Лабораторна робота №2

ШИФРУВАННЯ ДАНИХ ЗА ДОПОМОГОЮ ГЕНЕРАТОРА ПСЕВДОВИПАДКОВИХ ЧИСЕЛ

Мета роботи: освоєння принципів шифрування гамуванням, вивчення властивостей генератора псевдовипадкових чисел, програмна реалізація методу гамування.

Основні теоретичні відомості

Принцип шифрування гамуванням полягає в генерації гами шифру за допомогою датчика псевдовипадкових чисел і накладенні отриманої гами шифру на відкриті дані оборотним чином (наприклад, використовуючи операцію додавання за модулем 2). Процес дешифрування зводиться до повторної генерації гами шифру при відомому ключі і накладенні такої ж гамми на зашифровані дані.

Отриманий зашифрований текст є досить важким для розкриття у тому випадку, якщо гама шифру не містить бітових послідовностей, що повторюються і змінюється випадковим чином для кожного шифрованого слова. Якщо період гами перевищує довжину всього зашифрованого тексту і невідома жодна частина початкового тексту, то шифр можна розкрити тільки прямим перебором (підбором ключа). В цьому випадку криптостійкість визначається розміром ключа.

Метод гамування стає безсилим, якщо відомий фрагмент вихідного тексту і шифрограма, що відповідає йому. В цьому випадку простим відніманням за модулем 2 виходить відрізок псевдовипадкової послідовності і по ньому відновлюється вся ця послідовність.

Шифрування даних за допомогою датчика псевдовипадкових чисел (ПВЧ)

Лінійні конгруентні датчики ПВЧ

Щоб отримати лінійні послідовності елементів гами, довжина яких не перевищує розмір шифрованих даних, використовують датчики ПВЧ. Одним з хороших конгруентних генераторів є лінійний конгруентний датчик ПВЧ. Він виробляє послідовності псевдовипадкових чисел T(i), що описуються співвідношенням

$$T(i+1) = (A * T(i) + C) \bmod M,$$

де A і C – константи, T(0) – початкова величина, що вибрана в якості генеруючого числа. Очевидно, що ці три величини і утворюють ключ.

Такий датчик ПВЧ генерує псевдовипадкові числа з визначеним періодом повторення, що залежить від вибраних значень A і C. Значення M зазвичай встановлюється рівним 2^b, де b – довжина машинного слова у бітах. Необхідно вибирати числа A і C так, щоб період M був максимальним.

Як показано Д. Кнуттом, лінійний конгруентний датчик має максимальну довжину M тоді, коли C непарне і A mod 4 = 1. Ще одними підходом до вибору відповідних чисел є: числа A і M та C і M мають бути взаємно простими (НСД(A,M)=1, НСД(C,M)=1), а $0 \le T(i) < M$.

Як приклад використання лінійного конгруентного датчика ПВЧ розглянемо процес шифрування початкового тексту "абв". Нехай b = 5, тоді у відповідності з номером у абетці: літера "а" має двійковий код 00001; літера "б" має двійковий код 00010; літера "в" має двійковий код 00011. Початковий текст буде представлений у вигляді послідовності 00001 00010 00011.

Для формування гами шифру виберемо параметри датчика ПВЧ : A=5; C=3; T(0)=7; $M=2^b$; b=5; $M=2^5=32$. Сформуємо три псевдовипадкові числа:

T(1) = (5*7+3) mod 32 = 6 (00110);

T(2) = (5*6+3) mod 32 = 1 (00001);

T(3) = (5*1+3) mod 32 = 8 (01000).

Отримана гама шифру 00110 00001 01000. Зашифрований текст виходить шляхом накладення гами шифру на початковий текст (шляхом додавання за модулем 2):

00001 00010 00011
<u>00110 00001 01000</u>
00111 00011 01011

що відповідає шифрограмі "еви", "е" (сьома буква в абетці) має код 00111, "в" (третя буква в абетці) має код 00011, "и" (одинадцята буква в абетці) має код 01011.

