Обязательное задание к практической работе №2
"Блочное шифрование, основанное на конструкции (сети) Фейстеля"
группа 14-502

Исходные данные:
Заданная в работе №1 последовательность десятичных чисел, представляющих номера уровней квантования (L=0÷15) выборок, полученная в результате аналого-цифрового преобразования некоторого информационного сигнала

Для выполнения задания необходимо:
I. Предварительный этап.
1. Разбить открытый текст на блоки с четным количеством символов (рекомендуемые длины блока – шесть, восемь или десять символов). В случае, если количество символов открытого текста не кратно длине блок, необходимо дополнить его любыми однотипными символами.
2. Выбрать секретный ключ (последовательность десятичных чисел), равный по количеству символов половине длины блока открытого текста который будет использоваться при вычислении функции шифрования.
II. Шифрование.
1. Первый блок открытого текста разбить на два равных блока L_0 и R_0.
2. Выполнить первый раунд шифрования:
- вычислить значение функции шифрования $f(R_0,k_1)$ путем сложения блока R_0 с выбранным ключом по mod16;
- получить блок R_1 путем сложения значения функции шифрования $f(R_0,k_1)$ с блоком L_0 по mod16;
- скопировать содержимое блока R_0 в L_1.
2. Выполнить второй раунд шифрования:
- осуществить циклический сдвиг ключа на одну позицию влево;
- вычислить значение функции шифрования $f(R_1,k_2)$ путем сложения блока R_1 с текущим ключом по mod16;
- получить блок R_2 путем сложения значения функции шифрования $f(R_1,k_2)$ с блоком L_1 по mod16;
- скопировать содержимое блока R_1 в L_2.
3. Объединить блоки L_2 и R_2 в один блок шифртекста.
III. Дешифрование.
1. Полученный блок шифртекста разбить на два равных блока L_2 и R_2.
2. Выполнить первый раунд дешифрования:
- вычислить значение функции дешифрования $f(L_2,k_2)$ путем сложения блока L_2 с соответствующим ключом по mod16;
- получить блок L_1 путем вычитания значения функции шифрования $f(L_2,k_2)$ из блока R_2 по mod16;
- скопировать содержимое блока L_2 в R_1.
2. Выполнить второй раунд шифрования:
- осуществить циклический сдвиг ключа на одну позицию вправо;
- вычислить значение функции шифрования $f(L_1,k_1)$ путем сложения блока L_1 с текущим ключом по mod16;
- получить блок L_0 путем вычитания значения функции шифрования $f(L_1,k_1)$ из блока R_1 по mod16;
- скопировать содержимое блока L_1 в R_0.
3. Объединить блоки L_0 и R_0 в один блок открытого текста.

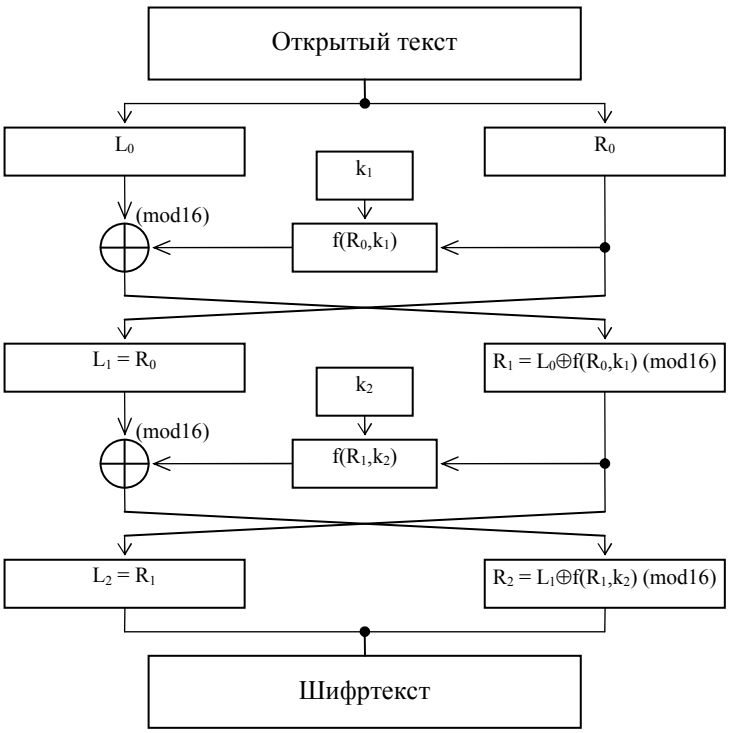
Повторить процедуры шифрования и дешифрования для остальных блоков открытого текста.

