

## Лабораторная работа №8.

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

---

Стариков Данила Андреевич

25 мая 2024

## Цели и задачи

---

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

## Выполнение

---

```
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  
}
```

```
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;
}
```



```
[dastarikov@dastarikov cypher]$ ./a.out
Изначальное сообщение:
P1: МесяцАпрельДень25
P2: Оплата1000СрокДень
Шифротекст:
C1: 0xFFFFFFFF9A 0xFFFFFFFFF0 0xFFFFFFFFB1 0xFFFFFFFFD3 0xFFFFFFFF9D 0xFFFFFFFFF7 0xFFFFFFFFE8 0xFFFFFFFFF9 0xFFFFFFFFBA 0xFFFFFFFFE3 0xFFFFFFFFB8 0
xFFFFFFFFD 0xFFFFFFFFA6 0xFFFFFFFFFB 0xFFFFFFFFE7 0xFFFFFFFFC8 0xFFFFFFFF84 0xFFFFFFFFC7 0xFFFFFFFF96 0xFFFFFFFF8E 0xFFFFFFFF9A 0xFFFFFFFFF 0xFFFF
FFBE 0xFFFFFFFFD2 0xFFFFFFFF9A 0xFFFFFFFFE6 0xFFFFFFFFF0 0xFFFFFFFF88 0xFFFFFFFF83 0xFFFFFFFFC0 0x62 0x44 0x0
C2: 0xFFFFFFFF9A 0xFFFFFFFFF2 0xFFFFFFFFB1 0xFFFFFFFFD9 0xFFFFFFFF9C 0xFFFFFFFFCD 0xFFFFFFFFE9 0xFFFFFFFFC6 0xFFFFFFFFBA 0xFFFFFFFFE7 0xFFFFFFFFB8 0
xFFFFFFFFD 0x47 0x74 0x6 0x78 0xFFFFFFFF84 0xFFFFFFFFD3 0xFFFFFFFF97 0xFFFFFFFFB5 0xFFFFFFFF9B 0xFFFFFFFFCD 0xFFFFFFFFBE 0xFFFFFFFFC 0xFFFFFFFF9
A 0xFFFFFFFFC7 0xFFFFFFFFF0 0xFFFFFFFF80 0xFFFFFFFF82 0xFFFFFFFFF1 0xFFFFFFFF81 0xFFFFFFFFD 0x0
Суммы:
C1+C2: 0x0 0x2 0x0 0xA 0x1 0x3A 0x1 0x3F 0x0 0x4 0x0 0x20 0xFFFFFFFFE1 0xFFFFFFFF8F 0xFFFFFFFFE1 0xFFFFFFFFB0 0x0 0x14 0x1 0x3B 0x1 0x
32 0x0 0x2E 0x0 0x21 0x0 0x8 0x1 0x31 0xFFFFFFFFE3 0xFFFFFFFFB9 0x0
P1+P2: 0x0 0x2 0x0 0xA 0x1 0x3A 0x1 0x3F 0x0 0x4 0x0 0x20 0xFFFFFFFFE1 0xFFFFFFFF8F 0xFFFFFFFFE1 0xFFFFFFFFB0 0x0 0x14 0x1 0x3B 0x1 0x
32 0x0 0x2E 0x0 0x21 0x0 0x8 0x1 0x31 0xFFFFFFFFE3 0xFFFFFFFFB9 0x0
>Месяц
>Оплата
>Оплата
МесяцА000!;2
>МесяцАвгуст
Оплата1=1ika
>МесяцАпрель
Оплата1000Сро
>Оплата1000Сро
МесяцАпрель
>Месяц1000Срок
Оплата1000Сро
>Оплата1000Срок
МесяцАпрельД
>МесяцАпельДень
Оплата101ЯзАМФ10
>МесяцАпрельДень
Оплата1000СрокДень0
>Оплата1000СрокДень
МесяцАпрельДень25
```

Рис. 1: Результат работы программы.

## Итоги

---

- Реализовали на языке Си программу, использующую однократное гаммирование для шифрования сообщения, проверили на практике систему кодирования двух сообщений одним ключом.