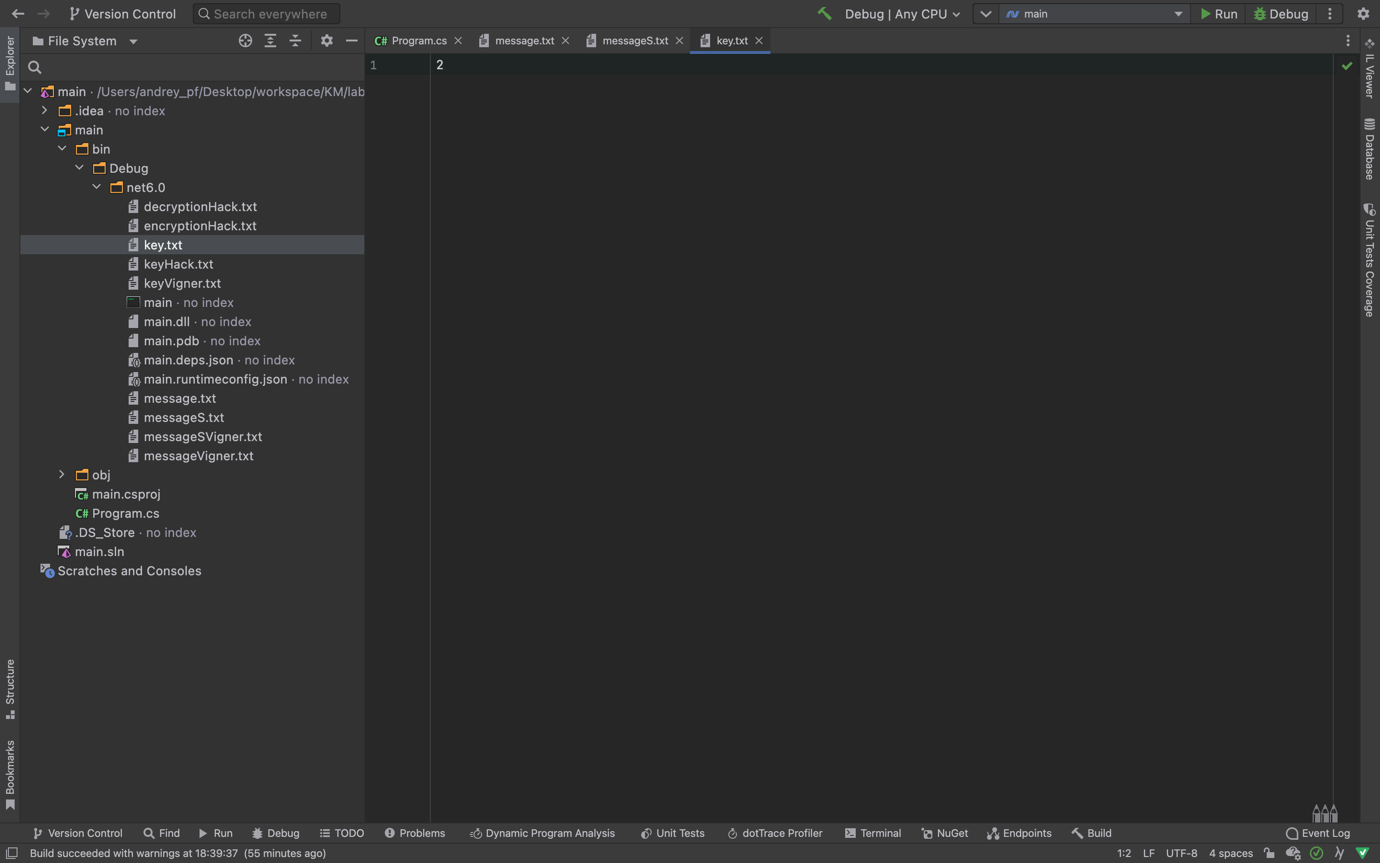
;

,

где - символ открытого текста, - символ шифрованного текста, -мощность алфавита, а - ключ.







