**МИНИСТЕРСТВО ПО РАЗВИТИЮ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И КОММУНИКАЦИЙ РЕСПУБЛИКИ УЗБЕКИСТАНА**

ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

***Практическая работа 6***

*по предмету* ***«Криптография»***

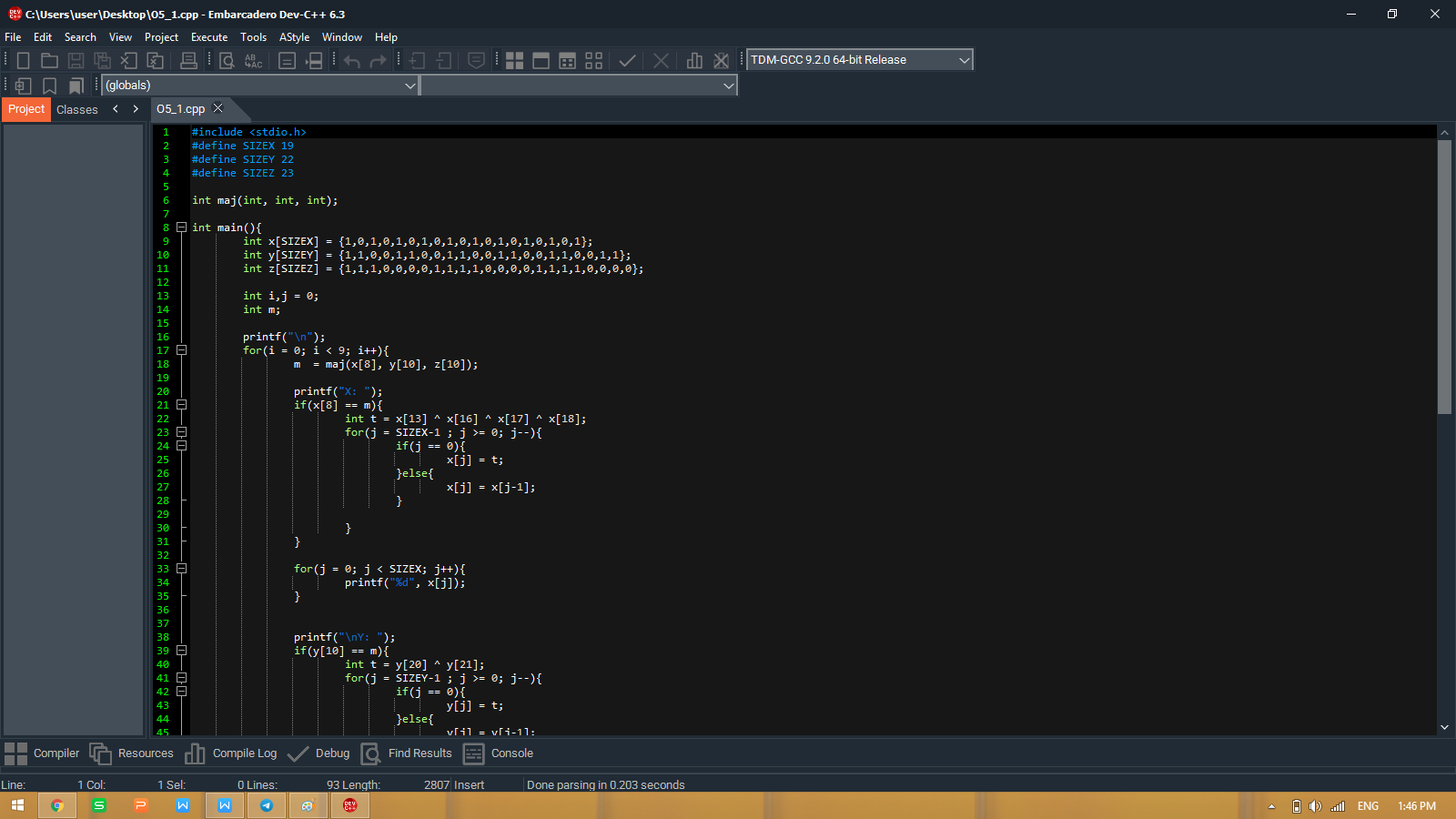
#### На тему: **«Разработка программу шифрования и дешифрования данных на основе алгоритма шифрования RC4»**

