Лабораторна робота № 3

МЕРЕЖІ ФЕЙШТЕЛЯ

Мета роботи: вивчити принципи роботи мережі Фейштеля, навчитися шифрувати інформацію за допомогою використання блокового криптоалгоритму.

Основні теоретичні відомості

Основи криптоалгоритмів на базі мережі Фейштеля

Мережа Фейштеля отримала широке поширення, оскільки забезпечує виконання вимоги про багатократне використання ключа і матеріалу вихідного блоку інформації. Класична мережа Фейштеля має наступну структуру:

Незалежні потоки інформації, породжені з початкового блоку, називаються вітками мережі. У класичній схемі їх дві. Величини V_i називаються параметрами мережі, звичайно це функції від матеріалу ключа. Функція F називається твірною. Дія, що складається з одноразового обчислення твірної функції, і подальшого накладення її результату на іншу вітку з обміном їх місцями, називається циклом або раундом (англ. round) мережі Фейштеля. Оптимальне число раундів K - від 8 до 32. Часто кількість раундів не фіксується розробниками алгоритму, а лише вказуються розумні межі (обов'язково нижній, і не завжди – верхній) цього параметра.

Ця схема є оборотною. Мережа Фейштеля має ту властивість, що навіть якщо в якості твірної функції F буде використане безповоротне перетворення, то і в цьому випадку увесь ланцюжок буде відновлюваний. Це відбувається внаслідок того, що для зворотного перетворення мережі Фейштеля не потрібне обчислення функції F^{-1}.

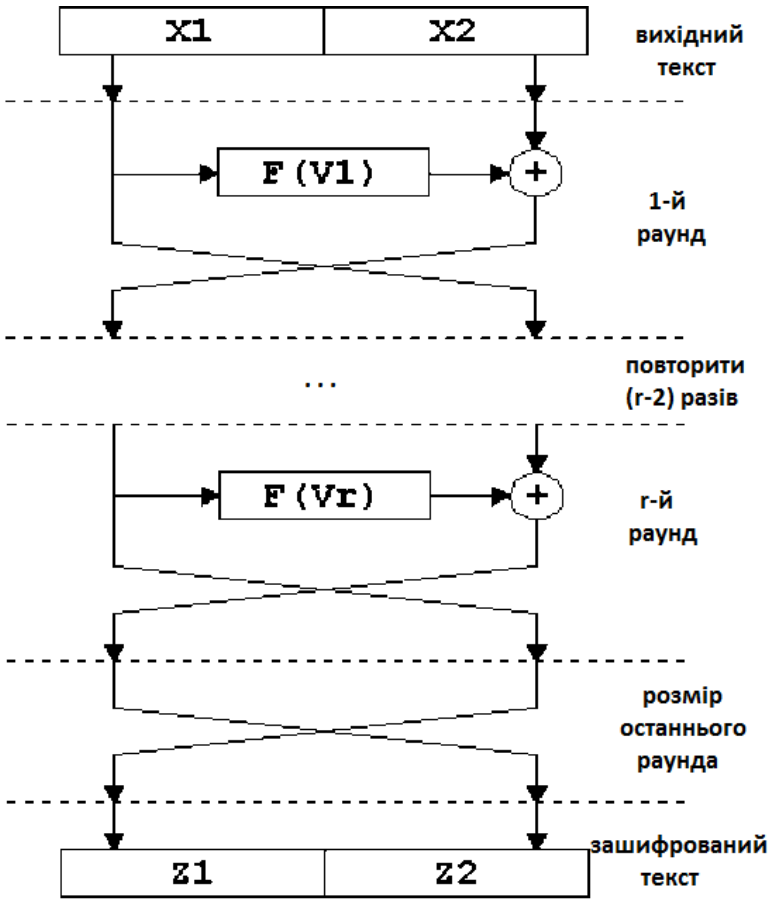

Рис. 1. Класична структура мережі Фейштеля.

Мережа Фейштеля симетрична за рахунок використання операції XOR і для її оборотності не має значення чи є число раундів парним або непарним числом.

