МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет кібербезпеки, комп’ютерної та програмної інженерії

Кафедра інженерії програмного забезпечення



Лабораторна робота №2

з дисципліни «Безпека ПД»

На тему: «Симетричні системи шифрування»

Варіант №5

Виконав студент:

групи ПІ-421Б

Іванюк Н. О.

Перевірив викладач:

Радішевський М. Ф.

Київ 2022

**Порядок виконання роботи**

**Завдання 1.** Дослідження адитивної групи класів залишків по модулю m=7

Скласти таблицю. додавання класів залишків по модулю m=7

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **+** | **1** | **2** | **3** | **4** | **5** | **6** |
| **1** | 2 | 3 | 4 | 5 | 6 | 0 |
| **2** | 3 | 4 | 5 | 6 | 0 | 1 |
| **3** | 4 | 5 | 6 | 0 | 1 | 2 |
| **4** | 5 | 6 | 0 | 1 | 2 | 3 |
| **5** | 6 | 0 | 1 | 2 | 3 | 4 |
| **6** | 0 | 1 | 2 | 3 | 4 | 5 |

На основі заповненої таблиці скласти таблицю зворотних елементів

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| a | 1 | 2 | 3 | 4 | 5 | 6 |
| -a | 6 | 5 | 4 | 3 | 2 | 1 |

Скласти таблиці віднімання класів залишків по модулю m=7

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| - | **1** | **2** | **3** | **4** | **5** | **6** |
| **1** | 0 | 6 | 5 | 4 | 3 | 2 |
| **2** | 1 | 0 | 6 | 5 | 4 | 3 |
| **3** | 2 | 1 | 0 | 6 | 5 | 4 |
| **4** | 3 | 2 | 1 | 0 | 6 | 5 |
| **5** | 4 | 3 | 2 | 1 | 0 | 6 |
| **6** | 5 | 4 | 3 | 2 | 1 | 0 |

Віднімання класів лишків зводиться до додаванню зворотного елемента

a – b mod m = a +(-b) mod m

**Завдання 2.** Дослідження адитивної групи класів залишків по модулю 6 По вище наданої методики скласти таблиці додавання, зворотних елементів та віднімання для групи класів залишків по модулю m=6

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **+** | **1** | **2** | **3** | **4** | **5** | **6** |
| **1** | 2 | 3 | 4 | 5 | 0 | 1 |
| **2** | 3 | 4 | 5 | 0 | 1 | 2 |
| **3** | 4 | 5 | 0 | 1 | 2 | 3 |
| **4** | 5 | 0 | 1 | 2 | 3 | 4 |
| **5** | 0 | 1 | 2 | 3 | 4 | 5 |
| **6** | 1 | 2 | 3 | 4 | 5 | 6 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| a | 1 | 2 | 3 | 4 | 5 | 6 |
| -a | 5 | 4 | 3 | 2 | 1 | 0 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| - | **1** | **2** | **3** | **4** | **5** | **6** |
| **1** | 0 | 5 | 4 | 3 | 2 | 1 |
| **2** | 1 | 0 | 5 | 4 | 3 | 2 |
| **3** | 2 | 1 | 0 | 5 | 4 | 3 |
| **4** | 3 | 2 | 1 | 0 | 5 | 4 |
| **5** | 4 | 3 | 2 | 1 | 0 | 5 |
| **6** | 5 | 4 | 3 | 2 | 1 | 0 |

**Завдання 3**. Дослідження мультиплікативної групи класів залишків по модулю m=7

Cкласти таблицю множення класів залишків по модулю m=7

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **\*** | **2** | **3** | **4** | **5** | **6** |
| **2** | 4 | 6 | 1 | 3 | 5 |
| **3** | 6 | 2 | 5 | 1 | 4 |
| **4** | 1 | 5 | 2 | 6 | 3 |
| **5** | 3 | 1 | 6 | 4 | 2 |
| **6** | 5 | 4 | 3 | 2 | 1 |

На основі заповненої таблиці скласти таблицю зворотних елементів

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| a | 2 | 3 | 4 | 5 | 6 |
|  | 4 | 5 | 2 | 3 | 6 |

Скласти таблиці ділення класів залишків по модулю 7

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **/** | **2** | **3** | **4** | **5** | **6** |
| **2** | 1 | 3 | 4 | 6 | 5 |
| **3** | 5 | 1 | 6 | 2 | 4 |
| **4** | 2 | 6 | 1 | 5 | 3 |
| **5** | 6 | 4 | 3 | 1 | 2 |
| **6** | 3 | 2 | 5 | 4 | 1 |

