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 2.1.

При выполнении получаем соответвующий вывод (рис. 2.1):

```
[dastarikov@dastarikov cypher]$ gcc cypher.c && ./a.out
С новым годом, друзья!
С новым годом, друзья!
0x0 0x3E 0xFFFFFFF1 0x50 0x6D 0x68 0x6E 0x62 0x62 0x64 0x5A 0x52 0xFFF
FFF90 0x0 0x0 0xF 0x0 0x6 0x1 0x34 0xFFFFFFF1 0xFFFFFF9E 0x0 0x26 0xFF
FFFFFC 0xFFFFFF90 0x0 0xE 0xFFFFFFF1 0x50 0x65 0x53 0x65 0x67 0x6A 0x5
C 0x61 0xFFFFFFB0 0x1 0x0
С новым годом, друзья!
```

Рис. 2.1: Результат выполнения программы.

Листинг 2.1 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;
}
```

3 Выводы

В результате лабораторной работы реализовали на языке Си программу, использующую однократное гаммирование для шифрования сообщения [1].

Список литературы

1. Shannon C.E. Communication theory of secrecy systems // The Bell System Technical Journal. 1949. Т. 28, № 4. С. 656–715.