

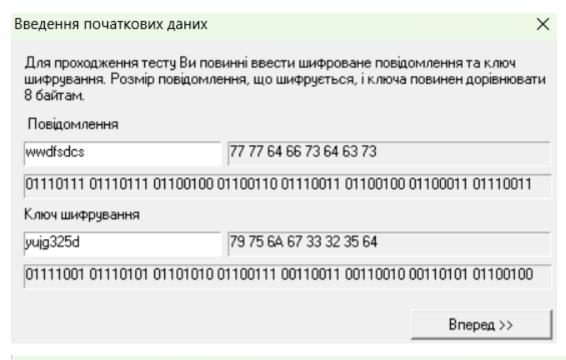
Міністерство освіти і науки України
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"
Факультет інформатики та обчислювальної техніки Кафедра інформаційних систем та технологій

Лабораторна робота №2

з дисципліни «Безпека інформаційних систем»

Виконав: студент групи IA-23: Лядський Д.С. Перевірив: Шимкович Л.Л.

Хід роботи:



Тест N1 "Початкова перестановка"

Виконайте перестановку вхідної послідовності згідно з таблицею. Результат введіть у вікні редактора "Результат".

Доведіть до кінця перестановку вхідної послідовності

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	б
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Номер зазначеного біта

7

Вхідна послідовність

Результат

Демонстрація

Вперед >>

X

Тест N2 "Отримання послідовностей R(0) та L(0)"				×
Розділіть отриману в попередньому тесті послідовність на дві послідовності L(0) та R(0), згідно з таблицями 1,2	Таблиц	я1		
відповідно. Натисніть кнопку "Демонстрація" для одержання послідовності L(0).	5	6	7	8
	9 13	10 14	11 15	12 16
Доведіть до кінця одержання послідовності R(0)	17 21	18 22	19 23	20 24
Номер зазначеного біта 32	25 29	26 30	27 31	28 32
Вхідна послідовність				
11111111 10010011 00101111 11010011 000000	0 00000 110	01101	1	
	0 00000 11(Таблиц		1	
	Таблиц	я2 34	35	36
11111111 10010011 00101111 11010011 000000	Таблиц — 33 37	я 2 34 38	35 39	40
Послідовність L(0) 111111110010011001111111010011	Таблиц - 33 - 37 - 41	я 2 34 38 42	35 39 43	40 44
Послідовність L(0) Послідовність B(0)	Таблиц — 33 37	я 2 34 38	35 39	40
Послідовність L(0) 111111110010011001111111010011	Таблиц 33 37 41 45 49 53	34 38 42 46 50	35 39 43 47 51 55	40 44 48 52 56
Послідовність L(0) Послідовність B(0)	Таблиц 33 37 41 45 49 53 57	34 38 42 46 50 54 58	35 39 43 47 51 55 59	40 44 48 52 56 60
Послідовність L(0) Послідовність B(0)	Таблиц 33 37 41 45 49 53	34 38 42 46 50	35 39 43 47 51 55	40 44 48 52 56

Демонстрація

Тест N3 "Функція		

Виконайте перестановку вхідної послідовності згідно з таблицею. Результат введіть у вікні редактора "Результат". Для демонстрації прикладу натисніть кнопку "Демонстрація".

Доведіть до кінця перестановку вхідної послідовності

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
б3	55	47	39	31	23	15
7	62	54	46	38	30	22
14	б	бl	53	45	37	29
21	13	5	28	20	12	4

 \times

Номер зазначеного біта

4

Вхідна послідовність

Результат

Демонстрація

Розділіть отриману в попередньому тесті	Табл	иця 1					
послідовність на дві послідовності С(0) та D(0), згідно з таблицями 1,2 відповідно. Натисніть	1	2	3	4	5	б	7
кнопку "Демонстрація" для одержання	8	9	10	11	12	13	14
послідовності С(0).	15	16	17	18	19	20	21
	22	23	24	25	26	27	28
Доведіть до кінця одержання послідовності D(0)	Табл	иця 2					
	29	30	31	32	33	34	35
Номер зазначеного біта	36	37	38	39	40	41	42
28	43	44	45	46	47	48	49
Вхідна послідовність	50	51	52	53	54	55	56
00000000 10001111 11111111 01110011 1100	1100 10	010000	0 0101	0011			
Послідовність С(0)							
1100/1405/11015 0(0)							
0000000010001111111111111111							