Открытый текст, разбитый на блоки

Начальный пользовательский ключ шифрования:

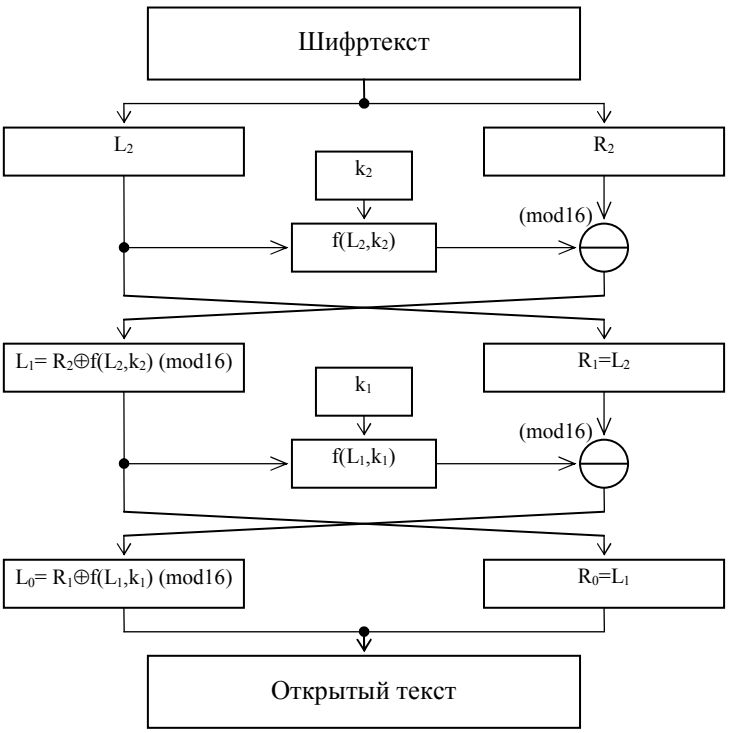
Схемы шифрования и дешифрования

шифрование



Функция шифрования $f = R_{i-1} + k_i \pmod{16}$

дешифрование



Функция дешифрования $f = L_i + k_i \pmod{16}$

Нижеследующую страницу скопировать нужное количество раз по числу блоков открытого текста

Блок открытого текста:

Шифрование

1 раунд.

$L_0 =$ $R_0 =$

$k_1 =$

$f(R_0,k_1) = R_0 + k_1 \pmod{16}$

R_0					
k_1					
$f(R_0,k_1)$					

$L_1 =$ $R_0 =$

$R_1 = L_0 + f(R_0,k_1) \pmod{16}$

L_0					
$f(R_0,k_1)$					
R_1					

$R_1 =$

2 раунд.

$k_2 =$

$f(R_1,k_2) = R_1 + k_2 \pmod{16}$

R_1					
k_2					
$f(R_1,k_2)$					

$L_2 =$ $R_1 =$

$R_2 = L_1 + f(R_1,k_2) \pmod{16}$

L_1					
$f(R_1,k_2)$					
R_2					

$R_2 =$

Блок шифртекста:

Дешифрование

1 раунд.

$f(L_2,k_2) = L_2 + k_2 \pmod{16}$

L_2					
k_2					
$f(L_2,k_2)$					

$L_1 =$

$L_1 = R_2 - f(L_2,k_2) \pmod{16}$

R_2					
$f(L_2,k_2)$					
L_1					

$R_1 = L_2 =$

2 раунд.

$f(L_1,k_1) = L_1 + k_1 \pmod{16}$

L_1					
k_1					
$f(L_1,k_1)$					

$L_0 =$

$L_0 = R_1 - f(L_1,k_1) \pmod{16}$

R_1					
$f(L_1,k_1)$					
L_0					

$R_0 = L_1 =$

Блок восстановленного открытого текста: