ЛАБОРАТОРНА РОБОТА № 1. СТВОРЕННЯ ПРОГРАМНОЇ РЕАЛІЗАЦІЇ АЛГОРИТМУ ШИФРУВАННЯ DES

1.1 Мета роботи

Ознайомитись з методами і засобами симетричної криптографії, отримати навички створювання програмних засобів з використанням криптографічних інтерфейсів.

1.2 Теоретичні відомості

1.2.1 Блоковий шифр

Вхідними даними для блокового шифру є блок розміром *n* біт і *k*-бітний ключ. На виході, після застосування шифрувального перетворення, виходить *n*-бітний зашифрований блок, причому незначні відмінності вхідних даних як правило призводять до істотної зміни результату. Блокові шифри реалізуються шляхом багаторазового застосування до блоків вихідного тексту деяких базових перетворень.

Так як перетворення проводиться по блоках, як окремий крок, необхідно поділити вихідні дані на блоки необхідного розміру. При цьому незалежно від формату вихідних даних, будь то текстові документи, зображення або інші файли, вони повинні бути інтерпретовані в бінарний вигляд і тільки після цього розбиті на блоки. Все вищезазначене може здійснюватися як програмними, так і апаратними засобами.

1.2.2 Перетворення Мережею Фейстеля

Це перетворення над блоками які представляють собою ліву і праву половини регістру зсуву. В алгоритмі DES використовуються пряме перетворення мережею Фейстеля в шифруванні представлене на рисунку 1.1 та зворотне перетворення мережею Фейстеля в розшифруванні представлене на рисунку 1.2. Н схемах використовуються наступні означення:

- L та R – послідовності бітів (ліва (left) и права (right));
- XOR — операція побітового додавання по модулю 2;
- f – функція шифрування;
- ki – ключ на кожному раунді.

