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

Звіт з виконання лабораторної роботи

Баєсівський підхід в криптоаналізі: побудова і дослідження детерміністичної та стохастичної вирішуючих функцій

Виконала студентка
групи ФІ-52мн
Балацька Вікторія

Варіант 10

Київ — 2025

1 Вступ

Мета роботи : 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 : Реалізувати алгоритми програмно і подати результати побудови детерміністичної та стохастичної вирішуючих функцій у вигляді таблиць. Для цього необхідно виконати:

1. Обрахунок розподілів $P(C)$ та $P(M,C)$.
2. Обрахунок $P(M|C)$.
3. Побудувати оптимальні детерміністичну та стохастичну вирішуючі функції шляхом максимізації.
4. Обчислити функції втрат для цих функцій.
5. Обчислити середні втрати.
6. Зробити порівняльний аналіз результатів.

2 Побудова вирішуючих функцій

Перш за все, мною було обраховано розподіли $P(C)$ (Таблиця 1) та $P(M,C)$(Таблиця 2) за допомогою наступних формул:

$$P(C) = \sum_{(M,k):E_k(M)=C} P(M,k);$$
$$P(M,C) = \sum_{k:E_k(M)=C} P(M,k).$$

Результати цих обрахунків дали можливість обчислити імовірність $P(M|C) = \frac{P(M,C)}{P(C)}$. Результати імовірностей подані у таблиці 3.

Після отримання імовірностей, було побудовано оптимальну детерміністичну функцію шляхом максимізації значень $P(M|C)$. Отримана функція подана у таблиці 4.

Отримавши результати, було обраховано функцію витрат та середні втрати детерміністичної вирішуючої функції за формулами:

$$L_{\delta_D}(M,C) = \begin{cases} 1, & \text{якщо } \delta_D(C) \neq M; \\ 0, & \text{якщо } \delta_D(C) = M. \end{cases}$$

$$l_{\delta_D} = \sum_{M\in\mathcal{M}} \sum_{C\in\mathcal{C}} P(M,C) \cdot L_{\delta_D}(M,C) = 0.678.$$

Після цього було побудовано оптимальну стохастичну функцію, подану в таблиці **??**. Її обчислення є подібним до оптимальної детерміністичної функції, проте у випадках, коли в рядках таблиці 3 максимальне значення ймовірності траплялося кілька разів, формувався відповідний імовірнісний розподіл.

Далі обраховано середні втрати стохастичної вирішуючої функції, за формулою:

$$l_{\delta_S} = \sum_{M \in \mathcal{M}} \sum_{C \in \mathcal{C}} P(M,C) \cdot L_{\delta_S}(M,C) = 0.678.$$

3 Опис труднощів та їх вирішення

Під час виконання роботи виникали такі труднощі:

1. При зчитування CSV файлу були проблеми, оскільки необхідно було зчитувати два типи даних: int та float. Для цього я реалізувала універсальну функцію, де обробляються обидва випадки

2. Складно було зрозуміти теоретичні відомості щодо стохастичної вирішуючої функції. Для цього скористалась додатковими лекціями

4 Висновок

У ході виконання роботи мною були розроблені алгоритми та реалізовані оптимальні детермінована й стохастична вирішувальні функції на основі баєсівського підходу у криптоаналізі.

Обидві функції було побудовано та досліджено їх середні втрати. Отримані результати показали, що середні втрати для обох функцій є однаковими. Це свідчить про те, що криптоаналітик має рівну ймовірність відновлення відкритого тексту за даним шифротекстом, незалежно від обраної вирішувальної функції.

Додатки

0.049	0.036	0.046	0.046	0.043	0.046	0.046	0.052	0.052	0.040	0.046	0.059	0.052	0.049	0.046	0.068	0.046	0.056	0.056	0.065

Табл. 1: Імовірності P(C)

