Дополнительное задание к практической работе №2
"Алгоритм блочного шифрования DES"
группа 14-502

Исходные данные:
64-битный блок открытого текста, 56-битный пользовательский ключ; прилагающийся раздаточный материал.

Необходимо:
I. Осуществить генерацию раундовых ключей k_1 и k_{16}:
I.1. Выполнить необходимое число правых циклических сдвигов столбцов универсального ключа, определяемое вариантом задания для получения пользовательского 56-битного ключа.
I.2. Дополнить каждый из восьми 7-битных блоков полученного после п.I.1 пользовательского ключа одним битом таким образом, чтобы каждый из результирующих 8-битных блоков содержал бы нечетное количество единиц.
I.3. Выполнить начальную перестановку полученного после п.I.2 64-битного пользовательского ключа в соответствии с табл.2.2 раздаточного материала, получить в результате начальные сеансовые ключи C_0 и D_0.
I.4. В соответствии с табл.2.5 осуществить циклический сдвиг вектора C_0D_0 для получения ключей C_1D_1.
I.5. Получить раундовый ключ k_1 путем выбора битов из вектора C_1D_1 согласно табл.2.7.
I.6. Выполнить действия, аналогичные п.I.4 и I.5 для получения раундового ключа k_{16}.

II. Выполнить 2 раунда шифрования: первый и последний для получения шифртекста:
II.1. Выполнить необходимое число левых циклических сдвигов столбцов универсального блока открытого текста, определяемое вариантом задания для получения открытого текста пользователя.
II.2. Произвести начальную перестановку IP открытого текста, полученного в п.II.1 в соответствии с табл.1.2 раздаточного материала, результат перестановки разбить на два 32-битных блока L_0 и R_0.
II.3. Выполнить над блоком R_0 операцию расширения E согласно табл.1.4, осуществить сложение по модулю два расширенного подблока R_0 с раундовым ключом k_1, полученным ранее в пункте I.5.
II.4. Для каждого из полученных 8-битных блоков B_i найти двоичные комбинации, соответствующие числам a_2 и b_2, свести их в таблицу и определить их десятичные представления a_{10} и b_{10}.
II.5. На основании найденных чисел a_{10} и b_{10} для каждого из блоков B_i при помощи табл.1.9 выполнить S-преобразование и найти числа c_{10}, двоичное представление которых c_2 даст блоки B'_i. Полученный в результате S-преобразования 32-битный блок $B'_1 \div B'_8$ свести в таблицу.
II.6. Получить окончательное значение функции шифрования $f(R_0, k_1)$ перестановкой P, определяемой таблицей 1.12
II.7. Полученное в предыдущем пункте значение функции f (32 бита) сложить по модулю два с подблоком L_0, свести результат сложения в таблицу.
II.8. Показать полученные в результате первого раунда шифрования блоки L_1 и R_1.
II.9. Выполнить последний, 16-й раунд шифрования. В качестве блоков L_{15} и R_{15} можно использовать либо блоки L_1 и R_1, либо самостоятельно сформировать два произвольных 32-битных блока. Шифрование выполнять аналогично п.II.3-II.8.
II.10. Полученные в результате 16-го раунда шифрования блоки L_{16} и R_{16} объединить в 64-битный блок и подвергнуть его конечной перестановке IP^{-1} согласно таблице 1.23, привести полученный 64-битный блок шифртекста.

III. Выполнить 2 раунда дешифрования: первый и последний для получения исходного открытого текста:
III.1. Выполнить начальную перестановку IP шифртекста в соответствии с табл.1.2 раздаточного материала, результат перестановки разбить на два 32-битных блока L_{16} и R_{16}.
III.2. Выполнить над блоком L_{16} операцию расширения E согласно табл.1.4, осуществить сложение по модулю два расширенного подблока L_{16} с раундовым ключом k_{16}, полученным ранее в пункте I.6.
III.3. Для каждого из полученных 8-битных блоков B_i найти двоичные комбинации, соответствующие числам a_2 и b_2, свести их в таблицу и определить их десятичные представления a_{10} и b_{10}.

