НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. Ігоря СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Звіт з виконання кваліфікаційного дослідження

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №1

З КУРСУ

МЕТОДИ КРИПТОАНАЛІЗУ 1

Виконала студентка
групи ФІ-32мн
Міснік Аліна Олексіївна

Викладач:
Ядуха Д.В.

Київ — 2024

ВСТУП

Метою роботи є ознайомлення з принципами баєсівського підходу в криптоаналізі, побудова детерміністичної та стохастичної вирішуючих функцій для моделей схем шифрування та криптоаналіз моделей шифрів за допомогою програмної реалізації, зокрема здійснення порівняльного аналізу вирішуючих функцій.

Задача полягає у реалізації алгоритмів програмно і поданні результатів побудови детерміністичної та стохастичної вирішуючих функцій у вигляді таблиць. Для цього необхідно:

(а) порахувати розподіли $P(C)$ та $P(M, C)$;

(б) ґрунтуючись на цих розподілах обчислити $P(M|C)$;

(в) побудувати оптимальні детерміністичну та стохастичну вирішуючі функції, що зводиться до максимізації $P(M|C)$.

Після цього обчислимо середні втрати і проведемо порівняльний аналіз вирішуючих функцій.

Будемо використовувати дані для варіанта №10.

1 ХІД РОБОТИ

Для заданої варіантом моделі шифру, реалізуємо алгоритм побудови стохастичної та детерміністичної вирішуючих функцій, а також проведемо їх порівняльний аналіз.

1.1 Опис алгоритму побудови детерміністичної вирішуючої функції

Означення 1.1. Детерміністичною вирішуючою функцією називається послідовність відображень:

$$\delta_D = \{\delta_D^{(n)} : Z_m^n \to Z_m^n, n \in \mathbb{N}\},$$

де Z_m — алфавіт шифротекстів та відкритих текстів, n — довжина шифротексту, що був перехоплений криптоаналітиком.

Оскільки детерміністична розв'язувальна функція оптимальна тоді і тільки тоді, коли вона байєсівська, то наведемо алгоритм для побудови баєсівської детерміністичної вирішуючої функці:

1) Порахувати розподіли $P(C)$ та $P(M, C)$.

2) За допомогоюь цих розподілів обчислити $P(M|C)$.

3) Побудувати оптимальну детерміністичну вирішуючу функцію шляхом максимізації $P(M|C)$.

4) Обчислити середні втрати.

1.2 Опис алгоритму побудови стохастичної вирішуючої функції

Означення 1.2. Стохастичною вирішуючою функцією називається послідовність $m^n \times m^n$-матриць:

$$\delta_S = \{\delta_S^{(n)} : ||\delta_S^{(n)}(C, M)||_1^{m^n}, n \in \mathbb{N}\},$$

де $\delta_S^{(n)}(C, M) \geqslant 0$ та для усіх C виконується:

$$\sum_M \delta_S^{(n)}(C, M) = 1$$

Алгоритм виглядає аналогічно до побудови детерміністичної вирішуючої функції:

1) Порахувати розподіли $P(C)$ та $P(M, C)$.

2) За допомогоюь цих розподілів обчислити $P(M|C)$.

3) Знайти усі максимуми $P(M|C)$ в кожному рядку. Якщо максимумів більше 1, то знаходиться ймовірнісний розподіл.

4) Сформувати матрицю оптимальної стохастичної вирішувальної функції з відповідних рядків.

5) Обчислити середні втрати.