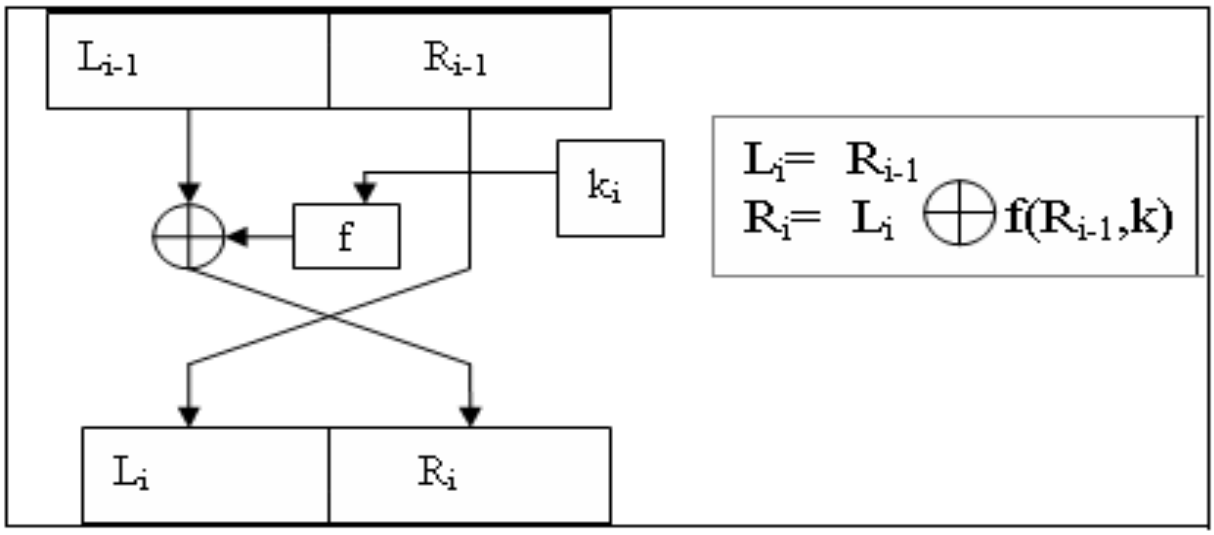

Рисунок 1.1 – Пряме перетворення мережею Фейстеля

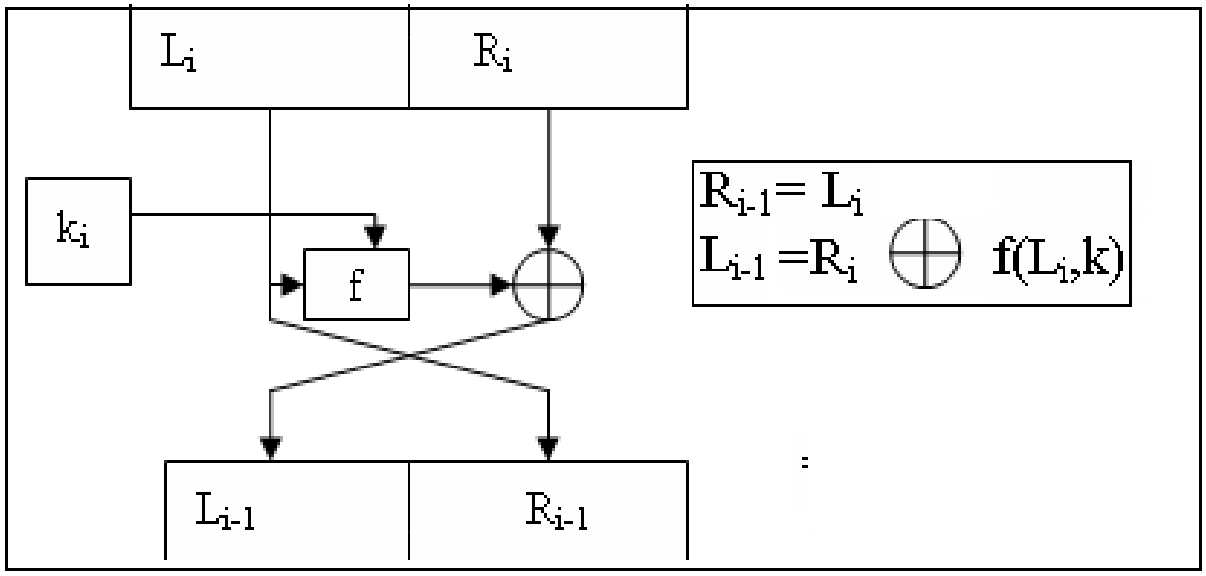

Рисунок 1.2 – Зворотне перетворення мережею Фейстеля

Функції шифрування та генерування ключів детальніше будуть розглянуті нижче.

1.2.3 Алгоритм DES

Загальна схема шифрування представлена на рисунку 1.3. Алгоритм DES – це симетричний алгоритм шифрування, який є типовим представником сімейства блокових шифрів. Призначений для шифрування даних 64-бітовими блоками. Довжина ключа дорівнює 56 бітам. Алгоритм представляє собою комбінацію двох основних методів шифрування підстановки і перестановки. Основним комбінаційним блоком DES є застосування до тексту одиничної комбінації цих двох методів. Такий блок називається раундом. DES включає в себе 16 раундів.

Рисунок 1.3 – Загальна схема шифрування в алгоритмі DES

Початкова перестановка IP (Initial Permutation). Згідно з рисунком 1.3 блок вхідного тексту перетворюється за допомогою матриці початкової перестановки IP, тобто біти вхідного блоку переставляються згідно з таблицею 1.1.

Таблиця 1.1 – Початкова перестановка IP

58	50	42	34	26	18	10	2	60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6	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

Після початкової перестановки 64-бітовий блок IP(T) приймає участь у 16 циклах перетворення Фейстеля.

Необхідно розбити IP(T) на дві частини L_0 та R_0, де L_0 та R_0 - відповідно 32 старших бітів і 32 молодших бітів блока. Припустимо$T_{i-1}=L_{i-1}R_{i-1}$ результат (i-1) ітерації, тоді результат і-ой ітерації $T_i = L_iR_i$ знаходиться:

$$L_i = R_{i-1}$$
$$R_i = L_{i-1} \oplus f(R_{i-1},k_i)$$

Ліва частина L_i дорівнює правій частині попереднього вектору $L_{i-1}R_{i-1}$. В свою чергу права частина R_i – це бітове додавання L_{i-1} та $f(R_{i-1},k_i)$ по модулю 2.

В 16 циклах перетворення Фейстеля функція f грає роль шифрування. Аргументами функції f є 32-бітовий вектор R_{i-1} та 48-бітовий ключ k_i, які є результатом перетворення 56-бітового начального ключа шифру.

Для обчислення функції f використовуються: функція розширення E, перетворення S (з 8 перетворень S-блоків), і перестановка P.

Функція E розширює 32-бітовий вектор R_{i-1} до 48-бітового вектору $E(R_{i-1})$ шляхом дублювання деяких бітів із R_{i-1}. Порядок бітів вектору $E(R_{i-1})$ приведено в табл. 1.2.

Таблиця 1.2 – Функція розширення E

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Після перестановки згідно з таблицею 1.2 блок $E(R_{i-1})$ додається по модулю 2 з ключами k_i. Далі представляється у вигляді восьми послідовних блоків B_1, B_2, ... B_8. $E(R_{i-1}) = B_1B_2 \ldots B_8$. Кожен B_j є 6-бітовим блоком. Далі кожен з блоків B_j трансформується в 4-бітови4й блок B'_j за допомогою перетворень S_j. Перетворення S_j визначаються таблицею 1.3.

