ЛАБОРАТОРИЯЛЫҚ ЖҰМЫС
«DES-ТӘРІЗДІ ШИФРДЫ ДИФФЕРЕНЦИАЛДЫҚ ТАЛДАУ»

1. ЖҰМЫСТЫҢ МАҚСАТЫ

DES-тәрізді жеңілдетілген шифрды дифференциалдық криптоталдау әдісін үйрену.

Студенттер мынадай дағдыларды дамытуы тиіс:
- S-блоктардың дифференциалдық таралу кестелерін (ДТК) құру
- Тиімді дифференциалдарды таңдау
- Дифференциалдық сипаттамаларды құру
- Дифференциалдық талдау арқылы кілт биттерін қалпына келтіру

2. ТЕОРИЯЛЫҚ НЕГІЗДЕР

2.1. Негізгі ұғымдар

Дифференциалдық криптоталдау - бұл блогтық шифрларды сынудың күшті әдісі,
ол 1990 жылы Eli Biham және Adi Shamir арқылы жарияланды.

Негізгі терминдер:
- Дифференциал (Δ) - екі мәтін арасындағы айырмашылық (XOR операциясы)
- Дифференциалдық сипаттама - бірнеше раундтар арқылы дифференциалдар тізбегі
- Сипаттаманың ықтималдығы - берілген сипаттаманың орындалу мүмкіндігі
- ДТК (Дифференциалдық таралу кестесі) - S-блоктың дифференциалдық қасиеттерін сипаттайтын кесте

2.2. Формулалар

- Ашық мәтін дифференциалы: $\Delta P = P \oplus P'$
- Шифрланған мәтін дифференциалы: $\Delta C = C \oplus C'$
- S-блок арқылы дифференциалдың ықтималдығы: $p = DDT[\Delta X][\Delta Y] / N$
- Сипаттаманың жалпы ықтималдығы: $P\_total = p1 \times p2 \times ... \times pn$

2.3. Дифференциалдық талдау алгоритмі

1. Шифр құрылымын зерттеу
2. Әр S-блок үшін ДТК құру
3. Жоғары ықтималдығы бар дифференциалдарды таңдау
4. Дифференциалдық сипаттаманы құру
5. Ашық/шифрланған мәтін жұптарын жинақтау
6. Кілт биттерін қалпына келтіру
7. Табылған кілтті тексеру

3. ТАПСЫРМА

3-раундты DES-тәрізді жеңілдетілген шифрды дифференциалдық талдау жүргізу.

3.1. Шифр параметрлері
S-блоктар:
S1: 4,6,1,3,5,7,2,5,5,7,2,4,6,1,3,6 (4 бит → 3 бит)
S2: 3,5,7,2,4,6,1,7,4,6,1,3,5,7,2,1 (4 бит → 3 бит)
S3: 1,3,2,1,2,1,3,2,3,2,1,3,1,3,2,1 (4 бит → 2 бит)

Кеңейту кестесі: 3 4 1 2 6 8 5 7 3 8 2 4
Ауыстыру кестесі: 4 6 8 1 3 5 7 2
Раунд саны: 3

3.2. Бақылау деректері
Ашық мәтіндер (мысал):
P1: 1100110011001100
P2: 1100110011011100 (P1 ⊕ 0000000000010000)

Шифрланған мәтіндер (сәйкес):
C1: (белгісіз кілтпен шифрлау)
C2: (белгісіз кілтпен шифрлау)

4. ЖҰМЫСТЫ ОРЫНДАУ ТӘРТІБІ

4.1. Параметрлерді дайындау
1. diff-analysis.html веб-қолданбасын ашу
2. «Параметрлерді баптау» қойыншасына өту
3. Берілген S-блок параметрлерін тексеру
4. Кеңейту және ауыстыру кестелерін тексеру
5. Параметрлерді сақтау