Код в *Приложении 1 и в Goncharenko\_15\_2.cs.*

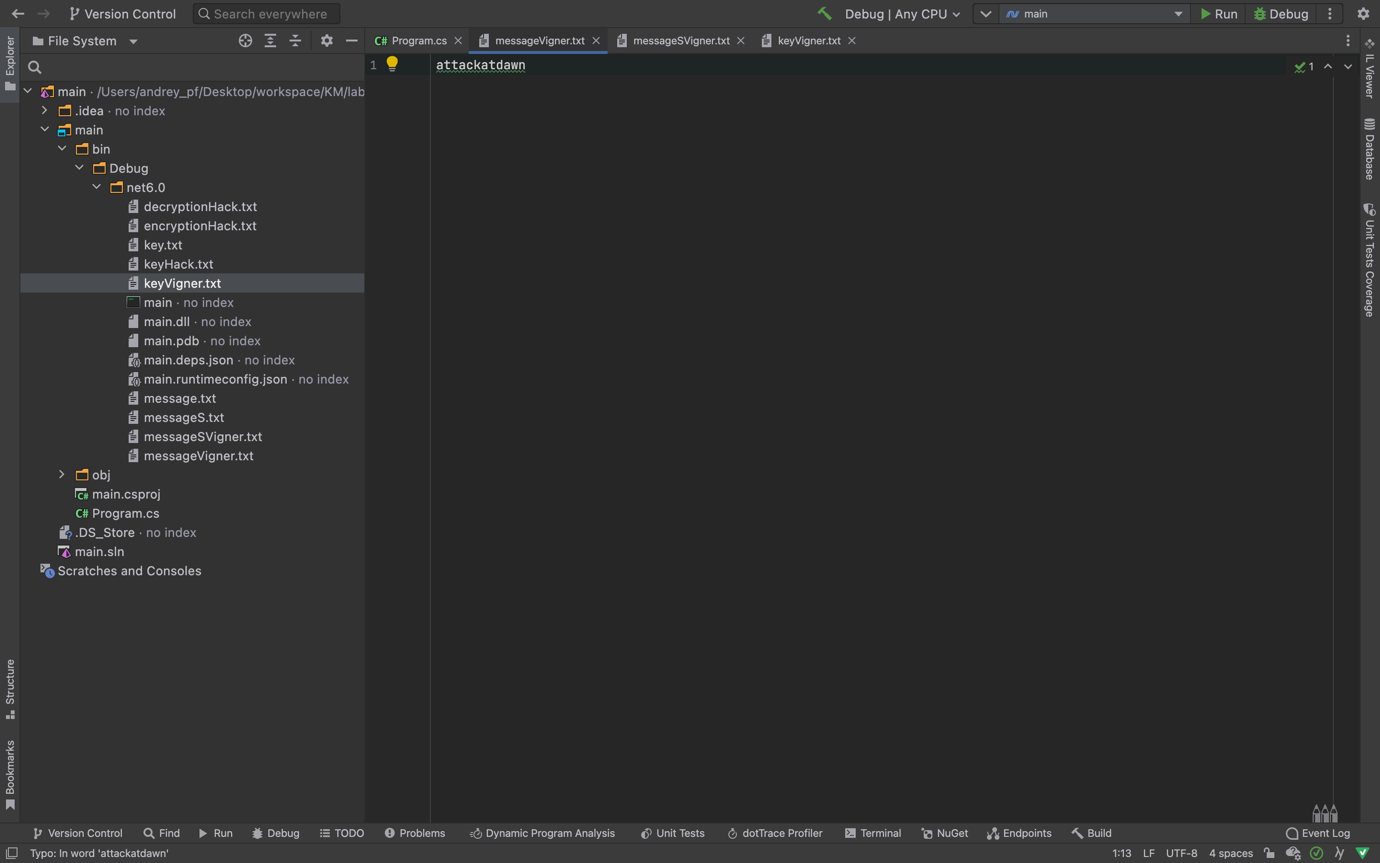
Шифр Виженера состоит из последовательности нескольких шифров Цезаря с различными значениями сдвига. Для зашифровывания может использоваться таблица алфавитов, называемая tabula recta или квадрат (таблица) Виженера. Применительно к латинскому алфавиту таблица Виженера составляется из строк по 26 символов, причём каждая следующая строка сдвигается на несколько позиций. Таким образом, в таблице получается 26 различных шифров Цезаря. На каждом этапе шифрования используются различные алфавиты, выбираемые в зависимости от символа ключевого слова.

