ӘДІСТЕМЕЛІК НҰСҚАУЛЫҚ
"Алгебралық криптоталдау" веб-қосымшасымен жұмыс істеу

1. ЖҰМЫС ТАҚЫРЫБЫ
Алгебралық криптоталдау әдістерін оқу шифры арқылы үйрену

2. ЖҰМЫС МАҚСАТЫ
- Алгебралық криптоталдаудың негізгі принциптерін түсіну
- Блокты шифрдың алгебралық моделін құруды үйрену
- Теңдеулер жүйесін шешу әдістерін меңгеру
- Криптоталдаудағы математикалық аппаратты қолдану дағдыларын дамыту

3. ҚАЖЕТТІ ҚҰРАЛ-ЖАБДЫҚТАР
- Компьютер
- Интернет браузері (Chrome, Firefox, Edge, Safari)
- "Алгебралық криптоталдау" веб-қосымшасы (index.html файлы)

4. ТЕОРИЯЛЫҚ НЕГІЗДЕР
4.1. Алгебралық криптоталдау
Алгебралық криптоталдау - криптографиялық алгоритмдерді сыну үшін оларды алгебралық теңдеулер жүйесіне түрлендіру әдісі.

4.2. Оқу шифры параметрлері
- **Блок өлшемі**: 8 бит
- **Кілт өлшемі**: 8 бит
- **Раунд саны**: 2
- **Құрылым**: Фейстель желісі
- **S-блоктар**: 4×4 (екеу)
- **P-блок**: Битерді ауыстыру

4.3. Негізгі ұғымдар
- **S-блок (Ауыстыру блокы)**: Енгізу биттерін шығыс биттеріне түрлендіреді
- **P-блок (Ауыстыру блокы)**: Битердің орнын ауыстырады
- **XOR операциясы**: Екілік қосу модулі 2 бойынша
- **Фейстель желісі**: Симметриялық шифр құрылымы

5. ЖҰМЫС БАРЫСЫ
5.1. Алғышарттарды дайындау
1. Браузерді ашыңыз
2. index.html файлын ашыңыз
3. Интерфейс тілін қазақшаға орнатыңыз (ҚАЗ түймесі)

5.2. БІРІНШІ САБАҚ: Шифр параметрлерімен танысу
Тапсырма 1: Параметрлерді зерттеу
1. "Шифр параметрлері" жолағын таңдаңыз
2. S-блоктардың алгебралық формулаларын оқыңыз
3. P-блок ауыстыруын талдаңыз
4. Раунд санын өзгертіп көріңіз

Тапсырма 2: Параметрлерді өзгерту
1. S-блоктардың формулаларын өзгертіңіз

2. P-блок ауыстыруын басқаша орнатыңыз
3. "Параметрлерді жаңарту" түймесін басыңыз
4. Өзгерістердің әсерін бақылаңыз

Тапсырма 3: Әдепкі параметрлерге қайту

1. "Әдепкі параметрлер" түймесін басыңыз
2. Бастапқы күйге қайтарылғанын тексеріңіз

5.3. ЕКІНШІ САБАҚ: Алгебралық теңдеулерді құру

Тапсырма 1: Белгілі жұптарды енгізу

1. "Алгебралық теңдеулер" жолағына өтіңіз
2. Ашық мәтін ретінде "00000010" енгізіңіз
3. Шифрмәтін ретінде "00001101" енгізіңіз

Тапсырма 2: Теңдеулер жүйесін құру

1. "Теңдеулер жүйесін құру" түймесін басыңыз
2. Құрылған теңдеулерді талдаңыз
3. Әрбір теңдеудің мағынасын түсіндіріңіз

Тапсырма 3: Әртүрлі кірістермен жұмыс

1. Әртүрлі ашық мәтіндер енгізіңіз
2. Әр жолы теңдеулер жүйесін қайта құрыңыз
3. Теңдеулердің қалай өзгеретінін бақылаңыз

