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
Драга Владислав
Чіхладзе Вахтанг

Перевірила:
Ядуха Д. В.

Київ 2021

Мета роботи:

Ознайомлення з принципами баєсівського підходу в криптоаналізі, побудова детермінистичної 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 детермінистичної 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 репозиторію);
   (б) весь процес створення програмного коду має бути відображений у відповідних комітах проекту (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 детермінистичної 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 детермінистичної та стохастичної вирішуючих функцій зводиться до максимізації $P(M|C)$.

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

Варіант завдання: 11

Опис алгоритму побудови детерміністичної та стохастичної вирішуючих функцій

Перш за все до лабораторної роботи дано таблицю шифрування 20×20. Вона представлена таким чином: по стовпцях індексується відкритий текст, по рядках ключ; на перетині i-го рядка і j-го стовпчика міститься індекс h шифротексту, який отриманий в результаті шифрування j-го відкритого тексту на і-му ключі. Також дана таблиця з двох рядків та 20 стовпців і містить ймовірнісний розподіл відкритих текстів в першому рядку та ймовірнісний розподіл ключів в другому.

Для побудови детерміністичної функції достатньо повернути індекс максимального значення по рядку, індекс рядка відповідає індексу шифротекста, побудованої таблиці ймовірностей $P(M|C)$.

Для побудови стохастичної функції потрібно повернути один із індексів який містить максимальне значення по рядку, індекс рядка відповідає індексу шифротекста, із ймовірністю $\frac{1}{|\hat{M}|}$, де $\hat{M}$ множина індексів які містять максимальне значення в рядку.

Таблиця ймовірностей для 11 варіанту $P(M|C)$

0	0	0.08	0.08	0.04	0.18	0.14	0.04	0.08	0.04
0.2	0	0.0333333	0.0666667	0.0333333	0.0333333	0	0.0333333	0.15	0
0.494118	0.0235294	0	0	0.0235294	0.0235294	0.0470588	0.0470588	0.0235294	0
0.2	0.0333333	0.116667	0	0.0666667	0.0333333	0.0333333	0.0333333	0	0.0333333
0.342857	0.0285714	0.0285714	0	0	0.1	0	0	0.0285714	0
0.2	0	0.0666667	0.0333333	0	0	0.15	0.0333333	0.0333333	0.0666667
0	0.08	0	0.08	0	0	0	0.08	0.04	0.18
0	0.08	0	0	0	0	0.08	0	0.04	0.14
0	0.04	0.04	0.04	0.18	0.16	0.12	0.14	0	0
0.45	0.05	0.025	0	0	0.025	0.025	0.05	0	0
0.2	0.0333333	0	0	0.0333333	0.0333333	0.0333333	0.116667	0	0.0666667
0	0.04	0.14	0.08	0	0.08	0.08	0	0.04	0.04
0.2	0.0333333	0.1	0.1	0.216667	0.0333333	0	0.0333333	0	0.0333333
0.2	0.0333333	0.0666667	0	0.0666667	0.0333333	0.0333333	0.0333333	0	0.0333333
0.342857	0	0	0.0571429	0	0	0.0285714	0	0.142857	0.0571429
0.2	0.0333333	0.0666667	0.0333333	0	0.0666667	0	0	0.116667	0.0333333
0.342857	0	0	0.128571	0.0571429	0.0285714	0	0.0285714	0.0285714	0
0.2	0.15	0	0	0.0333333	0	0.0333333	0.0333333	0.0333333	0.0666667
0.568421	0.0421053	0	0	0.0210526	0.0210526	0.0210526	0.0842105	0.0210526	0.0421053
0	0.14	0.12	0.18	0.08	0	0.04	0	0.04	0.04

0.04	0.04	0	0.04	0.04	0.04	0	0.08	0	0.04
0.0666667	0.0333333	0.116667	0.0666667	0	0.0666667	0.0333333	0	0	0.0666667
0	0.0470588	0	0.0470588	0.0235294	0	0.0235294	0.0235294	0.152941	0
0.1	0	0.0333333	0.116667	0.0333333	0	0	0.0666667	0	0.1
0.0285714	0.0571429	0.0857143	0	0	0.0285714	0.1	0.0571429	0.0571429	0.0571429
0	0	0.0666667	0.0666667	0	0.183333	0.1	0	0	0
0	0	0.04	0.08	0.12	0.08	0.04	0.18	0	0
0.08	0.08	0.22	0	0	0	0.08	0.08	0.04	0.08
0	0.04	0	0.04	0	0.08	0.08	0	0.04	0
0	0.025	0	0.0875	0.075	0	0.025	0.025	0.05	0.0875
0	0.0666667	0.0333333	0.0666667	0.15	0.0666667	0.0333333	0.0333333	0.0333333	0
0.04	0	0	0.04	0.04	0.04	0.04	0.12	0	0.18
0	0.0333333	0	0.0333333	0.0333333	0.15	0	0	0	0
0	0.0333333	0	0	0.183333	0	0.0333333	0	0.216667	0.0333333
0	0.228571	0.0857143	0	0	0.0285714	0	0	0.0285714	0
0.183333	0.0333333	0.0333333	0.0333333	0.0666667	0	0	0	0	0.1
0	0.0285714	0	0.0571429	0.0285714	0.0571429	0	0.128571	0.0571429	0.0285714
0.216667	0	0.1	0	0	0	0.0333333	0	0.0333333	0.0666667
0.0421053	0	0.0210526	0	0.0210526	0	0.0947368	0	0	0
0.04	0.04	0	0.04	0	0.04	0.08	0.08	0.04	0