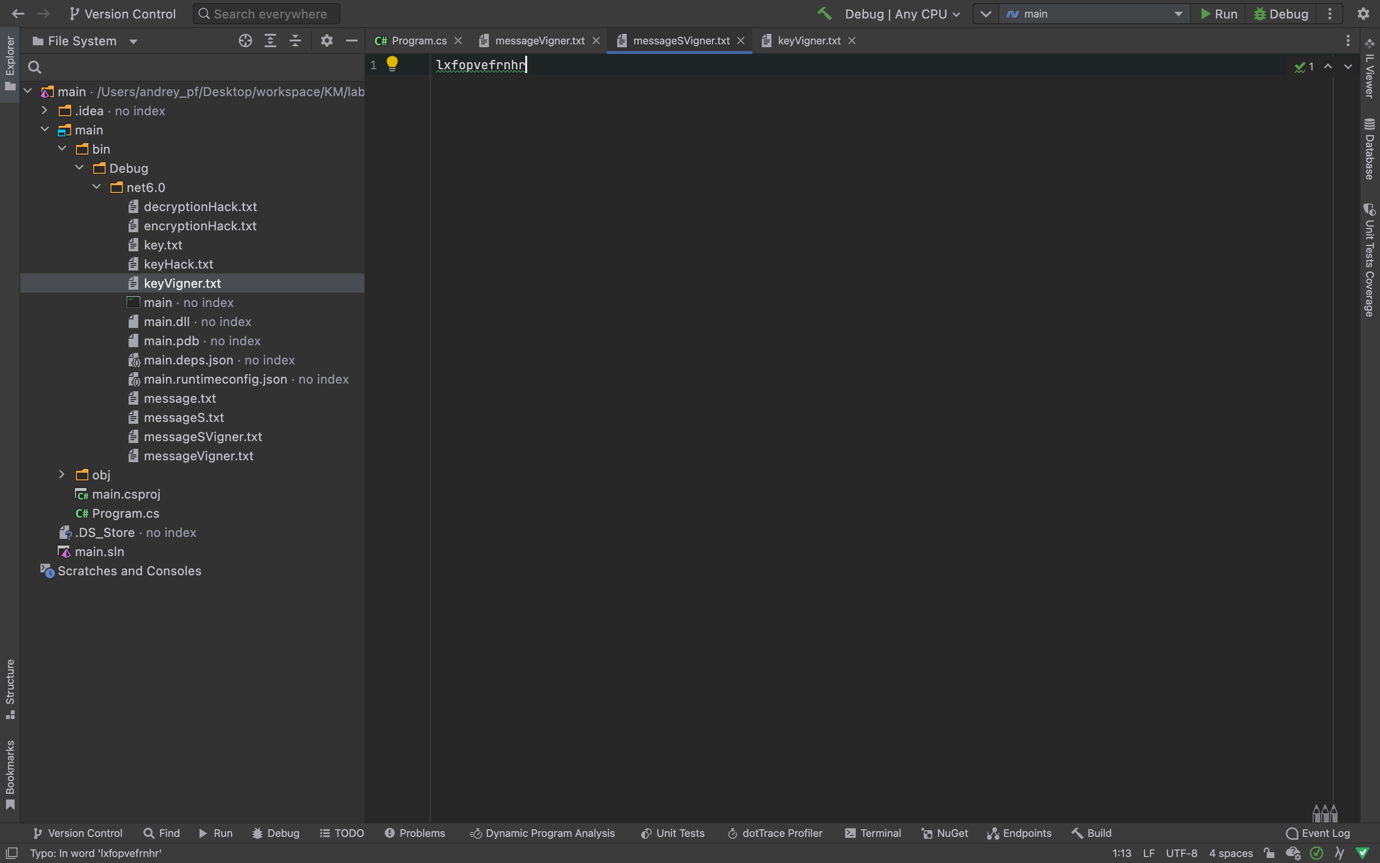
**Математическая модель**

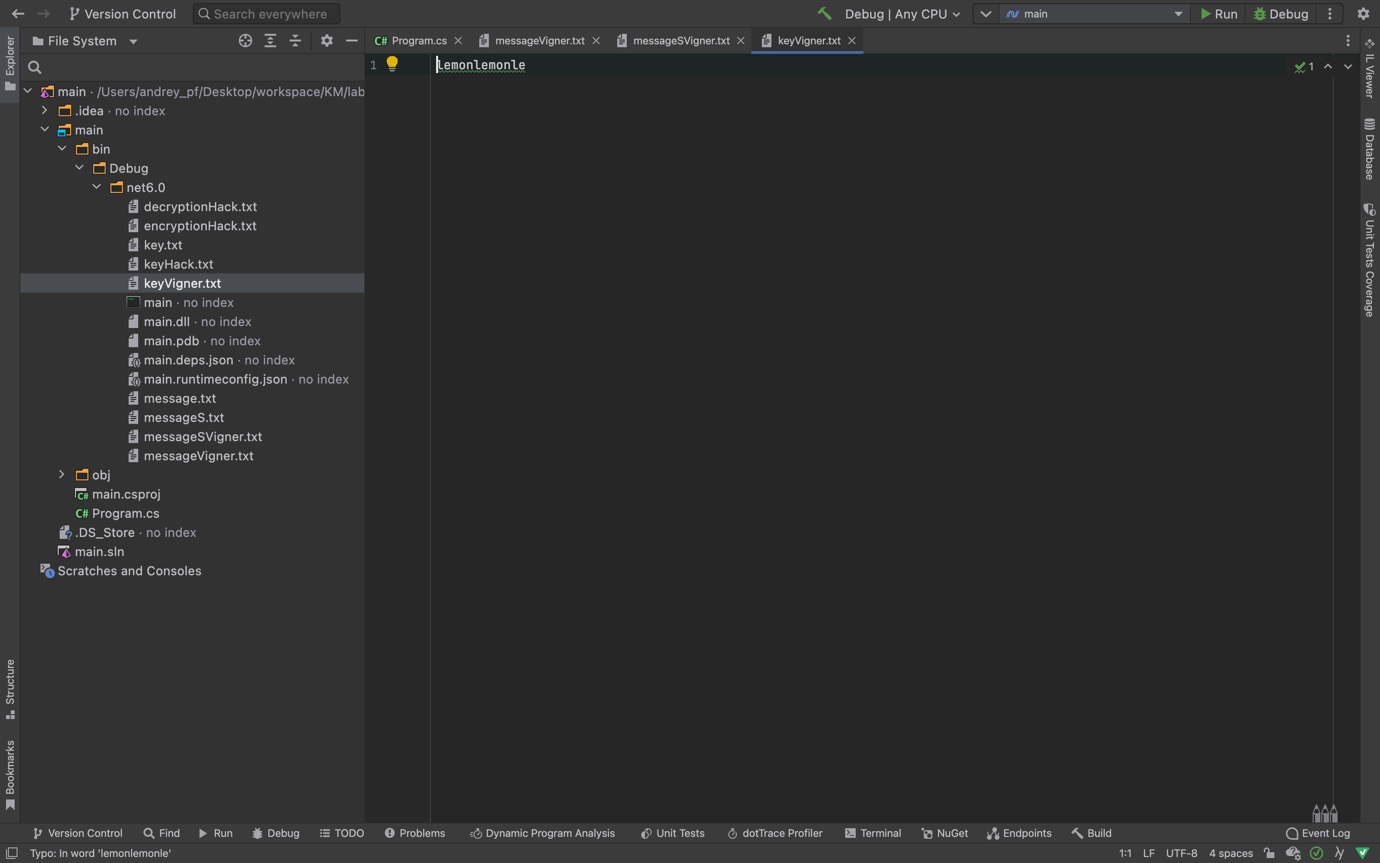
– шифрование;

– расшифровывание,

где - количество букв в алфавите, - номер буквы открытого текста, - номер буквы ключа в алфавите.



