Лабораторная работа №7.

Элементы криптографии. Однократное гаммирование

Стариков Данила Андреевич

Содержание

# 1 Цель работы

Освоить на практике применение режима однократного гаммирования.

# 2 Выполнение лабораторной работы

Для выполнения задания был выбран язык Си. Текст программы можно посмореть на Листинге 1.

Листинг 1: Программа cypher.c

void initKey(char key[], int size) {  
 for(int i=0; i<size; i++)  
 key[i] = 0x00;  
 key[size-1] = '\0';  
}  
void printKey(char key[], int size) {  
 for(int i=0; i<size; i++)  
 printf("0x%X ", key[i]);  
 printf("\n");  
}  
void xor(char out[], char str1[], char str2[], int size) {  
 for(int i=0; i<size; i++)  
 out[i] = str1[i] ^ str2[i];  
 out[size-1] = '\0';  
}  
int main() {  
 char open[] = "С новым годом, друзья!";  
 int size = sizeof(open)/sizeof(open[0]);  
 char key[size];  
 char test[size];  
 char cyphered[] = "Привет, мир! Как дела?";  
 printf("%s\n", open);  
   
 initkey(key, size);  
 xor(test, open, key, size);  
 printf("%s\n", test);  
   
 char key2[size];  
 xor(key2, open, cyphered, size);  
 printKey(key2, size);  
 xor(test, cyphered, key2, size);  
 printf("%s\n", test);  
 return 0;  
}

При выполнении получаем соответвующий вывод (рис. 1):

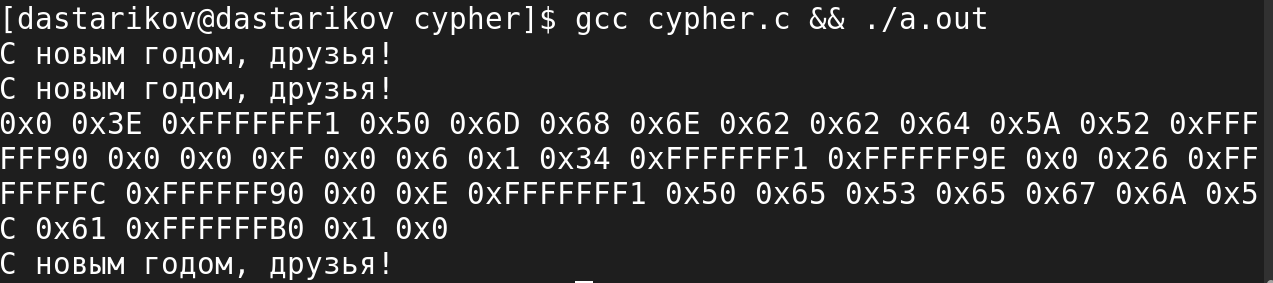


Рис. 1: Результат выполнения программы.

# 3 Выводы

В результате лабораторной работы реализовали на языке Си программу, использующую однократное гаммирование для шифрования сообщения [**shannon?**].

# Список литературы