Лабораториялық жұмыс нұсқаулығы
"Сәби адымы - Алып адымы алгоритмі" қолданбасымен жұмыс істеу

1. Жұмыс тақырыбы
Дискретті логарифм есебін шешу - Baby-Step Giant-Step (BSGS) алгоритмі

2. Жұмыс мақсаты
- Дискретті логарифм есебінің маңыздылығын түсіну
- BSGS алгоритмінің жұмыс принципін үйрену
- Алгоритмнің қадамдарын практикалық қолдану
- Модульдік арифметиканы қолдану дағдыларын дамыту

3. Қажетті құрал-жабдықтар
- Компьютер
- Интернет браузері (Chrome, Firefox, Edge)
- "Сәби адымы - Алып адымы алгоритмі" қолданбасы

4. Теориялық негіздер
4.1. Дискретті логарифм есебі
Дискретті логарифм мына теңдеуді шешу есебі:
text
a^x ≡ b (mod p)
мұндағы:
- a - база
- b - нәтиже
- p - жай сан (модуль)
- x - ізделінді дәреже

4.2. BSGS алгоритмінің идеясы
Алгоритм O(√p) уақыт пен жад күрделілігінде жұмыс істейді:
1. m = ⌈√p⌉ есептеу
2. Кіші қадамдар (baby steps): a^j mod p, j = 0...m-1
3. Үлкен қадамдар (giant steps): b·(a^(-m))^i mod p, i = 0...m-1
4. Сәйкестік табу: a^j ≡ b·(a^(-m))^i (mod p)
5. Шешім: x = i·m + j

5. Жұмыс барысы
5.1. Алғышарттарды дайындау
1. Браузерді ашыңыз
2. index.html файлын ашыңыз
3. Интерфейсті қазақ тілінде орнатыңыз

5.2. Тәжірибелік тапсырмалар
Тапсырма 1: Мысалды талдау
1. "Мысалды іске қосу" түймесін басыңыз
2. Алгоритм қадамдарын мұқият оқыңыз
3. Әрбір қадамды түсіндіріңіз

Тапсырма 2: Жеңіл есептер
1. Параметрлерді өзгертіңіз:
    - a = 3, p = 17, b = 5
    - a = 2, p = 23, b = 9

- a = 5, p = 29, b = 7

2. Әрбір жағдай үшін шешімді табыңыз
3. Нәтижені тексеріңіз

Тапсырма 3: Орташа күрделіліктегі есептер

1. Параметрлерді өзгертіңіз:
   - a = 2, p = 101, b = 13
   - a = 3, p = 103, b = 17
   - a = 7, p = 107, b = 23
2. Алгоритм қадамдарын салыстырыңыз
3. Есептеу уақытын бағалаңыз

Тапсырма 4: Күрделі есептер

1. Параметрлерді өзгертіңіз:
   - a = 2, p = 211, b = 37
   - a = 5, p = 307, b = 53
2. Шешім табылғанша күтіңіз
3. Память және уақыт күрделілігін талдаңыз

Тапсырма 5: Өз есептеріңіз

1. Өз параметрлеріңізді құрастырыңыз
2. Есепті шешіңіз
3. Нәтижені қолмен тексеріңіз

6. Есептер мен талдау

6.1. Бақылау сұрақтары:

1. BSGS алгоритмі неліктен "сәби адымы - алып адымы" деп аталады?
2. Алгоритмде m = ⌈√p⌉ не үшін есептеледі?
3. Кері элемент қалай есептеледі және не үшін қажет?
4. Алгоритмнің ең нашар жағдайдағы күрделілігі қандай?
5. Қандай жағдайларда алгоритм шешім таба алмайды?

6.2. Есептер:

1. Кесте толтырыңыз:

№	a	p	b	m	x	Тексеру (a^x mod p)	Уақыт (ms)
1	2	101	5	11	28	5	
2	3	17	5	5			
3	2	23	9	5			
4	5	29	7	6			
5	2	211	37	15			

2. Өз параметрлеріңізбен жұмыс жасап, кестені толтырыңыз

7. Бақылау және өлшеу

7.1. Алгоритмнің орындалу уақыты:

1. Әрбір есеп үшін орындалу уақытын өлшеңіз

2. p модулі үлкейген сайын уақыт қалай өзгереді?
3. Эксперименттік деректерді графикаға түсіріңіз

7.2. Жад пайдалануы:

1. Алгоритм қанша жад пайдаланады?
2. Baby steps жадта қалай сақталады?
3. Модуль үлкейген сайын жад қажеттілігі қалай өзгереді?

8. Қорытынды жасау

Төмендегі тармақтар бойынша қорытынды жазыңыз:

8.1. Алгоритмнің тиімділігі:

- Уақыт күрделілігі
- Жад күрделілігі
- Практикалық қолдану мүмкіндіктері

8.2. Артықшылықтары мен кемшіліктері:

Артықшылықтары:

- Brute force әдісінен тезірек
- Анық алгоритм
- Кіші модульдер үшін тиімді

Кемшіліктері:

- Үлкен модульдер үшін жад көп қажет
- Тек дискретті логарифм үшін ғана
- Толық автоматтандырылмаған

8.3. Қолдану салалары:

- Криптография (Diffie-Hellman, ElGamal)
- Сандық қолтаңбалар
- Публикалық кілттік криптожүйелер

8.4. Қиындықтар және шешу жолдары:

- Жад шектеулері
- Есептеу уақыты
- Дәлдік мәселелері

9. Өздік жұмыс тапсырмалары

9.1. Зерттеу тапсырмалары:

1. BSGS алгоритмін басқа тілде (Python, C++) іске асырыңыз
2. Әртүрлі модуль мәндерімен жұмыс жасаңыз
3. Алгоритмнің параллель нұсқасын ойлап табыңыз

9.2. Шығармашылық тапсырмалар:

1. Алгоритмге графикалық интерфейс қосыңыз
2. Есептеу процесін анимациялаңыз
3. Өлшемдерді салыстыру үшін графиктер құрыңыз

10. Қауіпсіздік ережелері

1. Программалық кодты тексеруден өткізіңіз
2. Жүйелік ресурстарды тиімді пайдаланыңыз
3. Есептеу процесін бақылаңыз

11. Әдебиеттер тізімі

1. Кнут Д. "Компьютерлік алгоритмдер өнері"

2. Menezes A., van Oorschot P., Vanstone S. "Handbook of Applied Cryptography"
3. Смаллиан Р. "Алгоритмдер теориясы негіздері"

12. Бағалау критерийлері

Критерий	Ұпай	Сипаттама
Теорияны меңгеру	25	Алгоритм принципін түсіну
Практикалық жұмыс	25	Тапсырмаларды орындау
Талдау және есептер	25	Нәтижелерді талдау
Қорытынды	15	Дұрыс қорытынды жасау
Әдептілік	10	Жұмыстың өздігіндігі

Ескерту: Бұл нұсқаулық студенттерге BSGS алгоритмін практикалық түрде үйренуге арналған. Әрбір тапсырманы орындағаннан кейін нәтижелерді тіркеп, талдау жасау қажет. Жұмысты орындау барысында мұғалімнен көмек сұрауға болады.