Таблиця ймовірностей для 6 варіанту $P(M|C)$

0	0.04	0	0.04	0	0.04	0	0.28	0.04	0.04
0	0	0.24	0.08	0	0.08	0.04	0.08	0.08	0.04
0.2	0.0333333	0	0.233333	0.0333333	0	0	0.0666667	0	0.0333333
0.2	0	0.133333	0	0.0333333	0.0666667	0	0.0666667	0.0333333	0.0333333
0	0.04	0.04	0	0	0.04	0.12	0.04	0.04	0.08
0.2	0.0333333	0	0	0	0	0.133333	0.0333333	0.0333333	0
0.45	0.025	0	0	0	0	0	0.05	0.05	0.025
0.2	0.0333333	0.0666667	0	0.0666667	0.0333333	0.2	0	0.0333333	0
0	0	0	0.04	0.32	0.04	0	0.04	0	0
0	0.08	0.04	0.04	0	0	0.16	0	0.32	0
0.2	0.1	0	0.0666667	0.0666667	0.1	0.0333333	0.0333333	0.0333333	0
0.45	0	0.05	0.05	0.075	0	0.05	0	0	0.05
0.2	0.3	0	0.0333333	0	0.0333333	0	0	0.0333333	0.0333333
0.2	0.0333333	0	0.0333333	0.1	0.0333333	0	0.0333333	0	0
0.654545	0	0.0181818	0.0363636	0	0	0	0.0363636	0.0181818	0.0363636
0.2	0	0.0666667	0	0.1	0.0333333	0.0333333	0.0666667	0.0333333	0
0	0.04	0.04	0.04	0	0	0.04	0	0.12	0.08
0.45	0	0	0.025	0	0.2	0	0	0.025	0.05
0.2	0.0666667	0.1	0.0333333	0	0.0333333	0.0666667	0	0	0.266667
0.2	0.0333333	0.0666667	0.0666667	0.0666667	0.0666667	0	0.0333333	0	0.0333333

0.04	0.08	0.04	0.08	0.04	0.04	0.04	0	0.08	0.08
0	0	0	0	0.04	0.16	0.08	0.04	0	0.04
0	0.0333333	0.1	0.1	0.0333333	0.0666667	0	0	0.0333333	0.0333333
0.0333333	0	0	0.233333	0.0333333	0	0	0.1	0.0333333	0
0.36	0	0.08	0	0	0	0	0.12	0.04	0
0	0.0333333	0.0333333	0	0.0666667	0.0666667	0	0.0333333	0.133333	0.2
0	0.025	0.025	0	0.05	0.025	0.1	0.15	0	0.025
0.0666667	0.0333333	0.0333333	0	0.0333333	0	0.0333333	0.0333333	0.0666667	0.0666667
0.04	0.04	0.04	0.04	0.12	0.08	0.04	0.08	0	0.08
0	0.08	0	0.16	0.04	0.04	0	0	0	0.04
0	0.0333333	0	0.0333333	0	0.2	0	0.0333333	0	0.0666667
0	0	0.025	0.025	0	0.025	0.175	0	0	0.025
0.0666667	0.0333333	0	0.0333333	0	0.0333333	0.0333333	0.1	0.0333333	0.0333333
0	0.0666667	0.0666667	0	0.266667	0.0333333	0.0666667	0	0	0.0666667
0.0181818	0.0181818	0	0.0363636	0	0	0.0363636	0.0363636	0.0363636	0.0181818
0.0666667	0.0333333	0.233333	0.0666667	0	0	0.0333333	0	0.0333333	0
0.08	0	0.04	0	0.08	0	0	0.04	0.32	0.08
0.025	0.05	0.05	0	0.025	0.05	0	0	0.05	0
0.0666667	0.0666667	0.0333333	0	0	0	0.0666667	0	0	0
0.0333333	0.2	0.0333333	0.0333333	0.0333333	0.0333333	0.0333333	0.0333333	0	0

Знайдені детерміністична та стохастична функції у вигляді таблиць для 11 варіанту

Детерміністична функція:

$$\begin{vmatrix}
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{vmatrix}$$

Стохастична функція:

$$\begin{vmatrix}
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.5 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{vmatrix}$$

Знайдені детерміністична та стохастична функції у вигляді таблиць для 6 варіанту

Детерміністична функція:

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	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	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
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	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	1	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	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	1	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	1	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	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

Стохастична функція:

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	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	1	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
0.5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.5
1	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	0.5	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	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
0.5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.5	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	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	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	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	1	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	1	0	0	0	0	0	0	0	0	0
0.5	0	0	0	0	0	0	0	0	0	0	0	0.5	0	0	0	0	0	0	0

Середні втрати для вирішуючих функцій для 11 варіанту

Average bayes loss function: 0.7128
Average stochastic loss function: 0.7128

Середні втрати для вирішуючих функцій для 6 варіанту

Average bayes loss function: 0.6704
Average stochastic loss function: 0.6704

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

У ході данної роботи перш за все виникли труднощі з розумінням теорії, але після медетуванням над методичними та лекційними матеріалами стало зрозуміло що вимагається в завданні. Також виникали труднощі із компіляцією та сумісністю написаної програми на мові програмування на C++ з середовища Windows з використанням wsl2 у середовище MacOS. Вирішилось написанням написанням ініціалізаційного bash-скрипта, що будує ієрархію проекту.

Висновок:

Отже, в даній роботі ми ознайомились з принципами баєсівського підходу в криптоаналізі. Навчились будувати та реалізовувати детерміністичну та стохастичну вирішуючу функцію для моделей схем шифрування. Також було зроблено порівняльну характеристику відносно вирішуючих функцій.