III.4. На основании найденных чисел a_{10} и b_{10} для каждого из блоков B_i при помощи табл.1.9 выполнить S-преобразование и найти числа c_{10}, двоичное представление которых c_2 даст блоки B'_i. Полученный в результате S-преобразования 32-битный блок $B'_1 \div B'_8$ свести в таблицу.
III.5. Получить окончательное значение функции шифрования $f(L_{16}, k_{16})$ перестановкой P, определяемой таблицей 1.12
III.6. Полученное в предыдущем пункте значение функции f (32 бита) сложить по модулю два с подблоком R_{16}, свести результат сложения в таблицу.
III.7. Показать полученные в результате первого раунда дешифрования блоки L_{15} и R_{15}.
III.8. Выполнить последний, 16-й раунд дешифрования над блоками L_1 и R_1. Дешифрование выполнять аналогично п.III.2-III.7.
III.9. Полученные в результате 16-го раунда дешифрования блоки L_0 и R_0 объединить в 64-битный блок и подвергнуть его конечной перестановке IP^{-1} согласно таблице 1.23, привести полученный 64-битный блок открытого текста, сравнить его с исходным открытым текстом.

Варианты задания:

Универсальный 64-битный блок открытого текста

0	0	0	1	1	1	1	0	0	0	0	0	1	1	1	1
0	1	1	0	0	1	1	0	0	0	1	1	0	0	1	1
1	0	1	0	1	0	1	0	0	1	0	1	0	1	0	1
0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1

Значение открытого текста для конкретного варианта находится путем выполнения некоторого количества левых циклических сдвигов столбцов универсального блока открытого текста, которое определяется нижеследующей таблицей

Номер варианта	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Величина сдвига	1	2	3	5	7	9	11	13	4	6	8	10	12	14	3	7	9	11	13	15

Универсальный 56-битный пользовательский ключ

1	1	1	0	0	0	0	1	1	1	1	0	0	0
1	0	0	1	1	0	0	1	1	0	0	1	1	0
0	1	0	1	0	1	0	1	0	1	0	1	0	1
1	1	1	1	1	1	1	0	0	0	0	0	0	0

Значение пользовательского ключа для конкретного варианта находится путем выполнения некоторого количества правых циклических сдвигов столбцов универсального ключа, которое определяется нижеследующей таблицей

Номер варианта	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Величина сдвига	3	7	9	11	13	15	1	2	3	5	7	9	11	13	4	6	8	10	12	14

I. Генерация раундовых ключей k_i

Секретный 56-битный пользовательский ключ

Секретный 64-битный пользовательский ключ (с контрольными битами)

Результат начальной перестановки пользовательского ключа – блоки C_0 и D_0.

																											C_0
																											D_0

Ключи C_1 и D_1, полученные в результате циклического сдвига блока C_0D_0

																											C_1
																											D_1

Раундовый ключ k_1

Сеансовые ключи C_{16} и D_{16}

																											C_{16}
																											D_{16}

Раундовый ключ k_{16}

II. Шифрование

1 раунд шифрования

Открытый текст

Результат начальной перестановки IP открытого текста

L_0:

R_0:

Блок R_0 после расширения E

Результат сложения по модулю два расширенного подблока R_0 с раундовым ключом k_1

						B_1
						B_2
						B_3
						B_4
						B_5
						B_6
						B_7
						B_8

Числа a и b, необходимые для S-преобразования, в двоичном и десятичном представлении

	a_2	a_{10}	b_2	b_{10}
B_1				
B_2				
B_3				
B_4				
B_5				
B_6				
B_7				
B_8				