4.2. S-блоктарды талдау
1. «S-блоктардың ДТК» қойыншасына өту
2. Әр S-блок үшін ДТК құру
3. Есепке жазу:
   - Әр ДТК өлшемі
   - Әр S-блок үшін максималды ықтималдық
   - Әр S-блок үшін ең ықтимал дифференциалдар
4. ДТК файл ретінде сақтау

4.3. Дифференциалдарды таңдау
1. «Дифференциалдар» қойыншасына өту
2. Раунд санын орнату: 3
3. Кіріс дифференциалын таңдау (бір- немесе екі-биттік ұсынылады)
4. Таңдалған дифференциалды жазу: ΔP = _____

5. Дифференциал таңдауын негіздеу

4.4. Дифференциалдық сипаттаманы құру
1. «Диф. сипаттама» қойыншасына өту
2. Таңдалған дифференциалды енгізу
3. Раунд санын орнату: 3
4. Сипаттаманы құру
5. Есепке жазу:
   - Әр раундтың ықтималдығы
   - Сипаттаманың жалпы ықтималдығы
   - Қажетті мәтін жұптарының саны
   - Толық сипаттама (әр раундтың кіріс және шығыс дифференциалдары)

4.5. Деректерді жинақтау
1. Оқытушыдан ашық/шифрланған мәтін жұптарын алу немесе генерациялау
2. Жұптар таңдалған кіріс дифференциалын қанағаттандыруы тиіс
3. Ұсынылатын жұптар саны: кемінде 4 × (1/сипаттама_ықтималдығы)
4. Есепке жиналған жұптар санын жазу

4.6. Кілт биттерін қалпына келтіру
1. «Кілт талдауы» қойыншасына өту
2. Жинақталған мәтін жұптарын енгізу
3. Мақсатты раундты таңдау (1-ші раунд)
4. Әр S-блок үшін:
   - Дифференциалды қанағаттандыратын мүмкін болатын кіріс мәндерін анықтау
   - Сәйкес кілт мәндерін есептеу
5. Есепке жазу:
   - Әр S-блок үшін мүмкін болатын кілт биттері
   - Белгісіз кілт биттерінің саны
   - Кілт биттері үшін теңдеулер (егер қолданылатын болса)

4.7. Кілтті тексеру
1. «Кілт үміткерлерін тексеру» функциясын қолдану
2. Ең ықтимал кілт үміткерлерін тексеру
3. Қалған биттер үшін brute-force әдісін қолдану (қажет болса)
4. Табылған толық кілтті жазу: K = _____
5. Бақылау мәтін жұптарында кілттің дұрыстығын тексеру

5. ЕСЕП БЕРУ ТӘРТІБІ

Есепте мыналар болуы тиіс:

1. Титулдық парақ (тақырып, Аты-жөні, топ, күні)
2. Жұмыстың мақсаты

3. Теориялық бөлім (негізгі ұғымдар, формулалар)
4. Талданатын шифр параметрлері
5. Әр кезең бойынша нәтижелер:
   - S-блоктардың ДТК (кестелер немесе файлға сілтемелер)
   - Негізделген дифференциалдар таңдауы
   - Ықтималдықтары бар дифференциалдық сипаттама
   - Жинақталған мәтін жұптары (қосымшада болуы мүмкін)
   - Кілт биттерін қалпына келтіру процесі
   - Табылған кілт
6. Қорытынды (әдістің тиімділігі, талдау күрделілігі, ұсынымдар)
7. Бақылау сұрақтарына жауаптар

6. БАҚЫЛАУ СҰРАҚТАРЫ

1. Дифференциал мен дифференциалдық сипаттама деген не?
2. Дифференциалдық сипаттаманың ықтималдығы қалай есептеледі?
3. Неге бір- және екі-биттік дифференциалдар әдетте ең тиімді?
4. S-блоктың ДТК шифрдың дифференциалдық талдауға тұрақтылығына қалай әсер етеді?
5. Дифференциалдық талдаудың табысты болуы үшін қанша мәтін жұбы қажет?
6. Дифференциалдық криптоталдаудың артықшылықтары мен кемшіліктері қандай?
7. Шифрдың дифференциалдық талдауға тұрақтылығын қалай арттыруға болады?
8. Дифференциалдық талдау сызықтық талдаудан қандай айырмашылықтары бар?

