Національний технічний університет України
«Київський політехнічний інститут»

Фізико технічний інститут

Кафедра математичних методів захисту інформації

МЕТОДИ КРИПТОАНАЛІЗУ
КОМП'ЮТЕРНИЙ ПРАКТИКУМ №1

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

Виконали:
студенти групи ФІ-73
Корж Нікіта
Тафтай Анастасія

Перевірила:
Ядуха Д. В.

Київ 2021

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.

Завдання

1) Ознайомитись з порядком виконання комп'ютерного практикуму та відповідними вимогами до виконання роботи.

2) Уважно прочитати необхідні теоретичні відомості до комп'ютерного практикуму.

3) Для заданого варіанта моделі шифру описати алгоритм побудови детерміністичної та стохастичної вирішуючих функцій. Створити репозиторій в системі контролю версій Git (бажано використовувати вебсервіс GitHub). Важливо:
(а) репозиторій створюється перед початком роботи над програмним кодом (якщо репозиторій приватний, то перед початком роботи має бути надано доступ викладачу до даного репози- торію);
(б) весь процес створення програмного коду має бути відображений у відповідних комітах про- екту (для кожної атомарної зміни коду має бути власний коміт);
(в) програмна реалізація не допускається до захисту при недотриманні вищевизначених вимог.

4) Реалізувати алгоритми програмно і подати результати 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) побудова оптимальних детерміністичної та стохастичної вирішуючих функцій зводиться до максимізації $P(M|C)$.

5) Обчислити середні втрати, провести порівняльний аналіз вирішуючих функцій.

Варіант завдання: 16

Хід роботи

Опис алгоритму побудови детерміністичної та стохастичної вирішуючих функцій

Для побудови детерміністичної функції використовувались значення $P(M|C)$ так, що $\delta_d(C) = index \max\limits_{M} P(M|C)$.

Стохастична функція зберігає усі максимуми, тому вона будувалась так що в кожному рядку матриці на місцях максимальних елементів вона дорівнювала (1 / кількість максмимальних елементів у рядку), а на місцях не максимальних елементів дорівнювала нулю.