Демонстрація

Тест N5 "Отримання послідовності С(і)"	×
Отримайте послідовність C(i) з отриманої на попередньому кроці	Таблиця
послідовності С(0), шляхом зсуву послідовності С(i-1) на кількість біт зазначених у таблиці. Для демонстрації отримання С(i-1) із С(i-2) натисніть кнопку "Демонстрація".	N Зрушє
	2 1
Для того щоб отримати послідовність С(3) зрушуємо на 2 біт(а)	3 2 4 2
послідовність С(2)	5 2
Номер ітерації і	6 2 7 2
4	8 2
Вхідна послідовність С(0)	9 1
00000000 10001111 11111111 0111	10 2 11 2
	12 2
Послідовність С(і-2)	13 2
0000001000111111111111011100	14 2
00000010001111111111100	15 2
Послідовність С(і-1)	16 1
00001000111111111111110000	
Послідовність С(ї)	
00100011111111111111000000	
Демонстрація	Вперед >>

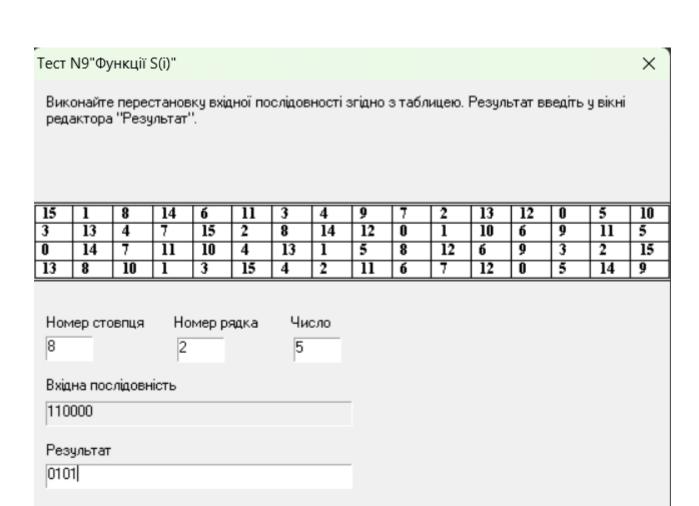
Тест N6 "Отримання послідовності D(i)"	×
Отримайте послідовність D(i) з отриманої на попередньому кроці послідовності D(0), шляхом зсуву послідовності D(i-1) на кількість біт зазначених у таблиці. Для демонстрації отримання D(i-1) із D(i-2) натисніть кнопку "Демонстрація". Для того щоб отримати послідовність D (10) зрушуємо на 2 біт(а) послідовність D(9) Номер ітерації і 11 Вхідна послідовність D(0) 00111100 11001010 00000101 0011	Таблиця N Зруше 1 1 2 1 3 2 4 2 5 2 6 2 7 2 8 2 9 1 10 2 11 2
Послідовність D(i-2) 0000001010011001111001100101 Послідовність D(i-1) 0000101001100111100110010100 Послідовність D(i) 0010100110011110011001010000	12 2 13 2 14 2 15 2 16 1
Демонстрація	Вперед>>