7. БАҒАЛАУ КРИТЕРИЙЛЕРІ

«Өте жақсы» (85-100 балл):
- Барлық кезеңдерді толық және дұрыс орындау
- Әдісті терең түсіну
- Толық түсіндірмелері бар сапалы есеп
- Барлық бақылау сұрақтарына дұрыс жауаптар

«Жақсы» (70-84 балл):
- Негізгі кезеңдерді шамалы қателермен орындау
- Әдістің негізгі принциптерін түсіну
- Есепте барлық қажетті бөлімдердің болуы
- Көпшілік сұрақтарға дұрыс жауаптар

«Қанағаттанарлық» (50-69 балл):
- Оқытушының көмегімен негізгі кезеңдерді орындау
- Әдісті ішінара түсіну

- Есептің рәсімделуі, бірақ кемшіліктерінің болуы
- Оқытушының көмегімен сұрақтарға жауап беру

«Қанағаттанарлықсыз» (0-49 балл):
- Негізгі кезеңдерді орындамау
- Әдісті түсінбеу
- Есептің рәсімделмеуі немесе өрескел қателерінің болуы

Баллдық үлестіру:
- Параметрлердің дұрыстығы: 10 балл
- ДТК талдауы: 20 балл
- Дифференциалдар таңдауы: 15 балл
- Сипаттама құру: 25 балл
- Кілтті қалпына келтіру: 20 балл
- Есепті рәсімдеу: 10 балл
- БАРЛЫҒЫ: 100 балл

8. СТУДЕНТТЕРГЕ АРНАЛҒАН ҰСЫНЫМДАР

1. Жұмысты орындау алдында теориялық материалды мұқият оқып шығыңыз
2. Есептеулерді автоматтандыру үшін веб-қолданбаны пайдаланыңыз, бірақ әр қадамды түсініңіз
3. Барлық аралық нәтижелерді жазып алыңыз
4. Әр кезеңде есептеулерді тексеріңіз
5. Есепте өз шешімдеріңізді міндетті түрде негіздеңіз
6. Автоматты тұрғыда құрастырылған есептерді көшірмелеңіз - нәтижелерді талдап, түсіндіріңіз

9. ҚОСЫМША

3 раунд үшін дифференциалдық сипаттама мысалы:

1-раунд:
Кіріс: $\Delta P = 0000000000010000$
S1: $\Delta X = 0001 \rightarrow \Delta Y = 010$ ($p = 6/16$)
S2: $\Delta X = 0000 \rightarrow \Delta Y = 000$ ($p = 1$)
S3: $\Delta X = 0000 \rightarrow \Delta Y = 00$ ($p = 1$)
Раунд ықтималдығы: 0.375

2-раунд:
(ДТК бойынша есептеу)
...

3-раунд:
(ДТК бойынша есептеу)

...

Жалпы ықтималдық: ~0.05
Қажетті жұптар саны: ~20

10. ӘДЕБИЕТТЕР

1. Biham E., Shamir A. Differential Cryptanalysis of DES-like Cryptosystems // Journal of Cryptology. 1991.
2. Stinson D. Cryptography: Theory and Practice. CRC Press, 2005.
3. Мао В. Заманауи криптография: теория және практика. М.: Вильямс, 2005.
4. Handbook of Applied Cryptography. CRC Press, 1996.

ӘЗІРЛЕГЕНДЕР: Ақпараттық қауіпсіздік кафедрасы
КҮНІ: _____
НҰСҚА: 1.0