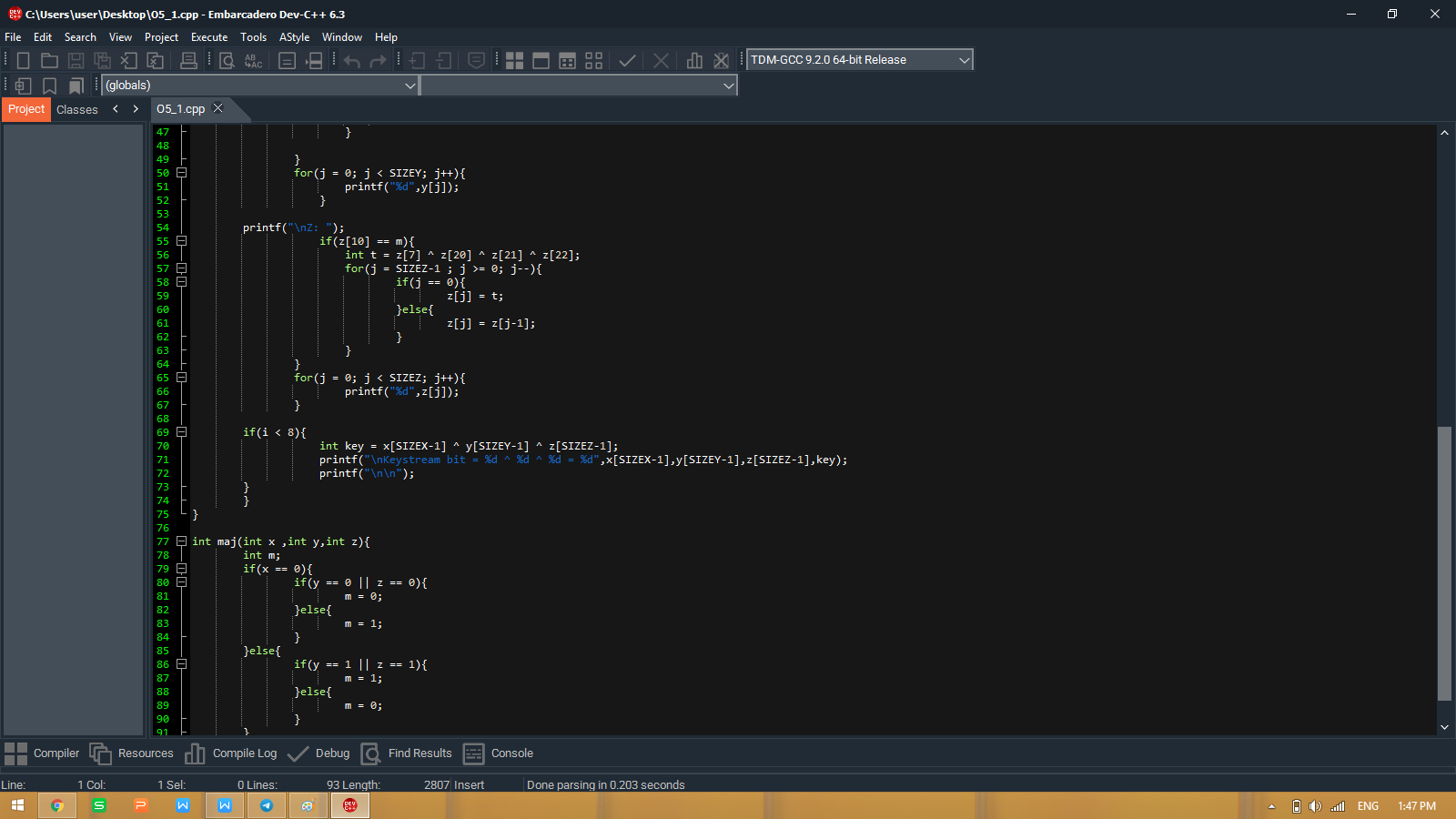
Группа: 721-19

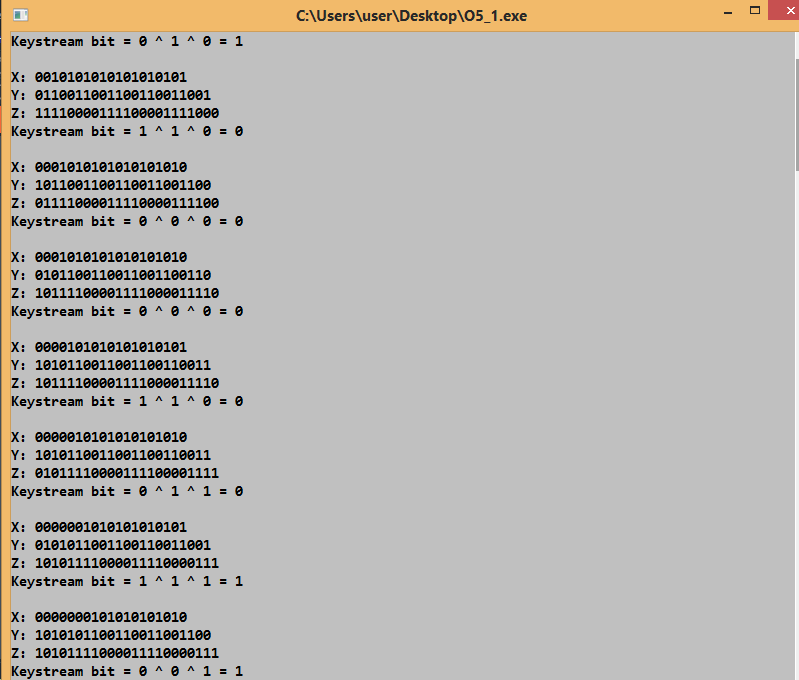
Выполнил: Хакимбеков Дониёрбек

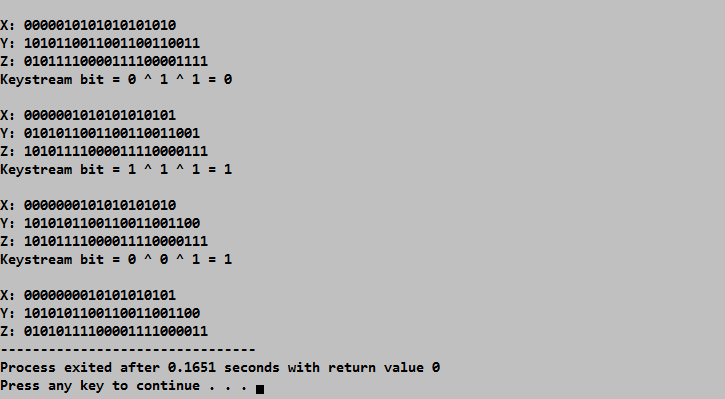
Принял: Хамидов Шерзод

***Ташкент 2021***









**#include <stdio.h>**

**#define SIZEX 19**

**#define SIZEY 22**

**#define SIZEZ 23**

**int maj(int, int, int);**

**int main(){**

**int x[SIZEX] = {1,0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1};**

**int y[SIZEY] = {1,1,0,0,1,1,0,0,1,1,0,0,1,1,0,0,1,1,0,0,1,1};**

**int z[SIZEZ] = {1,1,1,0,0,0,0,1,1,1,1,0,0,0,0,1,1,1,1,0,0,0,0};**

**int i,j = 0;**

**int m;**

**printf("\n");**

**for(i = 0; i < 9; i++){**

**m = maj(x[8], y[10], z[10]);**

**printf("X: ");**

**if(x[8] == m){**

**int t = x[13] ^ x[16] ^ x[17] ^ x[18];**

**for(j = SIZEX-1 ; j >= 0; j--){**

**if(j == 0){**

**x[j] = t;**

**}else{**

**x[j] = x[j-1];**

**}**

**}**

**}**

**for(j = 0; j < SIZEX; j++){**

**printf("%d", x[j]);**

**}**