Таблиця 1.3 – Перетворення S_j, j=1…8

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	
0	14	4	13	1	2	5	11	8	3	10	6	12	5	9	0	7	**S_1**
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8	
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0	
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13	
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10	**S_2**
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5	
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15	
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9	
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8	**S_3**
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1	
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7	
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12	
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15	**S_4**
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9	
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4	
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14	

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9	**S_5**
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6	
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14	
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3	
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11	**S_6**
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8	
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6	
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13	
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1	**S_7**
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6	
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2	
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12	
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7	**S_8**
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2	
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8	
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11	

Припустимо, що B_3 = 101111, і ми хочемо знайти B'_3. Перший і останній розряди B_3 є двійковим записом числа **a**, 0<=**a**<=3, середні 4 розряди представляють число **b**, 0<=b<=15. Рядки таблиці 1.3 нумеруються від 0 до 3, стовпці – нумеруються від 0 до 15. Пара чисел (**a**, **b**) визначає число, що знаходиться на перетині рядка **a** і стовпця **b**. Двійкове подання цього числа дає B'_3. У нашому випадку **a** = 11_2 = 3, **b** = 0111_2 = 7, та число, яке визначається парою (3,7), дорівнює 7. Його двійкове подання B'_3 = 0111.

Значення функції f (R_{i-1}, k_i) (32 біт) знаходиться перестановкою P, яку застосовують до 32-бітового блоку $B'_1B'_2$ ... B'_8. Перестановка P задана таблицею 1.4.

Таблиця 1.4 – Перестановка P

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

$f(R_{i-1}, k_i)=P(B'_1B'_2...B'_8)$

Згідно таблиці 1.4, перші чотири біта результуючого вектору після дії функції f – це біти 16, 7, 20, 21 вектору $B'_1B'_2$ ... B'_8.

Генерування ключів k_i

Ключі k_i виходять з початкового ключа k (64 біт = 8 байтів або 8 символів у ASCII). Вісім бітів, що знаходять в позиціях 8, 16, 24, 32, 40, 48, 56, 64 додаються в ключ k таким чином щоб кожен байт містив непарне число одиниць. Це використовується для виявлення помилок при обміні і зберіганні ключів. Потім роблять перестановку для розширеного ключа (крім бітів що додаються 8, 16, 24, 32, 40, 48, 56, 64). Така перестановка визначена у таблиці 1.5.

Таблиця 1.5 – Перестановка бітів для знаходження розширеного ключа

57	49	41	33	25	17	9	1	58	50	42	34	26	18	**C_0**
10	2	59	51	43	35	27	19	11	3	60	52	44	36	
63	55	47	39	31	23	15	7	62	54	46	38	30	22	**D_0**
14	6	61	53	45	37	29	21	13	5	28	20	12	4	

Ця перестановка визначається двома блоками C_0 і D_0 по 28 біт кожен. Перші 3 біти C_0 є біти 57, 49, 41 розширеного ключа. А перші три біта D_0 є біти 63, 55, 47 розширеного ключа. C_i, D_i i = 1,2,3 ... виходять з C_{i-1}, D_{i-1} одним або двома лівими циклічними зсувами згідно з таблицею 1.6.

Таблиця 1.6 – Циклічні зсуви

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Число зсуву	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Ключ k_i, i = 1 ... 16 складається з 48 біт, вибраних з бітів вектору C_iD_i (56 біт) згідно з таблицею 1.7. Перший і другий біти k_i є біти 14, 17 вектору C_iD_i.

Таблиця 1.7 – 48 біт ключа

14	17	11	24	1	5	3	28	15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2	41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56	34	53	46	42	50	36	29	32

Кінцева перестановка.

Кінцева перестановка IP^{-1} діє на T_{16} і використовується для відновлення позиції. Вона є зворотною до перестановки IP. Кінцева перестановка визначається таблицею 1.8.

Таблиця 1.8 – Кінцева перестановка

40	8	48	16	56	24	64	32	39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30	37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28	35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26	33	1	41	9	49	17	57	25

Схема розшифрування

При розшифруванні даних всі дії виконуються в зворотному порядку. У 16 циклах розшифрування, на відміну від шифрування за допомогою прямого перетворення мережею Фейстеля, тут використовується зворотне перетворення мережею Фейстеля.

$R_{i-1} = L_i$

$L_{i-1} = R_i \oplus f(L_i, k_i)$

1.3 Завдання до виконання роботи

1. Створити програмну реалізацію алгоритму* шифрування DES (без використання готових функцій).

* завдання узгодити з викладачем лабораторних робіт.

2. Зробити перевірку на виключення слабких ключів.

3. На кожному раунді мережі Фейстеля визначити ентропію появи біту, що дорівнює 1.

4. Створити приємний та зрозумілий інтерфейс для перевірки зробленої роботи.

5. Сформувати звіт в електронному вигляді.

1.4 Зміст звіту

1. Тексти розроблених програм.
2. Копії екранних форм з результатами.
3. Висновки.

1.5 Контрольні запитання

1. Які криптографічні шифри називають симетричними?
2. Зобразить схематично роботу алгоритму DES.
3. Що мається на увазі під поняттям блоковий шифр?
4. Що представляє собою мережа Фейстеля?
5. Назвіть головні параметри шифру DES (довжина блоків, довжина ключа, кількість раундів роботи мережі Фейстеля).

6. Як генеруються ключі в раундах?
7. Які перестановки існують в даному алгоритмі?
8. Що представляють собою S-блоки?
9. Які ви знаєте слабкі ключі?

Як проходить розшифрування по алгоритму DES?