Лабораторна робота №1

Програмна реалізація шифрів DES, AES та ДСТУ 7624:2014

Мета роботи: створити криптографічну систему шифрування даних, яка базується на алгоритмах шифрування DES, AES та ДСТУ 7624:2014.

Завдання до роботи

Програмна реалізація криптографічної системи, ґрунтованої на алгоритмах шифрування DES, AES та ДСТУ 7624:2014, має бути оформлена як деяка програмна оболонка. У програмній реалізації має бути розроблений інтерфейс, зручний для експлуатації програми, в інтерфейсі слід передбачити:

- два режими формування ключа - ключ заданий, ключ формується за умовчанням;
- введення початкової інформації з сформованого заздалегідь файлу і з файлу, який створюється в оболонці програми;
- режими шифрування, які передбачені в DES, AES та ДСТУ 7624:2014 (ECB, CBC, PCBC, CFB, OFB);
- режими шифрування і дешифрування інформації.

Підготувати звіт по роботі. У звіті описати алгоритми DES, AES та ДСТУ 7624:2014 та режими їх роботи, описати структуру представлення даних в програмі, основні функції програми, призначення функцій, вхідні і вихідні параметри функцій. У звіт включити опис алгоритму генерації ключа, деталі програмної реалізації, які представляють інтерес з точки зору розробника.

Контрольні запитання

1. По якому принципу побудовані шифри *DES, AES* та *ДСТУ 7624:2014?*
2. Який шифри передували шифрам *DES, AES* та *ДСТУ 7624:2014?*
3. Вказати довжину початкового ключа в алгоритмах *DES, AES* та *ДСТУ 7624:2014.*
4. Вказати основні етапи формування ключів в алгоритмах *DES, AES* та *ДСТУ 7624:2014.*
5. Скільки раундів в алгоритмах *DES, AES* та *ДСТУ 7624:2014?*
6. Скільки ключів формується в алгоритмах *DES, AES* та *ДСТУ 7624:2014* для шифрування тексту?
7. Вказати довжину ключа при шифруванні тексту в алгоритмах *DES, AES* та *ДСТУ 7624:2014.*
8. Які арифметичні операції використовуються при перетвореннях в алгоритмах *DES, AES* та *ДСТУ 7624:2014?.*
9. Вкажіть довжину шифрованого блоку в алгоритмах *DES, AES* та *ДСТУ 7624:2014.*
10. Порівняйте криптостійкість алгоритмів і вкажіть їх основні переваги і недоліки.

Лабораторна робота №2

Програмна реалізація алгоритмів шифрування RSA та Ель-Гамаля.

Мета роботи: створити учбовий варіант криптографічної системи з відкритим ключем на алгоритмах RSA, Ель-Гамаля та Ель-Гамаля для еліптичних кривих.

Завдання до роботи

Програмна реалізація має бути оформлена як деяка програмна оболонка.
У програмній реалізації має бути розроблений інтерфейс, зручний для експлуатації програми, в інтерфейсі передбачити режим завдання параметрів системи за умовчанням і режим генерування параметрів системи. У програму включити простий алгоритм формування простих чисел і перевірки чисел на простоту. Оформити програми перевірки чисел на простоту як самостійні модулі, щоб при необхідності ці модулі можна було замінити на інші програмні реалізації.
Підготувати звіт по роботі. У звіт включити опис алгоритмів RSA та Ель-Гамаля і алгоритм перевірки чисел на простоту та Ель-Гамаля для еліптичних кривих. Підготувати для демонстрації програми контрольний приклад.
Обгрунтувати вибір типу та параметрів еліптичної кривої.
У роботу включити програми:

- формування простого числа;
- перевірки чи є число простим
- шифрування та дешифрування даних.

Контрольні запитання

1.Дати визначення односторонньої функції.
2.Дати визначення односторонньої функції з секретом.
3. На якій базі зазвичай створюються криптографічні системи з відкритими ключами?
4. Перерахувати число параметрів в криптографічних системах RSA та Ель-Гамаля.
5. Перерахувати секретні параметри систем RSA та Ель-Гамаля.
6. Перерахувати відкриті параметри систем RSA та Ель-Гамаля.
7. Яким умовам повинні задовольняти параметри систем RSA та Ель-Гамаля?
8. На яких математичних задачах з теорії чисел базуються алгоритми RSA та Ель-Гамаля?
9. Опишіть схему шифрування тексту з використанням алгоритмів RSA та Ель-Гамаля.
10. Опишіть схему дешифрування тексту з використанням алгоритмів RSA та Ель-Гамаля.
11. Дати визначення еліптичної кривої.

Лабораторна робота №3

Програмна реалізація MD 5, SHA 3 і ДСТУ 7564:2014.

Мета роботи: створити програму, яка обчислює профіль початкового тексту. Надалі програму можна використати для виконання лабораторної роботи при реалізації електронного цифрового підпису(ЭЦП).

Завдання до роботи

Програмна реалізація має бути оформлена як деяка програмна оболочка, яка включає два алгоритми MD 5, SHA 3 і ДСТУ 7564:2014 для обчислення профілю початкової інформації.

Підготувати звіт по роботі. У звіті описати алгоритми MD 5, SHA 3 і ДСТУ 7564:2014 описати структуру алгоритмів. Представлення даних в програмі, основні функції програми, призначення функцій, вхідні і вихідні параметри функцій. Підготувати для демонстрації програми контрольний приклад.

Контрольні запитання

1.Основне призначення хеш-функції ?
2. Перерахувати клас завдань, які вирішуються із застосуванням хеш-функції.
3. Перерахувати, які основні властивості повинна мати хеш-функція.
4. Довжина вхідного блоку у бітах для функції стискування алгоритму.
5. Назвати число раундів в алгоритмі.
6. Назвати число кроків в кожному раунді алгоритму.
7.Назвати, які операції використовуються у функції стискування алгоритму MD 5.
8. Перерахувати основні постійні дані, які використовуються в алгоритмі MD 5.
9. Скільки примітивних функцій використовуються в алгоритмі MD 5?
10. Назвати, які операції використовуються у функції стискування алгоритму SHA 3.
11. Перерахувати основні постійні дані, які використовуються у алгоритмі SHA 3.
12. Назвати число раундів в алгоритмі SHA 3.
13. Скільки примітивних функцій використовуються в алгоритмі SHA 3?
14. Довжина вхідного блоку у бітах для функції стискування алгоритму SHA 3.
15. Число кроків в кожному раунді алгоритму SHA 3.
16. Назвати, які операції використовуються у функції стискування алгоритму ДСТУ 7564:2014.
17. Перерахувати основні постійні дані, які використовуються у алгоритмі ДСТУ 7564:2014.
18. Назвати число раундів в алгоритмі ДСТУ 7564:2014.
19. Скільки примітивних функцій використовуються в алгоритмі ДСТУ 7564:2014?
20. Довжина вхідного блоку у бітах для функції стискування алгоритму ДСТУ 7564:2014.
21. Число кроків в кожному раунді алгоритму ДСТУ 7564:2014.

Лабораторна робота 4
Програмна реализація алгоритмів ЕЦП

Ціль роботи – створити програму, яка реалізує різні варіанти схем ЕЦП, використовуючи алгоритми з відкритими ключами.

Завдання до роботи

Реалізувати ЕЦП на базі алгоритмів Ель-Гамаля, RSA, Шнорра і Рабіна. При формуванні ЕЦП на базі алгоритма RSA використовувати результати лабораторної работи № 2. Передбачити режими формування параметрів криптосистем. Програму оформити, як інтегроване середовище із зручним інтерфейсом формування ЕЦП і її перевірки. Підготувати звіт, в який включити опис алгоритмів формування ЕЦП, опис функцій з яких складається програма. Підготувати для демонстрації контрольний приклад. При формуванні цифрового підпису передбачити схему ЕЦП з використанням хеш-функцій (див. лабораторну роботу № 3).

Контрольні питання:

1.Перерахувати число параметрів в криптографічній системі Ель- Гамаля.
2.Перерахувати секретні параметри системи Ель-Гамаля.
3.Перерахувати відкриті параметри системи Ель-Гамаля.
4.На якому досить важкому завданні з теорії чисел базується криптографічна система Ель-Гамаля.
5.Описати схему формування ЕЦП з використанням алгоритму Ель- Гамаля.
6.Описати схему перевірку ЕЦП з використанням алгоритму Ель- Гамаля.
7.Описати схему формування цифрового підпису з вживання алгоритму RSA.
8.Описати схему перевірки цифрового підпису вживання алгоритму RSA.
9.Що загального між звичайним і цифровим підписами? Чим вони розрізняються?
10.Які завдання дозволяє вирішити цифровий підпис?
11.У чому полягає принципова складність в практичному вживанні систем цифрового підпису?
12.Чому в криптографічних системах, заснованих на відкритих ключах, не можна використовувати для шифрування і цифрового підпису?
13.Перевірити, що вказаний в тексті спосіб підбору підписаних повідомлень для схеми Ель-Гамаля дійсно дає вірні цифрові підписи.

Лабораторна робота 5

Програмна реалізація криптографічних протоколів

Мета роботи – ознайомиться з криптографічними протоколами, які в даний час широко використовуються для забезпечення інформаційної безпеки. Освоїти основні поняття, які пов'язані з криптографічними протоколами.

Завдання до роботи

Реалізувати два прості протоколи. Протокол Діффі-Хелмана формування загального ключа і протокол підкидання монети. Підготувати звіт. У звіті дати алгоритми протоколів і описати їх програмні реалізації. Підготувати для демонстрації учбові варіанти контрольних прикладів, які моделюють роботу з використанням криптографічних протоколів.

Теоретичний матеріал

Схема Діффі-Хеллмана

Протокол формування загального ключа по відкритому каналу зв'язку

1. Є два користувачі (абонента) A і B.
2. Дано просте число p, яке відоме користувачам A і B.
3. Вибирається загальне число g, g < p-1.
4. Абоненти A і B незалежно один від одного вибирають відповідно секретні ключі a, 0 < a < p-1 і b, 0 < b < p-1.
5. Абонент A посилає абонентові B повідомлення

$$g^a mod\ p.$$

6. Абонент B посилає абонентові A повідомлення

$$g^b mod\ p.$$

7. Абонент A обчислює загальний ключ

$$g^a mod\ p.$$

8. Абонент В обчислює загальний ключ

$$g^b mod\ p.$$

Протокол взаємної аутентифікації

Існує декілька схем аутентифікації джерела даних ([1],[7]).Приведемо умови і алгоритм реалізації однієї з них.

1. Дано двох абонентів А і В.

2. Дани просте число p і число g, $g<p-1$, які відомі абонентам A *і* B.

3. Абоненти А і В володіють відповідно відкритими функціями шифруваннz E_a і E_b і закритими функціями де шифрування D_a і D_b, які володіють властивостями

$$D_a E_a(M) = M,\ D_b E_b(M) = M,$$

де М-код –передаване повідомлення. Відзначимо, що рівність не залежить від порядку вживання функцій.

4. Абоненти А і В незалежно один від одного вибирають відповідно секретні ключі a, 0 < a < p-1 і b, 0 < b < p-1.

5. Абонент А посилає абонентові В повідомлення

$$g^a mod\ p.$$

6. Абонент В

• обчислює загальний ключ

$$K \equiv [g^a]^b \mathrm{mod}\ p;$$

• використовуючи закриту функцію D_b, створює підпис (повідомлення)

$$D_b(g^a \bmod p, g^b \bmod p);$$

• використовуючи ключ до, шифрує підпис

$$E_k(D_a(g^a \bmod p, g^b \bmod p))$$

де E_k загальна функція шифрування;

• відправляє абонентові А повідомлення

$$g^b \bmod p, E_k(D_a(g^a \bmod p, g^b \bmod p))$$

7. Абонент А

• обчислює загальний ключ

$$K \equiv [g^a]^b \bmod p;$$

• використовуючи закриту функцію DA, створює підпис (повідомлення)

$$D_a(g^a \bmod p, g^b \bmod p);$$

• використовуючи ключ до, шифрує підпис

$$E_k(D_a(g^a \bmod p, g^b \bmod p));$$

• відправляє абонентові В повідомлення

$$E_k(D_a(g^a \bmod p, g^b \bmod p)$$

• перевіряє підпис В, обчислюючи

$$E_b(D_k(E_k(D_b(g^a \bmod p, g^b \bmod p)))) = (g^a \bmod p, g^b \bmod p)$$

де D_k - загальна функція дешифровки.

8. Абонент В перевіряє підпис А, обчислюючи

$$E_a(D_k(E_k(D_a(g^a \bmod p, g^b \bmod p)))) = (g^a \bmod p, g^b \bmod p).$$

Контрольні питання

1.Дати визначення протоколу.

2.Перерахувати завдання захисту інформації, в яких використовуються криптографічні протоколи.

3.Способи класифікації криптографічних протоколів.

4.Класифікація криптографічних протоколів за функціональним призначенням.

5.Призначення протоколу аутентифікації повідомлень.

6.Призначення протоколу ідентифікації.

7.Призначення протоколу обміну секретами.

8.Перерахувати основні види атак на протоколи.

Лабораторна робота 6

Обчислення найбільшого загального дільника для двох чисел за допомогою алгоритму Евкліда

Цель роботи – використовуючи алгоритм Евкліда створити програму, яка для чисел a і b визначає найбільшого загального дільника.

Завдання до роботи

У програмній реалізації алгоритму Евкліда має бути розроблений інтерфейс, зручний для експлуатації. У інтерфейсі слід передбачити:

• введення початкової інформації з сформованого заздалегідь файлу, і файлу, який створюється в оболонці програми;

• введення початкової інформації з клавіатури.

Підготувати звіт по роботі. У звіті описати алгоритм Евкліда, описати структуру представлення даних в програмі, основні функції програми, призначення функцій, вхідні і вихідні параметри функцій.

Теоретичний матеріал

Прості числа Натуральне число p, більше одиниці називається простим, якщо воно ділиться без остачі лише на одиницю і на себе.

Теорема (Евклід). Безліч простих чисел безкінечна.

Позначимо через $\neq x$ функцію, яка дорівнює числу простих чисел p в інтервалі $1 < x"\ p$. Російський математик П.Л. Чебишев в 1850г. показав, що має місце

$$0.921\frac{x}{\ln x} <\neq (x) < 1.106\frac{x}{\ln\ x}.$$

Прості числа є важливим поняттям в криптографії. Багато сучасних криптографічних систем будуються на базі простого числа. Тому алгоритми генерації простих чисел і

перевірки на простоту сформованого числа в даний час є важливими інструментами при створенні криптографічної системи.

Відмітимо, що існує близько 10151 простого числа завдовжки від 1 до 512 біт включно [5]. Для чисел, близьких n, вірогідність довільно вибраному числу виявитися простим числом, рівна (*1 / ln n*). При випадковому виборі двох простих чисел в діапазоні від 1 до 151 бита вірогідність збігу цих чисел нікчемно мала.

Хай дано два цілі числа a і b. Говорять, що число a ділить *b,* якщо існує таке ціле число *d,* що *b=ad.* Число a в цьому випадку називають дільником *b.* Для факту, що a ділить b, прийнято позначення a|b. Справедливі наступні властивості подільності*:*

- якщо *a|b i c* – будь-яке число, то *a|(bc)*;
- якщо *a|b i b|c*, то *a|c*;
- якщо *a|b i a|c*, то *a|(b ± з).*

Тут доречно зробити зауваження, що важливу роль в арифметиці цілих чисел має теорема про ділення.

Теорема про ділення. Для будь-якого цілих чисел *a* і *b, b > 0*, існують, і притому єдині, цілі числа *q* і *r*, такі, що

$$a = bq + r,\ 0" \quad r < b.$$

Визначення. Натуральне число *p, p > 1*, називається складеним, якщо число p має принаймні одного позитивного дільника, відмінного від одиниці і *p*. Якщо число *p* складене, то справедлива наступна теорема.

Теорема. Для будь-якого складеного числа найменший відмінний від одиниці позитивний дільник є простим числом. Одним з основних затверджень арифметики є факт, що будь-яке натуральне число *p* можна єдиним чином представити у вигляді твору простих чисел.Наприклад,

*4290 = 3*2*5*11*13,*

В загальному випадку канонічним розкладанням цілого числа а називається вистава у вигляді

$$a = {p_1}^{a1}, {p_2}^{a2}, \dots, {p_k}^{ak},$$

де

$p_i, \quad i = 1,2, \dots \dots, k$ – прості числа. Наприклад, *133100 = 2252113.*

Відмітимо, що, взагалі кажучи, представлення великого числа в канонічному записі, тобто у вигляді твору простих співмножників є важкою і дуже важливим завданням в криптографії.

Визначення. Загальним дільником цілих чисел

$$a_1, a_2, \dots\dots, a_k$$

називається будь-яке ціле число d, таке, що

$$d|a_1, d|a_2, \dots\dots d|a_k.$$

Визначення. Найбільшим загальним дільником (НОД) цілих чисел $a_1, a_2, \dots\dots, a_k$ називається такий позитивний загальний дільник цих чиселякий ділиться на будь-якого іншого дільника цих чисел.

Якщо d – найбільший загальний дільник для чисел a і b, то для нього вводиться позначення $(a, b) = d$.

Теорема. Якщо натуральне число p не ділиться ні на одне просте число

$$d"\sqrt{p},,$$

то число p – просте.

Визначення. Числа $a_1, a_2, \dots\dots, a_k$ називаються взаємно простими, якщо найбільший загальний дільник цих чисел дорівнює 1.

Визначення. Числа $a_{1,}a_2, \ldots\ldots, a_k$ називаються попарно взаємно простими, якщо

$$(a_i, a_j) = 1,\ i \uparrow j,\quad 1i''k\ ,\ 1''j''.$$

Якщо числа попарно взаємно прості, то всі вони взаємно прості.

Приклад.

Числа 15, 21, 77 – взаємно прості, але ці числа не є попарно взаємно простими, тому що (15, 21) = 3.

Числа 34, 53, 99, 115 – попарно взаємно прості числа.

Алгоритм Евкліда

Для двох цілих чисел a і b існує порівняно швидкий метод обчислення найбільший загальний дільник. Згаданий метод обчислення найбільший загальний дільник називається алгоритмом Евкліда. Приведемо схему роботи цього алгоритму.

1. Ділимо число a на число b, отримуємо

$$a = bq_0 + r_1;$$

2. Ділимо число b на число $r1$, маємо

$$b = r_1 q_1 + r_2;$$

3. Ділимо число r_1 на число r_2, запишемо

$$r_1 = r_2 q_2 + r_3;$$

4. Ділимо число r_2 на число r_3, отримуємо

$$r_2 = r_3 q_3 + r_4;\ .;$$

$$\ldots\ldots;$$

$$r_{t-1} = r_1 q_t + r_{t+1}.$$

Якщо залишок від ділення $r_{t+1} = 0$, то в цьому випадку найбільший загальний дільник дорівнює числу r_t і алгоритм обчислення найбільший загальний дільник завершується.

Коротко алгоритм Евкліда можна сформулювати таким чином. Дано два цілі числа *a і b*. Для визначеності передбачимо, що *a > b*. Для пошуку найбільшого загального дільника слід виконати наступні операції.

1. Розділити *a* на *b*. Хай залишок рівний

$$r,\ 0 < r" a.$$

2. Якщо $r = 0$, то алгоритм завершується, найбільший загальний дільник рівний *b*.
3. Покладемо *a* = *b і b* = r.
4. Повертаємося на крок 1.

Приклад. Знайти найбільшого загального дільника чисел *a = 1173 і b = 323*.

1. Ділимо число *1173* на число *323*, отримуємо

$$1173 = 323*3 + 204;$$

2. Ділимо число *323* на число *204*, отримуємо

$$323 = 204*1 + 119;$$

3. Ділимо число *204* на число *119*, отримуємо

$$204 = 119*1 + 85;$$

4. Ділимо число *119* на число *85*, отримуємо

$$119 = 85*1 + 34;$$

5. Ділимо число *85* на число *34*, отримуємо

$$85 = 34*2 + 17;$$

6. Ділимо число *34* на число *17,* отримуємо

$$34 = 17*23 + 0;$$

Отже, у результаті отримуємо

$$(1173, 323) = 17.$$

Контрольні питання

1. Дати визначення простого числа.
2. Дати визначення складеного числа.
3. Сформулювати алгоритм Евкліда.
4. Дати визначення найбільшого загального дільника.
5. Сформулювати теорему про ділення двох цілих чисел.

Лабораторна робота 7

Розширений алгоритм Евкліда

Мета роботи. Нехай число d - найбільший загальний дільник для цілихчисел a і b. Використовуючи розширений алгоритм Евкліда, створити програмудля визначення таких двох чисел x і y, для яких виконується рівність

$$d = ax + by.$$

Завдання до роботи

У програмнійреалізаціїрозширеного алгоритму Евклідаповинен бути розробленийінтерфейс, зручнийдляексплуатаціївінтерфейсіпередбачити:

• введенняпочатковоїінформації з сформованогозаздалегідь файлу, і файла, якийстворюється в оболонціпрограми;

• введенняпочатковоїінформації з клавіатури.

Підготуватизвіт по роботі. У звітіописати алгоритм Евкліда, описати

структуру представленняданих в програмі, основніфункціїпрограми, призначенняфункцій, вхідні і вихідніпараметрифункцій.

$$d = ax + by.$$

Іншими словами найбільшийспільнийдільникдвох чисел можна подати у

вигляділінійноїкомбінаціїцих чисел з цілимикоефіцієнтами.

Схема розширеного алгоритму Евкліда

1. Визначити

$$a_0 = 1,\ a_1 = 0,\ b_0 = 0,$$

$$b_1 = 1,\ \alpha = \text{a},\ \beta = \text{b}.$$

2. Нехай число q - часткавідділення числа a на число b, а число r -

залишоквідділенняцих чисел, тобто

$$a = qb + r.$$

3. Якщозалишоквідділення r дорівнює нулю, то виконуємокрок 6.
4. Визначаємо

$$a = b,\ b = r,\ t = a_0,\ a_0 = a_1,$$
$$a_1 = t - a_1 q,\ t = b_0,\ b_0 = b_1;$$
$$b_1 = t - b_1 q;$$

5. Повертаємося на крок 2.
6. Визначаємо

$$x = x_0,\ y = y_0 d = \alpha x + \beta y.$$

Наприклад. Дано a = 1769, b = 551. Використовуючи розширений алгоритм Евкліда, знайти цілі числа x і y такі, що

$$d = ax + by,$$

де d - найбільший спільний дільник чисел a і b.

І етап послідовності обчислень

1. Визначити

$$a_0 = 1,\ a_1 = 0,\ b_0 = 0,\ b_1 = 1,$$
$$\alpha = 1769,\ \beta = 551.$$

2. Частка від ділення

$$q = a/b = 1769/551 = 3,$$

а залишок від ділення r = 116.

3. Якщо залишок від ділення r дорівнює нулю, то виконуємо крок 6.
4. Визначаємо

$$a = 551,\ b = 116,\ t = a_0 = 1,\ a_0 = a_1 = 0,$$
$$a_1 = t - a_1 q = 1 - 0 \cdot 3 = 1$$
$$t = b_0 = 0,\ b_0 = b_1 = 1,\ b_1 = t - b_1 q = -3;$$

В результаті поточного кроку отримали наступні проміжні значення параметрів

$$a = 551,\ b = 116,\ a_0 = 0,$$
$$a_1 = 1,\ b_0 = 1,\ b_1 = -3.$$

5. Так як залишок від ділення r ≠ 0, то повертаємося на крок 2.

ІІ етап послідовності обчислень

1. значення параметрів

$$a = 551,\ b = 116,\ a_0 = 0,$$
$$a_1 = 1,\ b_0 = 1,\ b_1 = -3.$$

2. Частка від ділення

$$q = a/b = 551/116 = 4,$$

а залишок від ділення r = 87.

3. Якщо залишок від ділення r дорівнює нулю, то виконуємо крок 6.
4. визначаємо

$$a = 116, \quad b = 87, \quad t = a_0 = 0, \quad a_0 = a_1 = 1,$$
$$a_1 = t - a_1 q = 0 - 1 \cdot 4 = -4,$$
$$t = b_0 = 1, \quad b_0 = b_1 = -3,$$
$$b_1 = t - b_1 q = 1 - (-3) \cdot 4 = 13.$$

В результаті поточного кроку отримали наступні проміжні значення Параметрів

$$a = 116, \; b = 87, \; a_0 = 1,$$
$$a_1 = -4, \; b_0 = -3, \; b_1 = 13.$$

5. Так як залишок від ділення $r \neq 0$, то повертаємося на крок 2.

III етап послідовності обчислень

1. Значення параметрів

$$a = 116, \; b = 87, \; a_0 = 1,$$

$$a_1 = -4, \; b_0 = -3, \; b_1 = 13.$$

2. Частка від ділення $q = a / b = 116/87 = 1$, а залишок від ділення $r = 29$.

3. Якщо залишок від ділення r дорівнює нулю, то виконуємо крок 6.

4. визначаємо

$$a = 87, \quad b = 29, \quad t = a_0 = 1, \quad a_0 = a_1 = -4,$$

$$a_1 = t - a_1 q = 1 - (-4) \cdot 1 = 5;$$

$$t = b_0 = -3, \quad b_0 = b_1 = 13;$$

$$b_1 = t - b_1 q = -3 - (13) \cdot 1 = -16.$$

В результаті поточного кроку отримали наступні проміжні значення

Параметрів

$$a = 87, \; b = 29, \; a_0 = -4,$$

$$a_1 = 5, \; b_0 = 13, \; b_1 = -16.$$

5. Так як залишок від ділення $r \neq 0$, то повертаємося на крок 2.

IV етап послідовності обчислень

1. значення параметрів

$$a = 87, \; b = 29, \; a_0 = -4, \quad a_1 = 5,$$
$$b_0 = 13, \; b_1 = -16.$$

2. Частка від ділення $q = a / b = 87/29 = 3$, а залишок від ділення $r = 0$.

