ЛАБОРАТОРИЯЛЫҚ ЖҰМЫС: DES-ТӘРІЗДІ ШИФРДЫ СЫЗЫҚТЫҚ ТАЛДАУ

1. ЖҰМЫСТЫҢ МАҚСАТЫ

DES-тәрізді шифрды сызықтық криптоталдау әдісімен бұзуды үйрену, сызықтық статистикалық теңдеулерді құру және кілт биттерін есептеу.

2. ҚАЖЕТТІ БАҒДАРЛАМАЛАР

1. **Веб-нұсқасы** (ұсынылады):
    - Кез келген заманауи браузер (Chrome, Firefox, Edge)
    - Интернет байланысы қажет емес
2. **Python нұсқасы** (альтернатива):
    - Python 3.8 немесе одан жоғары
    - Tkinter кітапханасы

3. ЖҰМЫСТЫҢ ЖҮРГІЗІЛУ ТӘРТІБІ

3.1 ВЕБ-ҚОЛДАНБАНЫ ҚОЛДАНУ

1-қадам: Қолданбаны іске қосу

- index.html файлын браузерде ашыңыз
- "Веб-қолданбаны іске қосу" батырмасын басыңыз
- Барлық функциялар las-des.html файлында ашылады

2-қадам: Шифр параметрлерін орнату

- "Баптаулар" қойындысына өтіңіз
- Келесі параметрлерді енгізіңіз:
    - **S-блоктар**: әрқайсысы 16 мәннен
    - **Кеңейту кестесі**: 12 сан (1-8 аралығында)
    - **Ауыстыру кестесі**: 8 сан (1-8 аралығында)
    - **Кілт**: 24 бит (0 және 1)

3-қадам: Параметрлерді сақтау

- "Параметрлерді сақтау" батырмасын басыңыз
- Барлық параметрлер браузердің жадында сақталады

3.2 S-БЛОКТАРДЫ ТАЛДАУ

1-қадам: Сызықтық кестені құру

- "S-блоктар талдауы" қойындысына өтіңыз
- Талданатын S-блокты таңдаңыз (S1, S2, S3)
- "Сызықтық кестені құру" батырмасын басыңыз

2-қадам: Кестені талдау

- Кестеде әрбір кіріс/шығыс маска жұбы үшін:
  - Болу саны (0-16 аралығында)
  - Ықтималдық (0-1 аралығында)
- Максималды ауытқуы бар жұптарды табыңыз (1/2-ден айтарлықтай өзгеше)

3.3 ШИФРЛЕУ/ДЕШИФРЛЕУ

1-қадам: Деректерді енгізу

- "Шифрлеу/Дешифрлеу" қойындысына өтіңіз
- 16 биттік кіріс деректерін енгізіңіз (тек 0 және 1)
- Раунд санын таңдаңыз (3 немесе 5)
- Операцияны таңдаңыз (шифрлеу немесе дешифрлеу)

2-қадам: Орындау және талдау

- "Орындау" батырмасын басыңыз
- Әр раундтың аралық нәтижелерін қараңыз
- Финальды нәтижені талдаңыз

3.4 СЫЗЫҚТЫҚ ТАЛДАУ

1-қадам: Теңдеулерді құру

- "Сызықтық талдау" қойындысына өтіңіз
- Кіріс блокты енгізіңіз (16 өрнек: X1-X16)
- Раунд кілтін енгізіңіз (12 өрнек: K1-K12)
- Шығыс айнымалыларды енгізіңіз (8 өрнек: C1-C8)
- Әр S-блок үшін маскаларды енгізіңіз

2-қадам: Теңдеулерді алу

- "Теңдеулерді құру" батырмасын басыңыз
- Автоматты түрде сызықтық теңдеулер генерацияланады
- Әр теңдеумен бірге оның ықтималдығы көрсетіледі

3-қадам: Теңдеулерді сақтау

- "Теңдеулерді сақтау" батырмасын басыңыз
- Теңдеулер `equations.txt` файлына жүктеледі