0.000	0.000	0.009	0.000	0.009	0.000	0.009	0.004	0.004	0.000	0.000	0.000	0.022	0.009	0.004	0.009	0.000	0.026	0.000	0.004
0.013	0.000	0.004	0.009	0.000	0.000	0.000	0.009	0.009	0.004	0.004	0.009	0.000	0.009	0.000	0.004	0.000	0.004	0.000	0.031
0.000	0.000	0.000	0.004	0.000	0.009	0.004	0.000	0.004	0.004	0.018	0.000	0.000	0.004	0.009	0.035	0.004	0.004	0.000	0.009
0.013	0.000	0.009	0.000	0.009	0.000	0.000	0.013	0.009	0.004	0.000	0.004	0.004	0.000	0.000	0.000	0.013	0.000	0.031	0.000
0.000	0.009	0.000	0.009	0.000	0.013	0.009	0.004	0.004	0.000	0.000	0.026	0.004	0.004	0.009	0.004	0.004	0.000	0.004	0.004
0.001	0.002	0.008	0.000	0.001	0.000	0.000	0.000	0.002	0.002	0.001	0.000	0.001	0.004	0.000	0.002	0.000	0.001	0.000	0.002
0.007	0.002	0.001	0.000	0.000	0.002	0.000	0.001	0.000	0.001	0.001	0.004	0.001	0.000	0.000	0.001	0.002	0.002	0.002	0.000
0.001	0.002	0.001	0.000	0.002	0.001	0.004	0.000	0.000	0.004	0.001	0.001	0.000	0.000	0.002	0.000	0.008	0.000	0.000	0.001
0.001	0.001	0.000	0.000	0.000	0.007	0.002	0.002	0.000	0.000	0.001	0.002	0.002	0.002	0.002	0.001	0.002	0.000	0.000	0.001
0.001	0.000	0.001	0.000	0.002	0.000	0.001	0.004	0.000	0.000	0.002	0.001	0.000	0.007	0.001	0.001	0.002	0.001	0.002	0.001
0.001	0.000	0.001	0.000	0.002	0.002	0.002	0.000	0.000	0.008	0.000	0.002	0.001	0.000	0.002	0.000	0.000	0.000	0.006	0.000
0.001	0.002	0.000	0.004	0.001	0.002	0.001	0.007	0.001	0.000	0.000	0.000	0.001	0.002	0.001	0.001	0.001	0.001	0.000	0.001
0.001	0.010	0.002	0.004	0.001	0.001	0.000	0.000	0.001	0.000	0.004	0.000	0.000	0.000	0.001	0.004	0.000	0.000	0.001	0.000
0.000	0.001	0.000	0.001	0.001	0.000	0.002	0.002	0.007	0.000	0.001	0.001	0.001	0.000	0.002	0.000	0.000	0.004	0.001	0.004
0.002	0.000	0.001	0.001	0.007	0.001	0.000	0.000	0.001	0.004	0.001	0.000	0.000	0.002	0.000	0.002	0.001	0.004	0.001	0.000
0.002	0.000	0.002	0.002	0.002	0.000	0.001	0.001	0.001	0.000	0.000	0.002	0.008	0.000	0.001	0.000	0.002	0.001	0.001	0.000
0.000	0.005	0.001	0.008	0.000	0.000	0.000	0.001	0.004	0.002	0.000	0.000	0.001	0.000	0.002	0.000	0.000	0.001	0.001	0.002
0.002	0.001	0.000	0.002	0.001	0.001	0.000	0.001	0.001	0.002	0.000	0.004	0.001	0.001	0.007	0.002	0.000	0.000	0.001	0.000
0.000	0.000	0.000	0.000	0.001	0.001	0.001	0.001	0.002	0.002	0.007	0.000	0.001	0.004	0.000	0.000	0.001	0.004	0.000	0.004
0.000	0.000	0.004	0.001	0.001	0.004	0.008	0.000	0.000	0.000	0.004	0.001	0.001	0.000	0.000	0.000	0.002	0.001	0.002	0.000

Табл. 2: Імовірності P(M,C)