3. Якщо залишок від ділення r дорівнює нулю, то виконуємо крок 6.
4. визначаємо

$$a = 87, \quad b = 29, \quad t = a_0 = -4, \quad a_0 = a_1 = 5,$$
$$a_1 = t - a_1 q = -4 - 5 \cdot 3 = -19,$$
$$t = b_0 = 13, \quad b_0 = b_1 = -16,$$
$$b_1 = t - b_1 q = 13 - (-16) \cdot 3 = 61.$$

В результаті поточного кроку отримали наступні проміжні значення Параметрів

$$a = 87, \ b = 29, \ a_0 = 5,$$
$$1 = -19, \ b_0 = -16, \ b_1 = 61.$$

5. Так як залишок від ділення $r = 0$, то виконуємо крок 6.
6. Обчислюємо найбільший спільний дільник за формулою

$$d = \alpha x + \beta y,$$

де

$$x = x_0 = 5, \ y = y_0 = -16,$$
$$\alpha = 1769, \ \beta = 551.$$

Підставляючи значення параметрів, отримуємо

$$d = \alpha x + \beta y = 1769*5 - 551*16 =$$
$$= 8845 - 8816 = 29.$$

Лабораторна робота № 8

Скласти програму генерування простих чисел

Мета роботи : використовуючи решето Ератосфена створити програму побудови простих чисел, які не перевершують деякого заданогочисла N.

Завдання до роботи

У програмній реалізації решета Ератосфена повинен бути розроблений інтерфейс, зручний для експлуатації в інтерфейсіпередбачити:

- введення початкової інформації з сформованого заздалегідь файлу і файла, який створюється в оболонці програми;
- введення початкової інформації з клавіатури.

Підготувати звіт по роботі. У звіті описати алгоритм Ератосфена,описати структуру представлення даних в програмі, основні функціїпрограми,призначення функцій, вхідні і вихідні параметри функцій.

Теоретичний матеріал

Решето Ератосфена

Для складання таблиці всіх простих чисел, які не перевершують заданого числа N, треба з таблиці чисел 2, 3, ..., N викреслити всі числа,які діляться на два, крім 2. Потім викреслити всі числа, якіділяться на три, окрім 3. Далі цей процес (залишити найменше ззалишилися простих і викреслювати все кратні цьому простому) продовжуємодо тих пір, поки чергове вбрання число не перевищить$\sqrt{N}$.

Даний метод дозволяє будувати безліч простих чисел, але віннезручний для перевірки простоти заданого числа.

Лабораторна робота 9

Скласти програму вирішення рівняння виду $ax \equiv b \bmod n$

Мета роботи: використовуючи розширений алгоритм Евкліда, скласти програми вирішення порівняння $ax \equiv b \bmod n$, де числа a і n взаємно прості.

Завдання до роботи

У програмній реалізації рішення порівняння

$$ax \equiv b \bmod n$$

повинен бути розроблений інтерфейс, зручний для експлуатації. В інтерфейсі слід передбачити:

- Введення початкової інформації з сформованого заздалегідь файлу і файлу, який створюється в оболонці програми;
- Введення початкової інформації з клавіатури.

Розробити тестові приклади для програми. Підготувати звіт по роботі. У звіті описати алгоритм рішення порівняння

$$ax \equiv b \bmod n,$$

описати структуру представлення даних в програмі, основні функції програми, призначення функцій, вхідні і вихідні параметри функцій.

Теоретичний матеріал

Наприклад. Вирішити рівняння

$$37x \equiv 5 \bmod 1940,$$

де $a = 37$, $b = 5$, модуль $n = 1940$.

Спочатку вирішимо рівняння

$$37x \equiv 1 \bmod 1940,$$

Тобто визначимо елемент 37^{-1}, обернений до елемента $a = 37$. Для вирішення цього рівняння використовується розширений алгоритм Евкліда.

1. Визначаємо параметри

$$U_0 = 0,\ U_1 = 1,\ U_2 = 1490,$$

$$V_0 = 1,\ V_1 = 0,\ V_2 = 37.$$

2. Обчислюємо часткове q_1 і залишокr_2відділення модуля порівняння

$U_2 = 1940$ на число $V_2 = 37$. Отримуємо$q_1 = 52$, а залишок$r_2 = 16$. Тоді, за визначенням маємо

$$t_0 = U_0 - V_0 \times q_1 = 0 - 1 \times 52 = -52,$$

$$U_0 = V_0,\ V_0 = t_0,$$

$$t_1 = U_1 - V_1 \times q_1 = 1 - 0 \times 52 = 1,$$

$$U_1 = V_1,\ V_1 = t_1,$$

$$t_2 = U_3 - V_3 \times q_1 = r_2 = 16,$$

$$U_2 = V_2,\ V_2 = t_2.$$

Для другого кроку отримуємо наступні значення параметрів

$$U_0 = 1,\ U_1 = 0,\ U_2 = 37,$$

$$V_0 = -52,\ V_1 = 1,\ V_2 = 16.$$

3. Обчислюємо часткове q_2 і залишокr_3відділення модуля рівняння $U_2 = 37$ на число $V_2 = 16$. Отримуємо $q_2 = 2$, а залишок$r_3 = 5$. Тоді, за визначенням