**Завдання 4.** Дослідження мультиплікативної групи класів залишків по модулю 6

По вище наданої методики скласти таблиці множення для групи класів залишків по модулю m=6. Відмітити, для яких класів відсутній зворотний клас і відповідно операція ділення.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **\*** | **2** | **3** | **4** | **5** | **6** |
| **2** | 4 | 6 | 2 | 4 | 6 |
| **3** | 6 | 3 | 6 | 3 | 6 |
| **4** | 2 | 6 | 4 | 6 | 3 |
| **5** | 4 | 3 | 6 | 1 | 2 |
| **6** | 6 | 6 | 3 | 2 | 6 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| a | 2 | 3 | 4 | 5 | 6 |
|  | - | - | - | 1 | - |

Таким чином у нас немає зворотніх значень для усіх класів з основою не простим числом. Тому операція ділення не є можливою них.

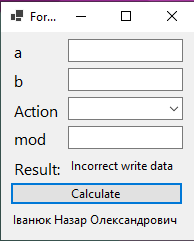
**Завдання 5.** Скласти таблицю піднесення в ступень класів залишків по модулю m =7.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **^** | **2** | **3** | **4** | **5** | **6** |
| **2** | 4 | 1 | 2 | 4 | 1 |
| **3** | 2 | 6 | 4 | 5 | 1 |
| **4** | 2 | 1 | 4 | 2 | 1 |
| **5** | 4 | 6 | 2 | 3 | 1 |
| **6** | 1 | 6 | 1 | 6 | 1 |

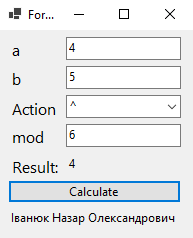
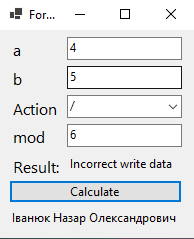
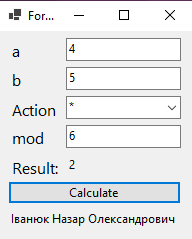
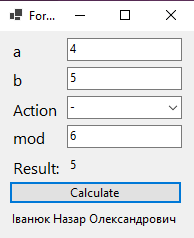
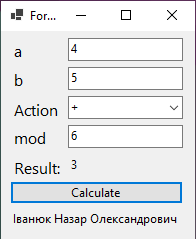
**Завдання 6.** Скласти таблицю піднесення в ступень класів залишків по модулю m =6.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **^** | **2** | **3** | **4** | **5** | **6** |
| **2** | 4 | 2 | 4 | 2 | 4 |
| **3** | 3 | 3 | 3 | 3 | 3 |
| **4** | 4 | 4 | 4 | 4 | 4 |
| **5** | 1 | 5 | 1 | 5 | 1 |
| **6** | 0 | 0 | 0 | 0 | 0 |

**Завдання 7**



Виконання



**Висновок:** Під час виконання лабораторної роботи вивчив симетричні системи шифрування, а саме простої підстановки та багато-абеткову систему шифрування. Також здобув практичний досвід в шифруванні даних цими системами. Дав відповіді на такі контрольні запитання:

**Контрольні питання**

1. Чому система шифрування зветься симетричною?

2. Як підрахувати кількість ймовірних ключів в системі шифрування з простою підстановкою?

3. Що треба робити, якщо сума номера букви та ключа більше розміру абетки.

4. Які недоліки метода простої підстановки усуває багато-абеткова система шифрування?

**Відповіді на контрольні запитання:**

Запитання 1: Системи шифрування називаються симетричними тому, що для їх шифрування і дешифрування використовується один і той же ключ.

Запитання 2: Для підрахування кількості ймовірних ключів в системі шифрування з простою підстановкою достатньо скористатися формулою . *Див примітка 1*

Запитання 3: Для того щоб вирішити проблему де сума номера букви та ключа більше розміру абетки достаньо від цієї суми відняти N.

Запитання 4: Недоліком простої підстановки є сильно обмежена кількість ключів які дорівнюють N-1. Багато-абеткова система шифрування усуває цю проблему таким чином що для кожного символу шифрованої фрази існує свій ключ, тобто збільшуючи кількість можливих ключів.

**Примітки :**

1. N- це розмір абетки (кількість різних символів в абетці).