Таблиця $P(M|C)$ для 16 варіанту

[0.0000, 0.0400, 0.0200, 0.0000, 0.2800, 0.0000, 0.0000, 0.0000, 0.0200, 0.2800, 0.0000, 0.0000, 0.0200, 0.0600, 0.2200, 0.0200, 0.0200, 0.0000, 0.0200, 0.0000]
[0.1091, 0.0000, 0.0000, 0.0364, 0.0364, 0.0000, 0.2000, 0.0545, 0.0182, 0.0000, 0.0182, 0.0000, 0.0545, 0.0364, 0.0000, 0.0182, 0.0182, 0.2000, 0.0000, 0.2000]
[0.2000, 0.0000, 0.0000, 0.0000, 0.2000, 0.2000, 0.0000, 0.0000, 0.0333, 0.2000, 0.0167, 0.0333, 0.0000, 0.0167, 0.0000, 0.0167, 0.0167, 0.0333, 0.0000, 0.0333]
[0.0000, 0.2200, 0.0000, 0.0000, 0.0000, 0.2800, 0.0200, 0.0000, 0.0400, 0.0400, 0.0600, 0.0200, 0.0000, 0.0000, 0.0000, 0.2600, 0.0000, 0.0200, 0.0400, 0.0000]
[0.0000, 0.0000, 0.0400, 0.2200, 0.0000, 0.0000, 0.0200, 0.0000, 0.2400, 0.0200, 0.0600, 0.0000, 0.0200, 0.0400, 0.0000, 0.0000, 0.0400, 0.2600, 0.0200, 0.0200]
[0.8471, 0.0118, 0.0000, 0.0000, 0.0059, 0.0000, 0.0000, 0.0000, 0.0059, 0.0059, 0.0176, 0.0118, 0.0059, 0.0000, 0.0000, 0.0000, 0.0000, 0.0706, 0.0000, 0.0059, 0.0118]
[0.6545, 0.0182, 0.0091, 0.0000, 0.0091, 0.0091, 0.0000, 0.1182, 0.0091, 0.0000, 0.0091, 0.0091, 0.0182, 0.0000, 0.0000, 0.0091, 0.1000, 0.0000, 0.0182, 0.0091]
[0.2000, 0.2000, 0.2000, 0.0333, 0.0000, 0.0333, 0.0000, 0.0000, 0.0167, 0.0000, 0.0000, 0.0333, 0.0000, 0.0000, 0.1833, 0.0167, 0.0333, 0.0000, 0.0333, 0.0167]
[0.0000, 0.0200, 0.0000, 0.0600, 0.0000, 0.0000, 0.2400, 0.2600, 0.0000, 0.0200, 0.0200, 0.2400, 0.0400, 0.0600, 0.0200, 0.0000, 0.0000, 0.0000, 0.0000, 0.0200]
[0.2000, 0.0000, 0.1833, 0.2000, 0.0167, 0.0167, 0.0000, 0.0167, 0.1833, 0.0000, 0.0167, 0.0000, 0.0000, 0.0167, 0.0333, 0.0333, 0.0167, 0.0167, 0.0500, 0.0000]
[0.0000, 0.0200, 0.0000, 0.2200, 0.0200, 0.0000, 0.0200, 0.0400, 0.0000, 0.0000, 0.0000, 0.0000, 0.0600, 0.0000, 0.0600, 0.4800, 0.0000, 0.0600, 0.0000, 0.0200]
[0.0000, 0.0200, 0.0000, 0.0000, 0.0200, 0.0000, 0.0800, 0.0200, 0.2200, 0.0200, 0.0000, 0.0000, 0.0000, 0.0400, 0.0200, 0.0200, 0.0000, 0.0400, 0.0400, 0.4600]
[0.2769, 0.0000, 0.0462, 0.0154, 0.0154, 0.0000, 0.0154, 0.0000, 0.0154, 0.0000, 0.1692, 0.1692, 0.0000, 0.1846, 0.0308, 0.0462, 0.0000, 0.0000, 0.0000, 0.0154]
[0.0000, 0.0400, 0.0000, 0.0400, 0.0000, 0.0000, 0.2600, 0.0200, 0.0000, 0.0400, 0.0200, 0.0400, 0.2200, 0.0000, 0.0200, 0.0000, 0.0800, 0.2200, 0.0000, 0.0000]
[0.2000, 0.1833, 0.0000, 0.0333, 0.0167, 0.0167, 0.0167, 0.0333, 0.0167, 0.2000, 0.0167, 0.0333, 0.0000, 0.0000, 0.0000, 0.0000, 0.0333, 0.0000, 0.1833, 0.0167]
[0.0000, 0.0000, 0.0600, 0.0000, 0.0200, 0.0200, 0.0200, 0.0000, 0.0200, 0.0000, 0.0200, 0.2600, 0.2200, 0.0000, 0.0600, 0.0000, 0.0000, 0.0200, 0.2400, 0.0400]
[0.1091, 0.0000, 0.0364, 0.0182, 0.2182, 0.0364, 0.0182, 0.2000, 0.0182, 0.0545, 0.2000, 0.0000, 0.0000, 0.0000, 0.0364, 0.0182, 0.0000, 0.0182, 0.0000, 0.0182]
[0.1091, 0.0545, 0.0182, 0.0182, 0.0000, 0.2545, 0.0000, 0.0000, 0.0182, 0.0182, 0.2000, 0.0182, 0.0182, 0.2000, 0.0000, 0.0182, 0.0000, 0.0000, 0.0182, 0.0364]
[0.0000, 0.0200, 0.2600, 0.0200, 0.0200, 0.0000, 0.0400, 0.0200, 0.0400, 0.0000, 0.0000, 0.0000, 0.0400, 0.2400, 0.0400, 0.0000, 0.2200, 0.0400, 0.0000, 0.0000]
[0.0000, 0.0200, 0.0200, 0.0200, 0.0200, 0.0400, 0.0200, 0.0400, 0.0000, 0.0000, 0.0000, 0.0200, 0.2400, 0.0200, 0.2200, 0.0000, 0.0400, 0.0400, 0.2400, 0.0000]