$$t_0 = U_0 - V_0 \times q_2 = 1 - (-52) \times 2 = 105,$$

$$U_0 = V_0,\ V_0 = t_0,$$

$$t_1 = U_1 - V_1 \times q_2 = 0 - 1 \times 2 = -2,$$

$$U_1 = V_1,\ V_1 = t_1,$$

$$t_2 = U_3 - V_3 \times q_2 = r_3 = 5,$$

$$U_2 = V_2,\ V_2 = t_2.$$

Для третього кроку отримуємо наступні значення параметрів

$$U_0 = -52,\ U_1 = 1,\ U_2 = 16,$$

$$V_0 = 105,\ V_1 = -2,\ V_2 = 5.$$

4. Обчислюємо часткове q_3 і залишок r_4 відділення модуля рівняння $U_2 = 16$ на число $V_2 = 5$. Отримуємо $q_3 = 3$, а залишок $r_4 = 1$. Тоді, за визначенням маємо

$$t_0 = U_0 - V_0 \times q_3 = -52 - (105) \times 3 = -367,$$

$$U0 = V0, \quad V0 = t0,$$

$$t_1 = U_1 - V_1 \times q_3 = 1 - (-2) \times 3 = 7,$$

$$U_1 = V_1, V_1 = t_1,$$

$$t_2 = U_3 - V_3 \times q_3 = r_4 = 1,$$

$$U_2 = V_2, V_2 = t_2.$$

Для четвертого кроку отримуємо наступні значення параметрів

$$U_0 = 105, U_1 = -2, U_2 = 5,$$

$$V_0 = -367, V_1 = 7, V_2 = 1.$$

5. Обчислюємо часткове q_4 і залишок r_5 відділення модуля порівняння U_2=5на число $V_2 = 1$. Отримуємо $q_4 = 5$, а залишок $r_5 = 0$. Тоді, за визначенням маємо

$$t_0 = U_0 - V_0 \times q_4 = 105 - (-367) \times 5 = 1940,$$

$$U_0 = V_0, V_0 = t_0,$$

$$t_1 = U_1 - V_1 \times q_4 = -2 - 7 \times 5 = -37,$$

$$U_1 = V_1, V_1 = t_1,$$

$$t_2 = U_3 - V_3 \times q_4 = r_4 = 0,$$

$$U_2 = V_2, V_2 = t_2.$$

Для п'ятого кроку отримуємо наступні значення параметрів

$$U_0 = -367, U_1 = 7, U_2 = 1,$$

$$V_0 = 1940, V_1 = -37, V_2 = 0,$$

Алгоритм завершується тому $U_2 = 1$. Рішення даного рівняння має вигляд

$$x \equiv 37^{-1} mod\ 1940 \equiv (-367 + 1940)\ mod\ 1940 \equiv$$

$$\equiv 1573\ mod\ 1940,$$

тобто

$$x \equiv 1573\ mod\ 1940.$$

Перевірка рішення рівняння $37x \equiv 1\ mod\ 1940$:

$$37x \equiv 37 \times 1573 \; mod \; 1940 \equiv 58201 \; mod \; 1940 \equiv$$

$$(1 + 30 \times 1940) \; mod \; 1940 \equiv 1 \; mod \; 1940.$$

Задача рішення рівняння $37x \equiv 1 \; mod \; 1940$ завершена.

Після рішення порівняння $37x \equiv 1 \; mod 1940$, можна записати рішення рівняння $37x \equiv 5 \; mod \; 1940$, яке визначається формулою:

$$x = 5x^{-1} mod \; 1940,$$

де x^{-1} є рішення рівняння $37x \equiv 1 \; mod 1940$. Остаточно отримуємо,що значення

$$x \equiv 5x^{-1} mod \; 1940 \equiv 5 \times 1573 \; mod \; 1940 \equiv 7865 \; mod \; 1940 \equiv 105 \; mod \; 1940$$

є рішення рівняння $37x \equiv 1 mod \; 1940$.

Перевірка. Підставляємо значення $x = 105$ у рівняння $37x \equiv 5 \; mod \; 1940$,

отримуємо:

$$37 \times 105 \equiv 3885 \; mod \; 1940 \equiv (5 + 2 \times 1940) \; mod \; 1940 \equiv 5 \; mod \; 1940,$$

що доводить справедливість знайденого рішення.