3.5 ТЕҢДЕУЛЕРДІ ТЕКСЕРУ

1-қадам: Тест параметрлерін орнату

- "Теңдеулерді тексеру" қойындысына өтіңіз
- Сынақ санын көрсетіңіз (100-10000)
- Раунд санын таңдаңыз (3 немесе 5)
- Маскаларды енгізіңіз (кіріс, шығыс, кілт)

2-қадам: Статистикалық тексеру
- "Тестті бастау" батырмасын басыңыз
- Кездейсоқ деректермен статистикалық тексеру жүргізіледі
- Теориялық және эксперименттік ықтималдықтар салыстырылады

3-қадам: Нәтижелерді сақтау
- "Нәтижелерді сақтау" батырмасын басыңыз
- Тест нәтижелері файлға жүктеледі

3.6 КІЛТ БИТТЕРІН ЕСЕПТЕУ

1-қадам: Теңдеулерді енгізу
- "Кілттерді есептеу" қойындысына өтіңіз
- Алынған сызықтық теңдеулерді енгізіңіз

2-қадам: Кілттерді шешу
- "Кілттерді шешу" батырмасын басыңыз
- Автоматты түрде кілт биттері есептеледі
- Шешім барысы көрсетіледі

3-қадам: Кілтті тексеру
- "Кілтті тексеру" батырмасын басыңыз
- Табылған кілт баптаулар қойындысына енгізіледі

4. ПРАКТИКАЛЫҚ ТАПСЫРМАЛАР

ТАПСЫРМА 1: Негізгі параметрлер
text
S1: 4,6,1,3,5,7,2,5,5,7,2,4,6,1,3,6
S2: 3,5,7,2,4,6,1,7,4,6,1,3,5,7,2,1
S3: 1,3,2,1,2,1,3,2,3,2,1,3,1,3,2,1
Кеңейту: 3 4 1 2 6 8 5 7 3 8 2 4
Ауыстыру: 4 6 8 1 3 5 7 2
Кілт: 010110011010011001011001

Тапсырмалар:
1. Параметрлерді енгізіп сақтаңыз
2. Әр S-блок үшін сызықтық кестені құрыңыз
3. Ықтималдығы 3/4 немесе 1/4 болатын маска жұптарын табыңыз

ТАПСЫРМА 2: Бірінші раунд теңдеулері
1. S1 блогы үшін мына маскаларды таңдаңыз: α=0101, β=010
2. Теңдеуді құрыңыз: X16 + K2 + X15 + K4 = C4 (p=3/4)
3. Теңдеудің дұрыстығын тексеріңіз (100 сынақ)

ТАПСЫРМА 3: Үш раундты шифр

1. 3 раундты шифрлеуді таңдаңыз
2. Мына теңдеуді тексеріңіз:
   X16+K2+X15+K4+Y16+K14+Y15+K16 = X4+Y4 (p=5/8)
3. 500 сынақ жүргізіп, эксперименттік ықтималдықты анықтаңыз

ТАПСЫРМА 4: Кілт биттерін есептеу

1. Мына теңдеулер жүйесін шешіңіз:

   text
   K1 + K13 = 0
   K3 + K15 = 1
   K5 + K17 = 1
   K8 + K20 = 0
   K9 + K21 = 1
   K10 + K22 = 1
   K2 + K4 + K14 + K16 = 0
   K2 + K3 + K4 + K14 + K15 + K16 = 1
2. Кілттің толық мәнін анықтаңыз
3. Табылған кілтпен шифрлеуді тексеріңіз

5. ЕСЕП БЕРУ ТӘРТІБІ

5.1 ЖҰМЫС ҚАҒАЗЫ (БАСҚАРМА)

1. **Жұмыстың аты, мақсаты**
2. **Қолданылған құрал-жабдықтар**
3. **Баптаулар**
4. **S-блоктар талдау нәтижелері**
5. **Теңдеулер (бір раундтық және көп раундтық)**
6. **Статистикалық тексеру нәтижелері**
7. **Кілт биттерінің шешімі**
8. **Қорытынды**