5.4. ҮШІНШІ САБАҚ: Теңдеулер жүйесін шешу

Тапсырма 1: Шешу әдісін таңдау

1. "Теңдеулер жүйесін шешу" жолағына өтіңіз
2. Шешу әдісін таңдаңыз (сызықтық теңдеулер)
3. "Теңдеулер жүйесін шешу" түймесін басыңыз

Тапсырма 2: Теңдеулерді жеңілдету

1. "Теңдеулерді жеңілдету" түймесін басыңыз
2. Жеңілдетілген теңдеулерді салыстырыңыз
3. Еркін айнымалыларды анықтаңыз

Тапсырма 3: Шешімдерді тексеру

1. "Шешімді тексеру" түймесін басыңыз
2. Табылған кілттердің дұрыстығын бағалаңыз
3. Кестедегі нәтижелерді талдаңыз

5.5. ТӘРТІНШІ САБАҚ: Тәжірибелік мысалдар

Тапсырма 1: Толық мысалды орындау

1. "Тәжірибелік мысал" жолағына өтіңіз
2. "Мысалды орындау" түймесін басыңіз
3. Барлық қадамдардың автоматты түрде орындалуын бақылаңыз

Тапсырма 2: Қадам-қадам талдау

1. "Қадам-қадам орындау" түймесін басыңыз
2. Әрбір қадамды мұқият оқыңыз
3. Әр қадамның мағынасын түсіндіріңіз

Тапсырма 3: Өз мысалыңызды жасау

1. Өз ашық мәтініңізді құрастырыңыз
2. Өз шифрмәтініңізді ойлап табыңыз
3. Толық талдау жасаңыз

6. ТӘЖІРИБЕЛІК ТАПСЫРМАЛАР

6.1. Деңгей 1: Негізгі дағдылар

1. Шифрдың жұмыс принципін сипаттаңыз
2. S-блоктардың әрекетін түсіндіріңіз
3. XOR операциясының рөлін анықтаңыз

6.2. Деңгей 2: Теңдеулерді құру

1. Берілген кіріс-шығыс жұбы үшін теңдеулер жүйесін құрыңыз
2. Теңдеулерді жеңілдетіңіз
3. Еркін айнымалыларды табыңыз

6.3. Деңгей 3: Кешенді талдау

1. Әртүрлі параметрлермен жұмыс жасаңыз
2. Әртүрлі шешу әдістерін салыстырыңыз
3. Өз криптожүйеңізді құрастырыңыз

7. ЕСЕПТЕР ЖӘНЕ ТАЛДАУ

7.1. Талдау сұрақтары:

1. Алгебралық криптоталдау қандай жағдайларда тиімді?
2. S-блоктардың қандай қасиеттері маңызды?
3. Фейстель желісінің қандай артықшылықтары бар?
4. Теңдеулер жүйесін шешудің қандай қиындықтары бар?

7.2. Есептер:

1. Берілген S-блок үшін алгебралық теңдеулерді жазыңыз
2. Теңдеулер жүйесін шешіп, кілтті табыңыз
3. Табылған кілттің дұрыстығын тексеріңіз

8. БАҚЫЛАУ ЖӘНЕ ӨЛШЕУ

8.1. Білім деңгейін бағалау:

Критерий	Баға	Сипаттама
Теорияны меңгеру	25	Алгоритм принциптерін түсіну
Практикалық дағдылар	30	Қосымшаны дұрыс пайдалану
Талдау қабілеті	25	Нәтижелерді талдап, қорытынды жасау
Шығармашылық	20	Өз мысалдарын құрастыру

8.2. Орындау уақыты:

- Әр тапсырма үшін орындау уақытын өлшеңіз
- Қиындық деңгейіне қарай уақытты талдаңыз
- Өз шеберлігіңіздің дамуын бақылаңыз