0.000	0.000	0.191	0.000	0.206	0.000	0.191	0.084	0.084	0.000	0.000	0.000	0.420	0.179	0.096	0.129	0.000	0.475	0.000	0.067
0.268	0.000	0.096	0.191	0.000	0.000	0.000	0.168	0.168	0.111	0.096	0.150	0.000	0.179	0.000	0.064	0.000	0.079	0.000	0.472
0.000	0.000	0.000	0.096	0.000	0.191	0.096	0.000	0.084	0.111	0.383	0.000	0.000	0.089	0.191	0.515	0.096	0.079	0.000	0.135
0.268	0.000	0.191	0.000	0.206	0.000	0.000	0.252	0.168	0.111	0.000	0.075	0.084	0.000	0.000	0.000	0.287	0.000	0.554	0.000
0.000	0.242	0.000	0.191	0.000	0.287	0.191	0.084	0.084	0.000	0.000	0.449	0.084	0.089	0.191	0.064	0.096	0.000	0.079	0.067
0.024	0.066	0.183	0.000	0.028	0.000	0.000	0.000	0.046	0.061	0.026	0.000	0.023	0.073	0.000	0.035	0.000	0.022	0.000	0.037
0.146	0.066	0.026	0.000	0.000	0.052	0.000	0.023	0.000	0.030	0.026	0.061	0.023	0.000	0.000	0.018	0.052	0.043	0.043	0.000
0.024	0.066	0.026	0.000	0.056	0.026	0.078	0.000	0.000	0.091	0.026	0.020	0.000	0.000	0.052	0.000	0.183	0.000	0.000	0.018
0.024	0.033	0.000	0.000	0.000	0.157	0.052	0.046	0.000	0.000	0.026	0.041	0.046	0.049	0.052	0.018	0.052	0.000	0.000	0.018
0.024	0.000	0.026	0.000	0.056	0.000	0.026	0.069	0.000	0.000	0.052	0.020	0.000	0.146	0.026	0.018	0.052	0.022	0.043	0.018
0.024	0.000	0.026	0.000	0.056	0.052	0.052	0.000	0.000	0.212	0.000	0.041	0.023	0.000	0.052	0.000	0.000	0.000	0.108	0.000
0.024	0.066	0.000	0.078	0.028	0.052	0.026	0.137	0.023	0.000	0.000	0.000	0.023	0.049	0.026	0.018	0.026	0.022	0.000	0.018
0.024	0.264	0.052	0.078	0.028	0.026	0.000	0.000	0.023	0.000	0.078	0.000	0.000	0.000	0.026	0.053	0.000	0.000	0.022	0.000
0.000	0.033	0.000	0.026	0.028	0.000	0.052	0.046	0.137	0.000	0.026	0.020	0.023	0.000	0.052	0.000	0.000	0.065	0.022	0.055
0.049	0.000	0.026	0.026	0.168	0.026	0.000	0.000	0.023	0.091	0.026	0.000	0.000	0.049	0.000	0.035	0.026	0.065	0.022	0.000
0.049	0.000	0.052	0.052	0.056	0.000	0.026	0.023	0.023	0.000	0.000	0.041	0.160	0.000	0.026	0.000	0.052	0.022	0.022	0.000
0.000	0.132	0.026	0.183	0.000	0.000	0.000	0.023	0.069	0.061	0.000	0.000	0.023	0.000	0.052	0.000	0.000	0.022	0.022	0.037
0.049	0.033	0.000	0.052	0.028	0.026	0.000	0.023	0.023	0.061	0.000	0.061	0.023	0.024	0.157	0.035	0.000	0.000	0.022	0.000
0.000	0.000	0.000	0.000	0.028	0.026	0.026	0.023	0.046	0.061	0.157	0.000	0.023	0.073	0.000	0.000	0.026	0.065	0.000	0.055
0.000	0.000	0.078	0.026	0.028	0.078	0.183	0.000	0.000	0.000	0.078	0.020	0.023	0.000	0.000	0.000	0.052	0.022	0.043	0.000

Табл. 3: Імовірності $P(M|C)$

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

Табл. 4: Оптимальна детерміністична вирішуюча функція

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	0.0	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	0.0	0.0	0.0	0.0	1.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
0.5	0.0	0.0	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	0.0	0.0	0.0
0.0	0.5	0.0	0.0	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	0.0	0.0
0.5	0.0	0.0	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	0.0	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	0.0	0.0	0.0	0.0	0.0
0.5	0.0	0.0	0.0	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	0.0	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	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	0.0	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	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	0.0	1.0	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	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	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	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	0.0	0.0	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	0.0	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	0.0	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	0.0	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	0.0	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	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	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	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0

Табл. 5: Оптимальна стохастична вирішуюча функція