Використання модифікації мережі Фейштеля для більшого числа віток пов'язане з тим, що при великих розмірах кодованих блоків (128 і більше біт) стає незручно працювати з математичними функціями за модулем 64 і вище. Основні одиниці інформації, що обробляються процесорами на сьогодні – це байт і подвійне машинне слово 32 біта. Буде логічно розбивати початкові блоки не на дві, а на 4 частини. В цьому випадку мережа Фейштеля може набирати такого вигляду:

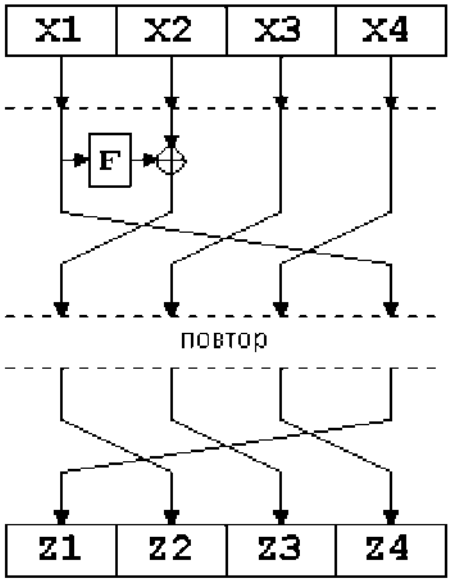

Рис. 2. Структура модифікованої мережі Фейштеля.

Алгоритм призначений для шифрування і дешифрування інформації, що представляється у вигляді слів, розрядністю 128 біт на основі 64-бітового ключа. Операції шифрування і дешифрування є інверсними і використовують один і той же ключ.

Розглянемо шифрування одного блоку.

Позначимо X1X2X3X4 конкатенацію послідовностей X1, X2, X3 і X4, в якій біти послідовностей X1, X2, X3, X4 слідують один за одним. Розмірність послідовності дорівнює сумі розмірностей всіх складових. Символом «+» позначимо операцію побітового складання за модулем 2.

Ітеративний процес шифрування описується наступними формулами:

$X1(i) = X2(i-1)+F(V_i)$, i = 1, 2, ..., n;

X2(i) = X3(i-1), i = 1, 2, ..., n;

X3(i) = X4(i-1), i = 1, 2, ..., n;

$X4(i) = X1(i-1)$, i = 1, 2, ..., n; де $F(V_i)$ – твірна функція;

n – кількість раундів, може змінюватися, залежно від вимог з швидкодії і криптостійкості (n= 8 - 128);

V_i =X1(i-1)+h(K) – параметр мережі;

h(K)= K1 ROL i + K2 ROR i,

K1 і K2 – ліва і права частині ключа K,

ROL і ROR – операції циклічного зсуву вліво і вправо відповідно.

Пропонований алгоритм має ряд достоїнств. В першу чергу – простота реалізації і висока швидкодія, яка досягається за рахунок використання операцій, що мають високу швидкість виконання.

Дешифрування блоку інформації проводиться тією ж мережею Фейштеля, але з інверсним порядком параметрів мережі. У явному виді ключ в алгоритмі не використовується, що підвищує його криптостійкість. При знанні ключа, але відсутності інформації про кількість раундів криптоаналітику буде досить складно дешифрувати зашифровану інформацію.

Методика виконання роботи

1. Вибрати в таблиці параметри для мережі Фейштеля
2. Розробити програму шифрування і дешифрування тексту.
3. Провести шифрування початкового тексту.
4. Виконати дешифрування отриманої шифрограми і порівняти результат з початковим текстом.
5. Результати роботи оформити у вигляді звіту.

Зміст звіту

1. Опис використовуваного методу, опис початкових даних.
2. Алгоритм роботи програми, текст програми, результати роботи програми.
3. Аналіз результатів, висновки.

Варіанти індивідуальних завдань

Варіанти завдань представлені в таблиці 1, номер варіанту вибирається відповідно до номера студента в списку групи.

Таблиця 1. Параметри мережі Фейштеля.

Номер вар.	Кількість раундів	Твірна функція
1	8	Додавання
2	10	Виключаюче АБО
3	12	Множення за модулем 2^N+1
4	14	Множення за модулем 2^N
5	10	Арифметичний зсув вправо
6	18	Арифметичний зсув вліво
7	20	Додавання
8	8	Множення за модулем 2^N+1
9	24	Виключаюче АБО
10	20	Додавання
11	18	Множення за модулем 2^N+1
12	28	Виключаюче АБО
13	12	Додавання
14	14	Додавання
15	24	Виключаюче АБО
16	22	Додавання
17	8	Додавання
18	10	Множення за модулем 2^N
19	22	Виключаюче АБО
20	14	Додавання