Таблиця $P(M|C)$ для 6 варіанту

[0.0000, 0.0400, 0.0000, 0.0400, 0.0000, 0.0400, 0.0000, 0.2800, 0.0400, 0.0400, 0.0400, 0.0800, 0.0400, 0.0800, 0.0400, 0.0400, 0.0400, 0.0000, 0.0800, 0.0800]
[0.0000, 0.0000, 0.2400, 0.0800, 0.0000, 0.0800, 0.0400, 0.0800, 0.0800, 0.0400, 0.0000, 0.0000, 0.0000, 0.0000, 0.0400, 0.1600, 0.0800, 0.0400, 0.0000, 0.0400]
[0.2000, 0.0333, 0.0000, 0.2333, 0.0333, 0.0000, 0.0000, 0.0667, 0.0000, 0.0333, 0.0000, 0.0333, 0.1000, 0.1000, 0.0333, 0.0667, 0.0000, 0.0000, 0.0333, 0.0333]
[0.2000, 0.0000, 0.1333, 0.0000, 0.0333, 0.0667, 0.0000, 0.0667, 0.0333, 0.0333, 0.0333, 0.0000, 0.0000, 0.2333, 0.0333, 0.0000, 0.0000, 0.1000, 0.0333, 0.0000]
[0.0000, 0.0400, 0.0400, 0.0000, 0.0000, 0.0000, 0.0400, 0.1200, 0.0400, 0.0400, 0.0800, 0.3600, 0.0000, 0.0800, 0.0000, 0.0000, 0.0000, 0.0000, 0.1200, 0.0400, 0.0000]
[0.2000, 0.0333, 0.0000, 0.0000, 0.0000, 0.0000, 0.1333, 0.0333, 0.0333, 0.0000, 0.0000, 0.0333, 0.0333, 0.0000, 0.0667, 0.0667, 0.0000, 0.0333, 0.1333, 0.2000]
[0.4500, 0.0250, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0500, 0.0500, 0.0250, 0.0000, 0.0250, 0.0250, 0.0000, 0.0500, 0.0250, 0.1000, 0.1500, 0.0000, 0.0250]
[0.2000, 0.0333, 0.0667, 0.0000, 0.0667, 0.0333, 0.2000, 0.0000, 0.0333, 0.0000, 0.0667, 0.0333, 0.0333, 0.0000, 0.0333, 0.0000, 0.0333, 0.0333, 0.0667, 0.0667]
[0.0000, 0.0000, 0.0000, 0.0400, 0.3200, 0.0400, 0.0000, 0.0400, 0.0000, 0.0000, 0.0400, 0.0400, 0.0400, 0.0400, 0.1200, 0.0800, 0.0400, 0.0800, 0.0000, 0.0800]
[0.0000, 0.0800, 0.0400, 0.0400, 0.0000, 0.0000, 0.1600, 0.0000, 0.3200, 0.0000, 0.0000, 0.0800, 0.0000, 0.1600, 0.0400, 0.0400, 0.0000, 0.0000, 0.0000, 0.0400]
[0.2000, 0.1000, 0.0000, 0.0667, 0.0667, 0.1000, 0.0333, 0.0333, 0.0333, 0.0000, 0.0000, 0.0333, 0.0000, 0.0333, 0.0000, 0.2000, 0.0000, 0.0333, 0.0000, 0.0667]
[0.4500, 0.0000, 0.0500, 0.0500, 0.0750, 0.0000, 0.0500, 0.0000, 0.0000, 0.0500, 0.0000, 0.0000, 0.0250, 0.0250, 0.0000, 0.0250, 0.1750, 0.0000, 0.0000, 0.0250]
[0.2000, 0.3000, 0.0000, 0.0333, 0.0000, 0.0333, 0.0000, 0.0000, 0.0333, 0.0333, 0.0667, 0.0333, 0.0000, 0.0333, 0.0000, 0.0333, 0.0333, 0.1000, 0.0333, 0.0333]
[0.2000, 0.0333, 0.0000, 0.0333, 0.1000, 0.0333, 0.0000, 0.0333, 0.0000, 0.0000, 0.0000, 0.0667, 0.0667, 0.0000, 0.2667, 0.0333, 0.0667, 0.0000, 0.0000, 0.0667]
[0.6545, 0.0000, 0.0182, 0.0364, 0.0000, 0.0000, 0.0000, 0.0364, 0.0182, 0.0364, 0.0182, 0.0182, 0.0000, 0.0364, 0.0000, 0.0000, 0.0364, 0.0364, 0.0364, 0.0182]
[0.2000, 0.0000, 0.0667, 0.0000, 0.1000, 0.0333, 0.0333, 0.0667, 0.0333, 0.0000, 0.0667, 0.0333, 0.2333, 0.0667, 0.0000, 0.0000, 0.0333, 0.0000, 0.0333, 0.0000]
[0.0000, 0.0400, 0.0400, 0.0400, 0.0000, 0.0000, 0.0400, 0.0000, 0.1200, 0.0800, 0.0800, 0.0000, 0.0400, 0.0000, 0.0800, 0.0000, 0.0000, 0.0400, 0.3200, 0.0800]
[0.4500, 0.0000, 0.0000, 0.0250, 0.0000, 0.2000, 0.0000, 0.0000, 0.0250, 0.0500, 0.0250, 0.0500, 0.0500, 0.0000, 0.0250, 0.0500, 0.0000, 0.0000, 0.0500, 0.0000]
[0.2000, 0.0667, 0.1000, 0.0333, 0.0000, 0.0333, 0.0667, 0.0000, 0.0000, 0.2667, 0.0667, 0.0667, 0.0333, 0.0000, 0.0000, 0.0000, 0.0667, 0.0000, 0.0000, 0.0000]
[0.2000, 0.0333, 0.0667, 0.0667, 0.0667, 0.0667, 0.0000, 0.0333, 0.0000, 0.0333, 0.0333, 0.2000, 0.0333, 0.0333, 0.0333, 0.0333, 0.0333, 0.0333, 0.0000, 0.0000]