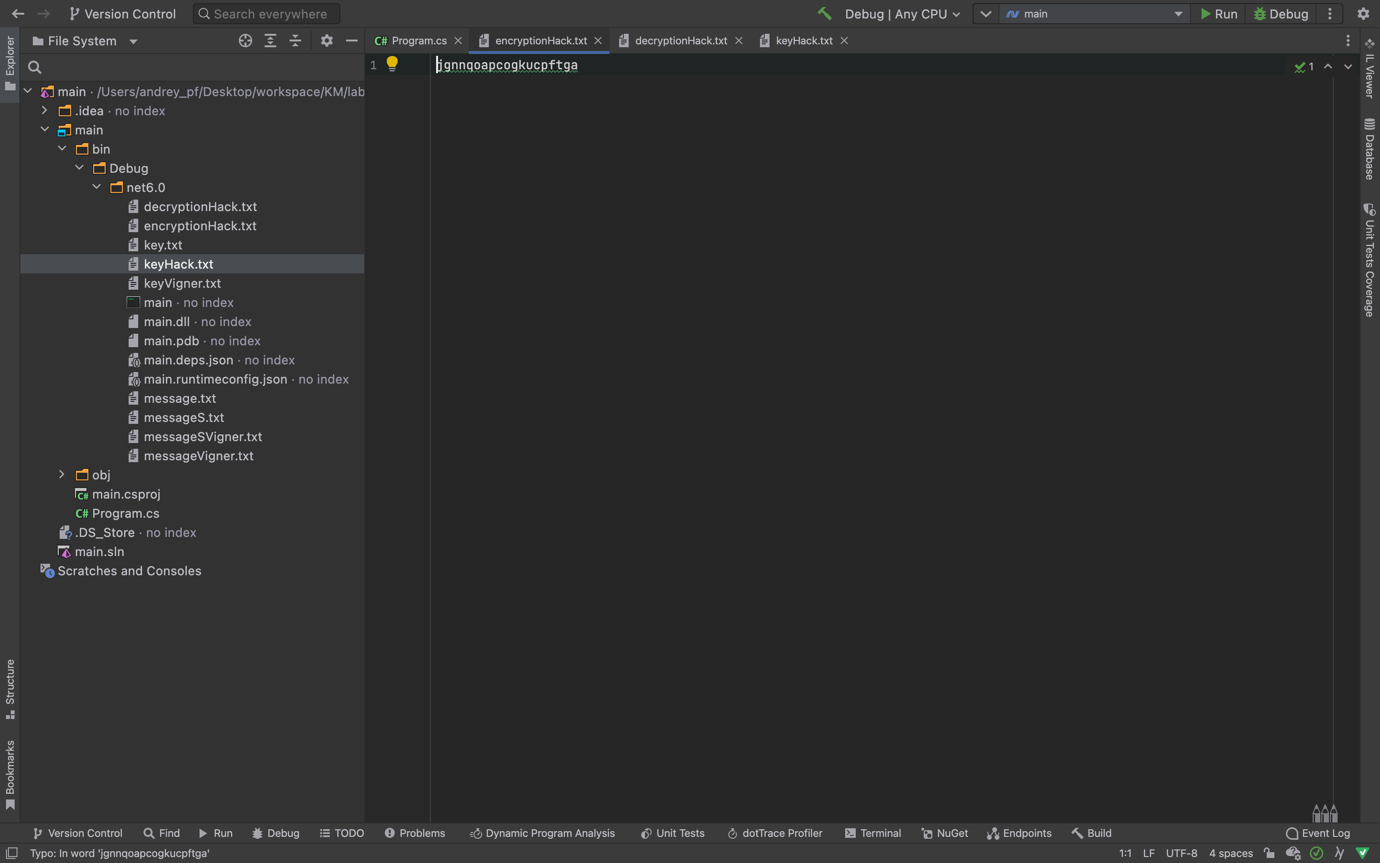


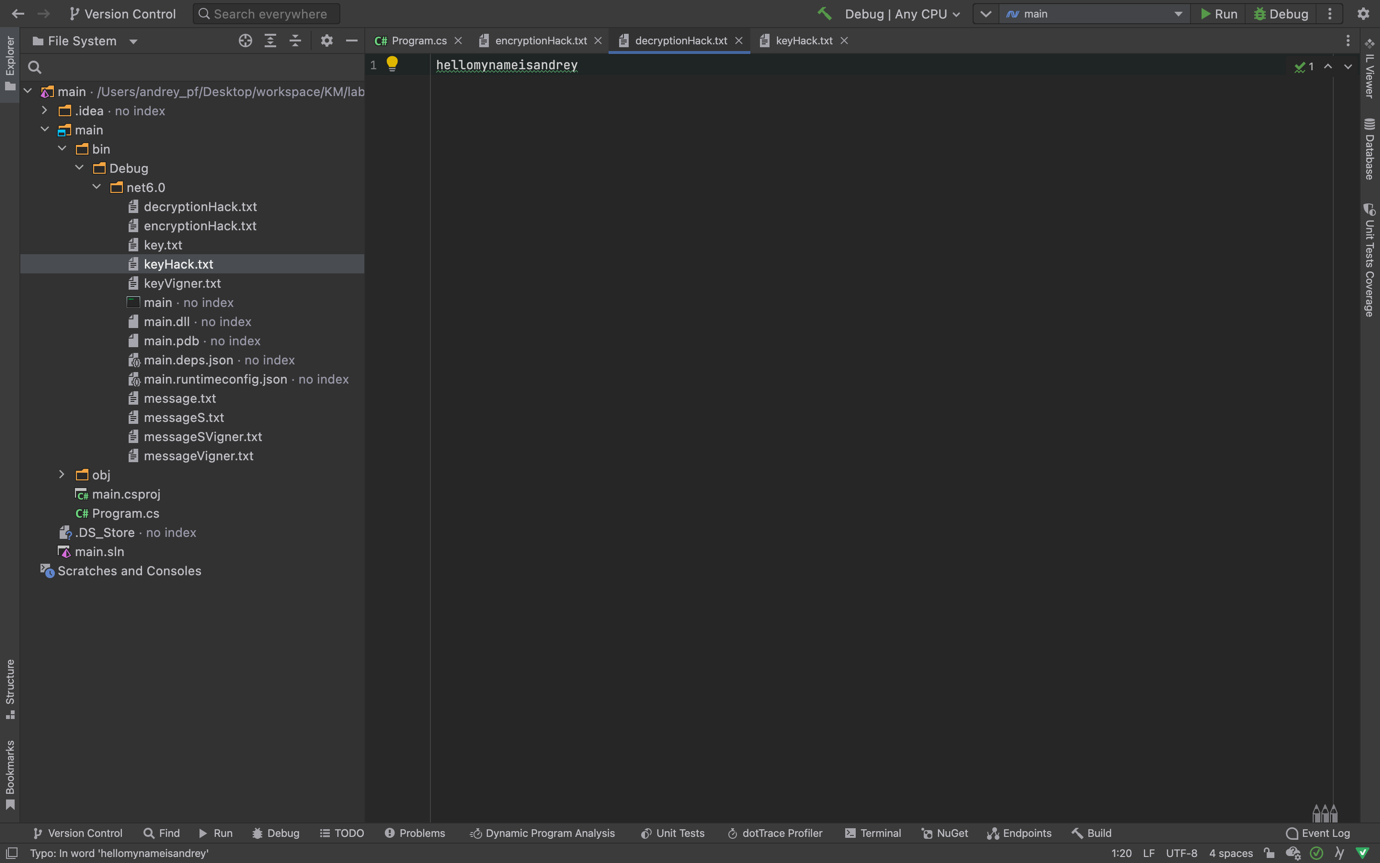


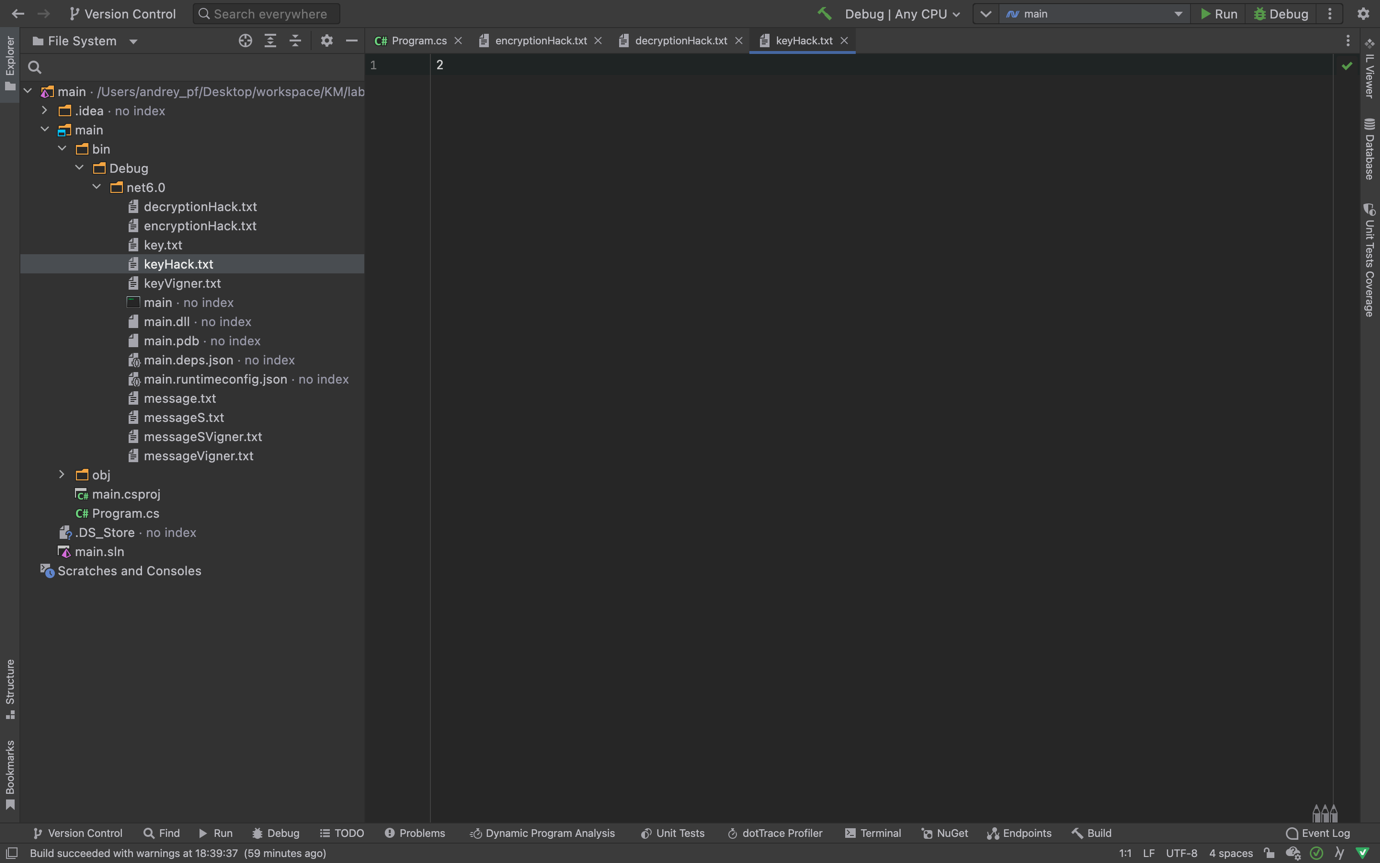
Код в *Приложении 1 и в Goncharenko\_15\_2.cs.*

**Взлом ключа шифра сдвига**

Берем первый элемент из зашифрованного сообщения и исходного текста. Находим их положение в алфавите, далее смотрим их разность по модулю, это и будет ключ, на который происходит сдвиг.







Код в *Приложении 1 и в Goncharenko\_15\_2.cs.*

**Приложение 1.**

using System;  
using System.Collections.Generic;  
using System.Linq;  
using System.Reflection;  
using System.Text;  