1.3 Таблиці

M/C	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	C15	C16	C17	C18	C19	C20
M1	0	0	0,19	0	0,21	0	0,19	0,8	0,8	0	0	0	0,42	0,18	0,1	0,13	0	0,47	0	0,07
M2	0,27	0	0,1	0,19	0	0	0	0,17	0,17	0,11	0,1	0,15	0	0,18	0	0,06	0	0,08	0	0,47
M3	0	0	0	0,1	0	0,19	0,1	0	0,08	0,11	0,38	0	0	0,09	0,19	0,51	0,1	0,08	0	0,13
M4	0,27	0	0,19	0	0,21	0	0	0,25	0,17	0,11	0	0,07	0,08	0	0	0	0,29	0	0,55	0
M5	0	0,24	0	0,19	0	0,29	0,19	0,08	0,08	0	0	0,45	0,08	0,09	0,19	0,06	0,1	0	0,08	0,07
M6	0,02	0,07	0,18	0	0,03	0	0	0	0,05	0,06	0,03	0	0,02	0,07	0	0,04	0	0,02	0	0,04
M7	0,15	0,07	0,03	0	0	0,05	0	0,02	0	0,03	0,03	0,06	0,02	0	0	0,02	0,05	0,04	0,04	0
M8	0,02	0,07	0,03	0	0,06	0,03	0,08	0	0	0,09	0,03	0,02	0	0	0,05	0	0,18	0	0	0,02
M9	0,02	0,03	0	0	0	0,16	0,05	0,05	0	0	0,03	0,04	0,05	0,05	0,05	0,02	0,05	0	0	0,02
M10	0,02	0	0,03	0	0,06	0	0,03	0,07	0	0	0,05	0,02	0	0,15	0,03	0,02	0,05	0,02	0,04	0,02
M11	0,02	0	0,03	0	0,06	0,05	0,05	0	0	0,21	0	0,04	0,02	0	0,05	0	0	0	0,11	0
M12	0,02	0,07	0	0,08	0,03	0,05	0,03	0,14	0,02	0	0	0	0,02	0,05	0,03	0,02	0,03	0,02	0	0,02
M13	0,02	0,26	0,05	0,08	0,03	0,03	0	0	0,02	0	0,08	0	0	0	0,03	0,05	0	0	0,02	0
M14	0	0,03	0	0,03	0,03	0	0,05	0,05	0,14	0	0,03	0,02	0,02	0	0,05	0	0	0,06	0,02	0,06
M15	0,05	0	0,03	0,03	0,17	0,03	0	0	0,02	0,09	0,03	0	0	0,05	0	0,04	0,03	0,06	0,02	0
M16	0,05	0	0,05	0,05	0,06	0	0,03	0,02	0,02	0	0	0,04	0,16	0	0,03	0	0,05	0,02	0,02	0
M17	0	0,13	0,03	0,18	0	0	0	0,02	0,07	0,06	0	0	0,02	0	0,05	0	0	0,02	0,02	0,04
M18	0,05	0,03	0	0,05	0,03	0,03	0	0,02	0,02	0,06	0	0,06	0,02	0,02	0,16	0,04	0	0	0,02	0
M19	0	0	0	0	0,03	0,03	0,03	0,02	0,05	0,06	0,16	0	0,02	0,07	0	0	0,03	0,06	0	0,6
M20	0	0	0,08	0,03	0,03	0,08	0,18	0	0	0	0,08	0,02	0,02	0	0	0	0,05	0,02	0,04	0

Таблиця 1.1 – Таблиця ймовірностей $P(M|C)$

M_1
M_{12}
M_0
M_1
M_0
M_4
M_0
M_3
M_1
M_10
M_2
M_4
M_0
M_0
M_2
M_2
M_3
M_0
M_3
M_1

Таблиця 1.2 – Оптимальна детерміністична вирішувальна функція

0	0,5	0	0,5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
0,5	0	0	0,5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0,5	0	0	0,5	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0,5	0	0	0,5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0,5	0	0	0	0,5	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0,5	0	0,5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0,5	0,5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0,5	0	0,5	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Таблиця 1.3 – Оптимальна стохастична вирішувальна функція

1.3.1 Середні втрати для вирішуючих функцій

Середні втрати детерміністичної вирішуючої функції: 0.6792560000000001 Середні втрати стохастичної вирішуючої функції: 0.6783999999999986

Криптоаналітик майже з однаковою ймовірністю зможе отримати відкритий текст за шифротекстом.

1.4 Опис труднощів

Труднощі виникли на етапі знаходження оптимальної детерміністичної і стохастичної вирішуючих функцій. Спочатку було не зрозуміло чим взагалі вони відрізняються і як максимізуючи одну матрицю можна знайти дві різних. Після більш детального аналізу різниця стала зрозуміла, проте з'явилася проблема зі знайденням розподілу по рядкам стохастичної функції. Втім, врешті вдалося порахувати і його.

ВИСНОВКИ

У роботі було досліджено і програмно реалізовано алгоритми побудови оптимальної детерміністичної та стохастичної вирішуючих функцій для моделей схем шифрування за допомогою принципів баєсівського підхіду в криптоаналізі.

Було знайдено розподіл $P(M|C)$ і отримано таблиці для оптимальної детерміністичної та стохастичної вирішуючих функцій шляхом максимізації цього розподіла, а також обчислено середні втрати обох функцій. Отримані середні втрати майже однакові, що означає, що для даної моделі шифру криптоаналітик має однакову ймовірність співпадіння обраного шифротексту з відповідним йому відкритим текстом.