5.2 ЭЛЕКТРОНДЫҚ НҰСҚА

1. settings.json - сақталған параметрлер
2. equations.txt - алынған теңдеулер
3. test_results.txt - тексеру нәтижелері
4. key_solution.txt - кілт шешімі

6. ҚАУІПСІЗДІК ЕСКЕРТУЛЕРІ

1. ⚠ Бұл оқулық шифр ғана
2. ⚠ Нақты криптожүйелерде қолданбаңыз

3. ⚠ Кілттерді қауіпсіз жерде сақтаңыз
4. ⚠ Шифрлеу алгоритмдерін өзгертуді тек тәжірибе мақсатында жасаңыз

7. ӨЗІНДІК ЖҰМЫС ҮШІН СҰРАҚТАР

1. S-блоктарды өзгерткенде сызықтық сипаттамалары қалай өзгереді?
2. Раунд санын арттырғанда теңдеулердің ықтималдығы қалай өзгереді?
3. Қандай S-блоктардың сызықтық қорғанышы ең мықты?
4. Сызықтық талдау әдісінің артықшылықтары мен кемшіліктері қандай?
5. Бұл шифрды қалай жақсартуға болады?

8. ҚОСЫМША АҚПАРАТ

8.1 ҚЫСҚАША ТЕОРИЯ

Сызықтық криптоталдау - бұл сызықтық теңдеулерді пайдаланып шифрды бұзу әдісі. Негізгі идеясы:

1. Ашық мәтін, шифрмәтін және кілт арасында сызықтық қатынастарды табу
2. Бұл қатынастар ықтималдықпен орындалады (1/2-ден айырмашылығы бар)
3. Көптеген ашық/шифрмәтін жұптарын жинақтау арқылы кілт биттерін анықтау

Сызықтық жуықтау:
text
$P[\alpha \cdot X \oplus \beta \cdot Y = \gamma \cdot K] = 1/2 + \varepsilon$

мұндағы ε - сызықтық ауытқу

8.2 ПАЙДАЛЫ КЕҢЕСТЕР

1. 📝 Әр қадамды мұқият жазып алыңыз
2. 🔍 Теңдеулерді жеңілдету үшін XOR ережелерін пайдаланыңыз ($A \oplus A = 0$)
3. 📊 Ықтималдықтарды бөлшек түрінде сақтаңыз
4. 🔢 Көптеген сынақтар жүргізіп статистиканы жинақтаңыз
5. 💾 Нәтижелерді мерзімді түрде сақтаңыз

8.3 МЫСАЛДЫ ШЕШІМ (ҮЛГІ)

S1 блогы үшін:
text

α = 0101, β = 010
Теңдеу: X16 + K2 + X15 + K4 = C4
Ықтималдық: 12/16 = 3/4
Сынақ нәтижесі: 74/100 = 0.74

Кілт шешімі:
text
K1=0, K2=1, K3=0, K4=1, K5=1, K6=1, K7=0, K8=0,
K9=1, K10=1, K11=1, K12=1, K13=0, K14=0, K15=1, K16=0,
K17=0, K18=0, K19=0, K20=0, K21=0, K22=0, K23=0, K24=0

9. БАҒАЛАУ КРИТЕРИЙЛЕРІ

Критерий	Ұпай	Талдау
Параметрлерді дұрыс енгізу	10	Баптаулар қойындысы
S-блоктарды талдау	20	Сызықтық кестелер
Бір раунд теңдеулері	20	Дұрыс теңдеулер саны
Көп раунд теңдеулері	20	Теңдеулердің дұрыстығы
Статистикалық тексеру	15	Эксперименттік ықтималдықтар
Кілт шешімі	15	Дұрыс кілт биттері
БАРЛЫҒЫ	**100**	

10. ҚОСЫМША РЕСУРСТАР

1. **Кітаптар:**
   - M. Matsui, "Linear Cryptanalysis Method for DES Cipher"
   - A. Menezes, "Handbook of Applied Cryptography"
   - D. Stinson, "Cryptography: Theory and Practice"
2. **Веб-ресурстар:**
   - CryptoLab веб-қолданбасы
   - Python құжаттамасы
   - Криптография бойынша оқу материалдары