using System.Threading.Tasks;  
  
namespace ConsoleApp1  
{  
 class Program  
 {  
 *//шифр простой замены* public static void encryption(int key, List<char> alphabet)  
 {  
 StreamWriter sw = new StreamWriter("messageS.txt");  
 StreamReader sr = new StreamReader("message.txt");  
  
 string message = sr.ReadLine();  
 var arrayList = new List<char>();  
  
 for (int i = 0; i < message.Length; ++i)  
 {  
 if (message[i] != ' ')  
 {  
 int index = 0;  
 for (int j = 0; j < alphabet.Count; ++j)  
 {  
 if (message[i] == alphabet[j]) arrayList.Add(alphabet[(j+key)%26]);  
 }  
 }  
 }  
  
 for (int i = 0; i < arrayList.Count; ++i)  
 {  
 sw.Write(arrayList[i]);  
 }  
   
 sw.Close();  
 sr.Close();  
 }  
  
 public static void decryption(int key, List<char> alphabet)  
 {  
 StreamWriter swd = new StreamWriter("message.txt");  
 StreamReader srd = new StreamReader("messageS.txt");  
   
 string message = srd.ReadLine();  
 var arrayList = new List<char>();  
  
 for (int i = 0; i < message.Length; ++i)  
 {  
 if (message[i] != ' ')  
 {  
 int index = 0;  
 for (int j = 0; j < alphabet.Count; ++j)  
 {  
 if (message[i] == alphabet[j]) arrayList.Add(alphabet[((j-key)+26)%26]);  
 }  
 }  
 }  
  