Дешифрування проводиться шляхом накладення тієї ж гамми на зашифрований текст:

00111 00011 01011
<u>00110 00001 01000</u>
00001 00010 00011

Метод гамування із зворотним зв'язком

Полягає в тому, що для отримання сегменту гами використовується контрольна сума певної ділянки шифрованих даних. Наприклад, якщо розглядати гаму шифру як об'єднання множин H(j), що не перетинаються, то процес шифрування можна представити наступними кроками:

1. Генерація сегменту гами H(1) і накладення його на відповідну ділянку шифрованих даних.
2. Підрахунок контрольної суми ділянки, що відповідає сегменту гами H(1).
3. Генерація з врахуванням контрольної суми вже зашифрованої ділянки даних наступного сегменту гам H(2).
4. Підрахунок контрольної суми ділянки даних, що відповідає сегменту даних H(2) і так далі.

Під контрольною сумою розуміють функцію f(t(1), ..., t(n)), де t(i) – і-е слово шифрованих даних.

Зашифруємо початковий текст "абв", представлений у вигляді послідовності 00001 00010 00011. Нехай A=5; C=3; b=5; M=32;T(0)=7. Тоді:

T(1) = (5*7+3) mod 32 = 6 (00110).

В якості контрольної суми ділянки даних, виберемо кількість одиниць на цій ділянці. Тоді сегменту H(1) відповідає ділянка 00010, кількість одиниць дорівнює 1.

T(2) = (5*1+3) mod 32 = 8 (01000).

Контрольна сума наступної ділянки (00010) дорівнює 1.

T(3) = (5*1+3) mod 32 = 8 (01000).

Отримана шифрограма:

00001 00010 00011
<u>00110 01000 01000</u>
00111 01010 01011

що відповідає тексту "ези".

Методика виконання роботи

1. Вибрати в таблиці параметри генератора псевдовипадкових чисел: A, C, T(0), b.
2. Розробити програму шифрування і дешифрування тексту.

3. Провести шифрування початкового тексту, отримати шифрограму, виконати її дешифрування і порівняння з початковим текстом.
4. Провести зміну одного або декілька параметрів генератора випадкових чисел, здійснити отримання шифрограми і порівняння її з попереднім варіантом.
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

Таблиця 1. Генератори ПВЧ

№ варіанту	Вид генератора ПВЧ	Кількість розрядів b
1	Лінійні конгруентні датчики ПВЧ	6
2	Гамування із зворотним зв'язком	7
3	Лінійні конгруентні датчики ПВЧ	8
4	Гамування із зворотним зв'язком	6
5	Лінійні конгруентні датчики ПВЧ	7
6	Гамування із зворотним зв'язком	8
7	Лінійні конгруентні датчики ПВЧ	6
8	Гамування із зворотним зв'язком	7
9	Лінійні конгруентні датчики ПВЧ	8
10	Гамування із зворотним зв'язком	6
11	Лінійні конгруентні датчики ПВЧ	7
12	Гамування із зворотним зв'язком	8
13	Лінійні конгруентні датчики ПВЧ	6
14	Гамування із зворотним зв'язком	7
15	Лінійні конгруентні датчики ПВЧ	8
16	Гамування із зворотним зв'язком	6
17	Лінійні конгруентні датчики ПВЧ	7
18	Гамування із зворотним зв'язком	8
19	Лінійні конгруентні датчики ПВЧ	6
20	Гамування із зворотним зв'язком	7
21	Лінійні конгруентні датчики ПВЧ	8
22	Гамування із зворотним зв'язком	6
23	Лінійні конгруентні датчики ПВЧ	7
24	Гамування із зворотним зв'язком	8

Контрольні запитання

1. Які параметри конгруентного генератора необхідно вибрати для отримання максимальної довжини послідовності псевдовипадкових чисел?
2. Від чого залежить довжина псевдовипадкової послідовності?

3. Принцип дії генераторів із зворотним зв'язком?
4. Які стандарти використовують методи гамування?