9. ҚОРЫТЫНДЫ ЖАСАУ

9.1. Негізгі қорытындылар:

- Алгебралық криптоталдау әдісінің тиімділігі
- Оқу шифрының артықшылықтары мен кемшіліктері
- Практикалық қолдану мүмкіндіктері

9.2. Ұсыныстар:

- Қандай тақырыптарды тереңірек зерттеу керек
- Қандай қосымша функционал қажет
- Қалай жетілдіруге болады

10. ҚАУІПСІЗДІК ЕРЕЖЕЛЕРІ

1. Тек оқу мақсатында пайдаланыңыз
2. Заңсыз әрекеттерден аулақ болыңыз
3. Авторлық құқықты құрметтеңіз

11. ӘДЕБИЕТТЕР ТІЗІМІ

1. Криптография негіздері
2. Алгебралық әдістер
3. Блокты шифрлар теориясы
4. Компьютерлік қауіпсіздік

12. ҚОСЫМША РЕСУРСТАР

12.1. Онлайн курслар:

- Криптография негіздері (Coursera)
- Алгебралық криптоталдау (edX)
- Киберқауіпсіздік (Stepik)

12.2. Кітаптар:

- Шнайер Б. "Қолданбалы криптография"
- Фергюсон Н. "Криптография: практикалық нұсқаулық"
- Кнут Д. "Компьютерлік алгоритмдер өнері"

12.3. Бағдарламалық құралдар:

- SageMath (алгебралық есептеулер)
- Cryptool (криптографияны үйрену)
- MATLAB (математикалық модельдеу)

13. ЖҰМЫС ТӘРТІБІ

13.1. Дайындық кезеңі:

1. Теориялық материалдарды оқу
2. Қосымшаны іске қосу
3. Интерфейспен танысу

13.2. Практикалық жұмыс:

1. Әр сабақты орындау
2. Тапсырмаларды шешу
3. Нәтижелерді тіркеу

13.3. Талдау кезеңі:

1. Нәтижелерді талдау
2. Қорытынды жасау
3. Ұсыныстар әзірлеу

14. КҮТІЛЕТІН НӘТИЖЕЛЕР

14.1. Білім деңгейі:

- Алгебралық криптоталдау принциптерін түсіну
- Теңдеулер жүйесін шешу дағдылары
- Криптоталдау әдістерін қолдану қабілеті

14.2. Дағдылар:

- Веб-қосымшаны тиімді пайдалану

- Математикалық аппаратты қолдану
- Нәтижелерді талдау және қорытынды жасау

14.3. Шығармашылық:

- Өз мысалдарын құрастыру
- Проблемаларды шешу жолдарын ойлап табу
- Жаңа идеялар ұсыну

15. КЕРІ БАЙЛАНЫС

15.1. Өзін-өзі бағалау:

- Әр тапсырмадан кейін өз жұмысыңызды бағалаңыз
- Қиындықтарды анықтаңыз
- Жетілдіру жолдарын жоспарлаңыз

15.2. Мұғалімнен кері байланыс:

- Жұмыстың дұрыстығын тексерту
- Қиын сұрақтарға жауап алу
- Қосымша материалдар алу

15.3. Топтық талқылау:

- Нәтижелерді салыстыру
- Тәжірибелермен бөлісу
- Жаңа идеялар талқылау

ЕСКЕРТУ: Бұл нұсқаулық студенттерге "Алгебралық криптоталдау" веб-қосымшасымен тиімді жұмыс істеуге арналған. Әрбір сабақты орындағаннан кейін нәтижелерді тіркеп, өзін-өзі бағалау жасау қажет.

МАҢЫЗДЫ ТҮЙІНДЕМЕ:

- Барлық тапсырмаларды ретімен орындаңыз
- Әр қадамды мұқият түсініңіз
- Қиындық туындаған жағдайда мұғалімнен көмек сұраңыз
- Практикалық дағдыларды дамытуға назар аударыңыз