 for (int i = 0; i < arrayList.Count; ++i)  
 {  
 swd.Write(arrayList[i]);  
 }  
   
 swd.Close();  
 srd.Close();  
 }  
  
 *// Шифр Виженера  
   
 /\*  
 \* Если n — количество букв в алфавите, m\_j — номер буквы открытого текста,  
 \* k\_j — номер буквы ключа в алфавите, то шифрование Виженера можно записать следующим образом:  
 \*  
 \* c\_j=(m\_j+k\_j) mod n  
 \*/* public static void encryptionVigner(string key, List<char> alphabet)  
 {  
 StreamReader srv = new StreamReader("messageVigner.txt");  
 StreamWriter swv = new StreamWriter("messageSVigner.txt");  
  
 var list = new List<char>();  
 string line = srv.ReadLine();  
  
 for (int i = 0; i < line.Length; ++i)  
 {  
 int m = 0, k = 0;  
   
 string a = Convert.ToString(line[i]);  
 string b = Convert.ToString(key[i]);  
  
 for (int j = 0; j < 26; ++j)  
 {  
 if (a == Convert.ToString(alphabet[j])) m = j;  
 if (b == Convert.ToString(alphabet[j])) k = j;  
 }  
   
 list.Add(alphabet[(m+k)%26]);  
 }  
  
 for (int i = 0; i < list.Count; ++i)  
 {  
 swv.Write(list[i]);  
 }  
   
 srv.Close();  
 swv.Close();  
 }  
   
 public static void decryptionVigner(string key, List<char> alphabet)  
 {  
 StreamReader desrv = new StreamReader("messageSVigner.txt");  
 StreamWriter deswv = new StreamWriter("messageVigner.txt");  
  
 var list = new List<char>();  
 string line = desrv.ReadLine();  
  
 for (int i = 0; i < line.Length; ++i)  
 {  
 int c = 0, k = 0;  
   
 string a = Convert.ToString(line[i]);  
 string b = Convert.ToString(key[i]);  
  
 for (int j = 0; j < 26; ++j)  
 {  
 if (a == Convert.ToString(alphabet[j])) c = j;  
 if (b == Convert.ToString(alphabet[j])) k = j;  
 }  
  
 int ind = (c - k) % 26;  
 if (c - k < 0) ind = 26 + (c - k);  
 list.Add(alphabet[ind]);  
 }  
  
 for (int i = 0; i < list.Count; ++i)  
 {  
 deswv.Write(list[i]);  
 }  
   
 desrv.Close();  
 deswv.Close();  
 }  
   
 *//hack key* public static void hack(List<char> alp)  
 {  
 StreamReader srh = new StreamReader("encryptionHack.txt");  
 StreamReader srdh = new StreamReader("decryptionHack.txt");  
 StreamWriter swh = new StreamWriter("keyHack.txt");  
  
 string line1 = srh.ReadLine();  
 string line2 = srdh.ReadLine();  
  
 char a = Convert.ToChar(line1[0]);  
 char b = Convert.ToChar(line2[0]);  
  
 int n = 0, m = 0;  
  
 for (int i = 0; i < alp.Count; ++i)  
 {  
 if (a == alp[i]) n = i;  
 if (b == alp[i]) m = i;  
 }  
  
 swh.Write(Math.Abs(n - m));  
   
 srh.Close();  
 srdh.Close();  
 swh.Close();  
 }  
  
 static void Main(string[] args)  
 {  
 StreamReader streamReader = new StreamReader("key.txt");  
 int key = Convert.ToInt32(streamReader.ReadLine());  
 var alphabet = new List<char>();  
 string alp = "abcdefghijklmnopqrstuvwxyz";  
  
 for (int i = 0; i < 26; ++i)  
 {  
 alphabet.Add(alp[i]);  
 }  
   
 Console.WriteLine("encryption or decryption?");  
 string answer = Console.ReadLine();  
 if (answer == "encryption")  
 {  
 encryption(key, alphabet);  
 }  
  
 if (answer == "decryption")  
 {  
 decryption(key, alphabet);  
 }  
 streamReader.Close();  
   
 *//-----------------------------* StreamReader srv = new StreamReader("keyVigner.txt");  
 string keyV = srv.ReadLine();  
   
 Console.WriteLine("encryption or decryption?");  
 string answerV = Console.ReadLine();  
 if (answerV == "encryption")  
 {  
 encryptionVigner(keyV, alphabet);  
 }  
  
 if (answerV == "decryption")  
 {  
 decryptionVigner(keyV, alphabet);  
 }  
 srv.Close();  
   
 *//-----------------------------* hack(alphabet);}  
 }  
}