Тест N7 "Отримання послідовностей K(i)"							×
Для отримання послідовності К(і) зробіть конке		14	17	11	24	1	5
послідовностей С(і) та D(і). В отриманій послідов С(і)D(і) переставте біти згідно з таблицею. Для	ності	3	28	15	6	21	10
демонстрації натисніть кнопку "Демонстрація".		23	19	12	4	26	8
——————————————————————————————————————		16	7	27	20 37	13 47	2
Доведіть до кінця перестановку послідовності	C(i)D(i)	41 30	52 40	31 51	45	33	55 48
Zobodno do Kinda Hopochanobka Hoealdobhoch	O(1)D(1)	44	49	39	56	34	53
		46	42	50	36	29	32
32 Послідовність C(i)							
10000000010001111111111111111							
Послідовність D(i)							
1001111001100101000000101001							
Послідовність C(i)D(i)							
10000000010001111111111111111011100	01010000	001010	01				
Послідовність К(і)							
1101100110111110000101100000000000101010	11010011						

Демонстрація

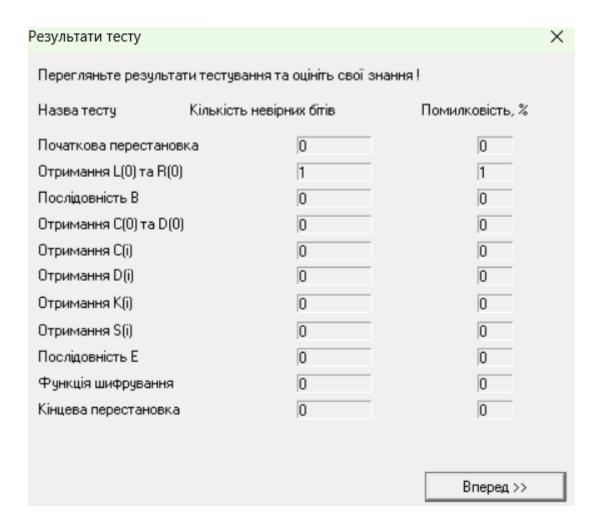
Тест N8 "Функція Е"						×
Використовуючи функцію E (дивись таблицю) провести перетворення послідовності R(i). Результат ввести у	32	1 5	6	3	4 8	5
вікні редактора "Результат". Для демонстрації натискайте кнопку "Демонстрація".	8	9	10 14	11	12 16	13 17
	16	17	18	19	20	21
Доведіть до кінця перестановку послідовності R(i)	20 24	21 25	22 26	23	24	25 29
	28	29	30	31	32	1
Номер зазначеного біта 27 Послідовність R(i) 01111100 00011011 01010110 11001001						
Результат						
101111111100000001111101101010101011011						

Демонстрація



X Тест N10 "Функція шифрування" Отримайте послідовність L(16)R(16), використовуючи послідовності L(15),R(15) і F(R(15),K(16)). Для демонстрації натискайте кнопку "Демонстрація". Доведіть побудову послідовностей L(16),R(16) і L(16)R(16) до кінця. Послідовність L(15) 01101111101000010000101000110011 Послідовність R(15) 01111100000110110101011011011001001 Послідовність F(R(15),K(16)) 1101100101111101110000100111110010 Послідовність L(16) 01111100000110110101011011011001001 Послідовність R(16) 10110110110110101000111011000001 Послідовність L(16)R(16) Демонстрація Вперед >>

Ruvousčes sosossavas	oo aia oo waari	10		10	120	1 7 7	101	100	122
Виконайте перестановку п отриманої на попередньом		40 39	7	48 47	16 15	56 55	24	64 63	32
таблицею. Результат введі		38	6	46	14	54	22	62	30
редактора "Результат".		37	5	45	13	53	21	бl	29
		36	4	44	12	52	20	60	28
Доведіть до кінця переста послідовності	новку вхідної	35	3	43	11 10	51 50	19 18	59 58	27
Послідовності		33	1	41	9	49	17	57	25
01111100 00011011 01010	0440 4004004 40	244044	1101	1010	10001	110 11	00000	14	
							00000	1	
Результат								еред>	>
								еред>	>
Результат 000100111011111001100110 Демонстрація	0001111001111101	1001100	000000)11001	111010	01011	Вп	еред>	>



Висновок: Отже, на цій лабораторній роботі ми розглянули Шифр DESта використали його на практиці.