Числа с в десятичном и двоичном представлении, полученные в результате S-преобразования

c_{10}	c_2	
		B'_1
		B'_2
		B'_3
		B'_4
		B'_5
		B'_6
		B'_7
		B'_8

Полученный в результате S-преобразования 32-битный блок $B'_1 \div B'_8$

Результирующее значение функции $f(R_0, k_1)$, полученное после перестановки P

Результат сложения по модулю два значения функции $f(R_0, k_1)$ с подблоком L_0

L_1:

R_1:

16 раунд шифрования

L_{15}:

R_{15}:

Блок R_{15} после расширения E

Результат сложения по модулю два расширенного подблока R_{15} с раундовым ключом k_{16}

						B_1
						B_2
						B_3
						B_4
						B_5
						B_6
						B_7
						B_8

Числа a и b, необходимые для S-преобразования, в двоичном и десятичном представлении

	a_2	a_{10}	b_2	b_{10}
B_1				
B_2				
B_3				
B_4				
B_5				
B_6				
B_7				
B_8				

Числа c в десятичном и двоичном представлении, полученные в результате S-преобразования

c_{10}	c_2	
		B'_1
		B'_2
		B'_3
		B'_4
		B'_5
		B'_6
		B'_7
		B'_8

Полученный в результате S-преобразования 32-битный блок $B'_1 \div B'_8$

Результирующее значение функции $f(R_{15}, k_{16})$, полученное после перестановки P

Результат сложения по модулю два значения функции $f(R_{15}, k_{16})$ с подблоком L_{15}

L_{16}:

R_{16}:

Результирующий 64-битный блок, полученный после выполнения 16-го раунда шифрования

Результирующий блок шифртекста, полученный после выполнения конечной перестановки IP^{-1}

III. Дешифрование

1 раунд дешифрования

Шифртекст

Результат начальной перестановки IP шифртекста

L_{16}:

R_{16}:

Блок L_{16} после расширения E

Результат сложения по модулю два расширенного подблока L_{16} с раундовым ключом k_{16}

						B_1
						B_2
						B_3
						B_4
						B_5
						B_6
						B_7
						B_8

Числа a и b, необходимые для S-преобразования, в двоичном и десятичном представлении

	a_2	a_{10}	b_2	b_{10}
B_1				
B_2				
B_3				
B_4				
B_5				
B_6				
B_7				
B_8				

Числа c в десятичном и двоичном представлении, полученные в результате S-преобразования

c_{10}	c_2	
		B'_1
		B'_2
		B'_3
		B'_4
		B'_5
		B'_6
		B'_7
		B'_8

Полученный в результате S-преобразования 32-битный блок $B'_1 \div B'_8$

Результирующее значение функции f (L_{16}, k_{16}), полученное после перестановки P

Результат сложения по модулю два значения функции f (L_{16}, k_{16}) с подблоком R_{16}

L_{15}:

R_{15}:

16 раунд дешифрования

L_1:

R_1:

Блок L_1 после расширения E

Результат сложения по модулю два расширенного подблока L_1 с раундовым ключом k_1

						B_1
						B_2
						B_3
						B_4
						B_5
						B_6
						B_7
						B_8

Числа a и b, необходимые для S-преобразования, в двоичном и десятичном представлении

	a_2	a_{10}	b_2	b_{10}
B_1				
B_2				
B_3				
B_4				
B_5				
B_6				
B_7				
B_8				

Числа c в десятичном и двоичном представлении, полученные в результате S-преобразования

c_{10}	c_2	
		B'_1
		B'_2
		B'_3
		B'_4
		B'_5
		B'_6
		B'_7
		B'_8

Полученный в результате S-преобразования 32-битный блок $B'_1 \div B'_8$

Результирующее значение функции $f(L_1, k_1)$, полученное после перестановки P

Результат сложения по модулю два значения функции $f(L_1, k_1)$ с подблоком R_1

L_0:

R_0:

Результирующий 64-битный блок, полученный после выполнения 16-го раунда дешифрования

Результирующий блок открытого текста, полученный после выполнения конечной перестановки IP^{-1}

Исходный блок открытого текста, полученный по заданию