**printf("\nY: ");**

**if(y[10] == m){**

**int t = y[20] ^ y[21];**

**for(j = SIZEY-1 ; j >= 0; j--){**

**if(j == 0){**

**y[j] = t;**

**}else{**

**y[j] = y[j-1];**

**}**

**}**

**}**

**for(j = 0; j < SIZEY; j++){**

**printf("%d",y[j]);**

**}**

**printf("\nZ: ");**

**if(z[10] == m){**

**int t = z[7] ^ z[20] ^ z[21] ^ z[22];**

**for(j = SIZEZ-1 ; j >= 0; j--){**

**if(j == 0){**

**z[j] = t;**

**}else{**

**z[j] = z[j-1];**

**}**

**}**

**}**

**for(j = 0; j < SIZEZ; j++){**

**printf("%d",z[j]);**

**}**

**if(i < 8){**

**int key = x[SIZEX-1] ^ y[SIZEY-1] ^ z[SIZEZ-1];**

**printf("\nKeystream bit = %d ^ %d ^ %d = %d",x[SIZEX-1],y[SIZEY-1],z[SIZEZ-1],key);**

**printf("\n\n");**

**}**

**}**

**}**

**int maj(int x ,int y,int z){**

**int m;**

**if(x == 0){**

**if(y == 0 || z == 0){**

**m = 0;**

**}else{**

**m = 1;**

**}**

**}else{**

**if(y == 1 || z == 1){**

**m = 1;**

**}else{**

**m = 0;**

**}**

**}**

**return m;**