Лабораторная работа №8.

Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом

Стариков Данила Андреевич

Содержание

# 1 Цель работы

Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом

# 2 Выполнение лабораторной работы

Для выполнения задания был выбран язык Си.. Функции xor и printKey взяты из лабораторной работы №7, отдельно была написана функция setKey, которая генерирует случайный ключ заданного размера (Листинг 1). Текст программы можно посмотреть на Листинге 2.

Листинг 1: Функция setKey

void setKey(char key[], int size) {  
 const char charset[] = "abcdefghijklmnopqrstuvwxyz \  
 ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789";  
 size\_t charset\_size = sizeof(charset) - 1;  
  
 srand(time(NULL));  
  
 for (int i = 0; i < size; ++i) {  
 int index = rand() % charset\_size;  
 key[i] = charset[index];  
 }  
 key[size-1] = '\0'; // Null-terminate the string  
}

Листинг 2: Программа cypher1.c

#include<stdio.h>  
#include<time.h>  
#include<stdlib.h>  
  
int main() {  
 char P1[] = "МесяцАпрельДень25";  
 char P2[] = "Оплата1000СрокДень";  
 int msgSize = sizeof(P1)/sizeof(P1[0]);  
 char testKey[msgSize];  
 setKey(testKey, msgSize);  
 char C1[msgSize];  
 char C2[msgSize];  
 xor(C1, P1, testKey, msgSize);  
 xor(C2, P2, testKey, msgSize);  
 printf("Изначальное сообщение: \n");  
 printf("%s\n", P1);  
 printf("%s\n", P2);  
  
 printf("Шифротексты: \n");  
 printKey(C1, msgSize);  
 printKey(C2, msgSize);  
  
 printf("Сравнение C1+C2 и P1+P2: \n");  
 char C12[msgSize];  
 char P12[msgSize];  
 xor(C12, C1, C2, msgSize);  
 xor(P12, P1, P2, msgSize);  
 printKey(C12, msgSize);  
 printKey(P12, msgSize);  
 char input[msgSize];  
 char output[msgSize];  
 while (1) {  
 printf(">");  
 scanf("%s", &input);  
 xor(output, input, C12, msgSize);  
 printf("%s\n", output);  
 }  
 return 0;  
  
}

При выполнении получаем соответвующий вывод (рис. 1):

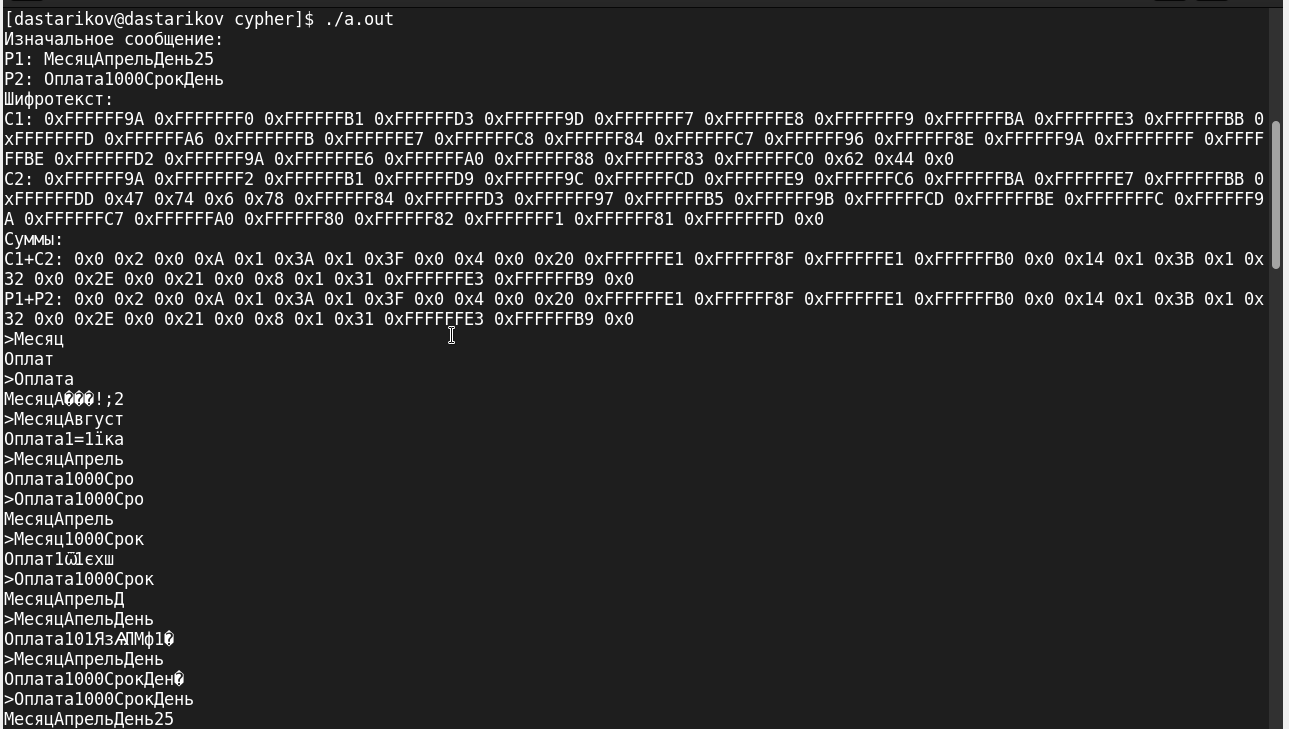


Рис. 1: Результат выполнения программы.

# 3 Выводы

В результате лабораторной работы реализовали на языке Си программу, использующую однократное гаммирование для шифрования сообщения, проверили на практике систему кодирования двух сообщений одним ключом [1].

# Список литературы

1. Shannon C.E. [Communication theory of secrecy systems](https://doi.org/10.1002/j.1538-7305.1949.tb00928.x) // The Bell System Technical Journal. 1949. Т. 28, № 4. С. 656–715.