Знайдені детерміністична та стохастична функції у вигляді таблиць для 16 варіанту

Детерміністична функція:

[4, 6, 4, 5, 17, 0, 0, 1, 7, 3, 15, 19, 0, 6, 9, 11, 4, 5, 2, 12]

Стохастична функція:

[0.0000, 0.0000, 0.0000, 0.0000, 0.5000, 0.0000, 0.0000, 0.0000, 0.0000, 0.5000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000]
[0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.3333, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.3333, 0.0000, 0.3333]
[0.0000, 0.0000, 0.0000, 0.0000, 0.3333, 0.3333, 0.0000, 0.0000, 0.0000, 0.3333, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000]
[0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 1.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000]
[0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 1.0000, 0.0000, 0.0000]
[1.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000]
[1.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000]
[0.0000, 0.5000, 0.5000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000]
[0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 1.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000]
[0.0000, 0.0000, 0.0000, 1.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000]
[0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 1.0000, 0.0000, 0.0000, 0.0000, 0.0000]
[0.0000, 1.0000]
[1.0000, 0.0000]
[0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 1.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000]
[0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 1.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000]
[0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 1.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000]
[0.0000, 0.0000, 0.0000, 0.0000, 1.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000]
[0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 1.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000]
[0.0000, 0.0000, 1.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000]
[0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.5000, 0.0000, 0.0000, 0.0000, 0.0000, 0.0000, 0.5000, 0.0000]

Знайдені детерміністична та стохастична функції у вигляді таблиць для 6 варіанту

Детерміністична функція:

[7, 2, 3, 13, 10, 0, 0, 0, 4, 8, 0, 0, 1, 14, 0, 12, 18, 0, 9, 0]

Стохастична функція:

0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	1.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
0.0000	0.0000	1.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
0.0000	0.0000	0.0000	1.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	1.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	1.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
0.5000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.5000
1.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
0.5000	0.0000	0.0000	0.0000	0.0000	0.0000	0.5000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
0.0000	0.0000	0.0000	0.0000	1.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	1.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
0.5000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.5000	0.0000	0.0000	0.0000
1.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
0.0000	1.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	1.0000	0.0000	0.0000	0.0000	0.0000	0.0000
1.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	1.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	1.0000	0.0000
1.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	1.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
0.5000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.5000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000

Середні втрати для вирішуючих функцій для 16 варіанту

Для детерміністичної вирішуючої функції : **0.6232000000000001**

Для стохастичної вирішуючої функції : **0.6232000000000001**

Середні втрати для вирішуючих функцій для 6 варіанту

Для детерміністичної вирішуючої функції: **0.6703999999999998**

Для стохастичної вирішуючої функції: **0.6703999999999998**

Опис труднощів, що виникали при виконанні комп'ютерного практикуму, та шляхи їх розв'язання:

Під час виконання лабораторної роботи виникли невеликі труднощі з побудовою ймовірностей та розумінням, як саме необхідно будувати стохастичну вирішуючу функцію, а також була проблема в похибці при операціях з числами з плаваючою точкою.

Порівняльний аналіз детерміністичної і стохастичної вирішуючих функцій

При виконанні даної роботи було побудовано детерміністичну і стохастичку вирішувані функції, а також було пораховано середні втрати для детермінстичної і стохастичної вирішуваних функцій. Після виконання роботи був проведений аналіз роботи цих функцій і був зроблений висновок, що обидві функції є однаково ефективними, оскільки середні втрати для обох функцій однакові.

ВИСНОВКИ

Під час роботи ми ознайомилися з принципами баєсівського підходу в криптоаналізі. Побудували детерміністичну та стохастичну вирішуючі функції, а також були пораховані середні втрати як для детерміністичної вирішуючої функції, так і для стохастичної вирішуючої функції. На основі результатів виконання роботи, було проведено аналіз заданих вирішуючих функцій і було зроблено висновок, що обидві функції є однаково ефективними.