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

Звіт за темою:

"БАЄСІВСЬКИЙ ПІДХІД В КРИПТОАНАЛІЗІ: ПОБУДОВА І ДОСЛІДЖЕННЯ ДЕТЕРМІНІСТИЧНОЇ ТА СТОХАСТИЧНОЇ ВИРІШУЮЧИХ ФУНКЦІЙ"

Виконали:
студенти групи ФІ-32мн
Баєвський Констянтин,
Шифрін Денис

Київ — 2023

ЗМІСТ

1 Мета практикуму

Ознайомитися з принципами баєсівського підходу в криптоаналізі, побудувати детерміністичну та стохастичну вирішуючі функції для заданих розподілів за допомогою програмної реалізації.

1. 1 Постановка задачі та варіант завдання

Варіант №2

Треба виконати	**Зроблено**
Опис алгоритмів побудови	✓
Обчислення таблиці ймовірностей $P(M\|C)$	✓
Вивід детерміністичної та стохастичної функцій	✓
Обчислення середніх втрат для вирішуючих функцій	✓

2 Хід роботи та опис труднощів

Для роботи з таблицями та написанням функцій для отримання розподілу шифротекстів, сумісного розподілу відкритих текстів та шифротекстів було обрано використовувати мову C#.

В результаті було отримано відповідні таблиці ймовірностей, які використовувались безпосередньо для побудови детерміністичної та стохастичної функцій, а також було знайдено значення середніх витрат побудованих функцій.

При виконанні практикуму виникли невеликі труднощі з форматом завантажуваних даних безпосередньо у код, через що було прийнято рішення перезаписати ці дані у вигляді масивів даних для зручності.

3 Результати дослідження

В результаті проробленої роботи було визначено, що детерміністична та стохастична функції вийшли різними, при цьому значення обох середніх похибок у відповідних функціях вийшли однаковими. Таким чином, отримали, що обидві функції досить добре підходять для нашого розподілу.

3. 1 Опис алгоритмів побудови вирішуючих функцій

Алгоритми побудови вирішуючих функцій схожі між собою і безпосередньо відрізняються лише останнім кроком.

Наведемо алгоритми для обчислення детерміністичної та стохастичної функцій:

Алгоритм 0.1. Побудова детерміністичної вирішуючої функції.

– Обчислюємо $P(C)$ за формулою:$\forall C : P(C) = \sum_{(M,k):E_k(M)=C} P(M,k)$.

– Обчислюємо $P(C)$ за формулою: $\forall (M,C) : P(M,C) = \sum_{k:E_k(M)=C} P(M,k)$.

– Обчислюємо $P(M|C)$ за формулою $\frac{P(M,C)}{P(C)}$.

– З отриманих значень треба обрати максимальні та присвоїти значення 1 до комірок матриці, де містилось дане максимальне значення.

Алгоритм 0.2. Побудова стохастичної вирішуючої функції.

– Обчислюємо $P(C)$ за формулою:$\forall C : P(C) = \sum_{(M,k):E_k(M)=C} P(M,k)$.

– Обчислюємо $P(C)$ за формулою: $\forall (M,C) : P(M,C) = \sum_{k:E_k(M)=C} P(M,k)$.

– Обчислюємо $P(M|C)$ за формулою $\frac{P(M,C)}{P(C)}$.

– З отриманих значень треба обрати максимальні та присвоїти значення $\frac{1}{s}$ до тих комірок матриці, де дане максимальне значення повторюється у рядку s разів.

3. 2 Таблиця ймовірностей $P(M|C)$

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
0	0.0	0.155556	0.0	0.28	0.0	0.28	0.14	0.0	0.155556	0.0	0.127273	0.381818	0.155556	0.107692	0.0	0.127273	0.381818	0.28	0.0	0.155556
1	0.28	0.0	0.155556	0.0	0.28	0.0	0.14	0.28	0.0	0.28	0.254545	0.0	0.0	0.430769	0.0	0.254545	0.0	0.0	0.28	0.0
2	0.08	0.044444	0.0	0.04	0.0	0.08	0.04	0.04	0.088889	0.0	0.0	0.036364	0.0	0.030769	0.0	0.072727	0.0	0.16	0.0	0.088889
3	0.0	0.0	0.044444	0.0	0.04	0.04	0.04	0.04	0.044444	0.0	0.036364	0.072727	0.133333	0.030769	0.05	0.036364	0.072727	0.0	0.04	0.088889
4	0.16	0.0	0.133333	0.08	0.0	0.04	0.0	0.0	0.0	0.16	0.036364	0.0	0.044444	0.0	0.05	0.0	0.036364	0.04	0.04	0.0
5	0.0	0.177778	0.044444	0.0	0.04	0.0	0.0	0.04	0.0	0.12	0.072727	0.109091	0.044444	0.030769	0.1	0.0	0.0	0.04	0.0	0.0
6	0.0	0.044444	0.088889	0.04	0.08	0.04	0.0	0.04	0.133333	0.04	0.036364	0.0	0.044444	0.0	0.05	0.0	0.0	0.04	0.08	0.088889
7	0.0	0.088889	0.044444	0.0	0.08	0.0	0.0	0.0	0.0	0.04	0.109091	0.072727	0.0	0.030769	0.1	0.0	0.036364	0.12	0.0	0.088889
8	0.04	0.0	0.088889	0.12	0.0	0.04	0.0	0.08	0.0	0.08	0.072727	0.0	0.088889	0.0	0.05	0.036364	0.036364	0.04	0.0	0.044444
9	0.0	0.088889	0.0	0.04	0.0	0.04	0.08	0.08	0.0	0.0	0.036364	0.036364	0.088889	0.030769	0.1	0.109091	0.0	0.0	0.08	0.0
10	0.04	0.133333	0.0	0.08	0.04	0.08	0.0	0.04	0.0	0.0	0.0	0.036364	0.0	0.0	0.1	0.036364	0.036364	0.04	0.12	0.044444
11	0.0	0.044444	0.044444	0.0	0.04	0.04	0.08	0.04	0.133333	0.08	0.036364	0.0	0.088889	0.030769	0.0	0.0	0.072727	0.0	0.04	0.044444
12	0.0	0.044444	0.044444	0.04	0.0	0.08	0.08	0.0	0.044444	0.0	0.0	0.0	0.0	0.061538	0.0	0.072727	0.109091	0.08	0.08	0.044444
13	0.0	0.0	0.044444	0.08	0.08	0.08	0.0	0.0	0.133333	0.04	0.072727	0.036364	0.088889	0.0	0.05	0.0	0.0	0.04	0.08	0.0
14	0.2	0.044444	0.0	0.0	0.04	0.0	0.2	0.04	0.044444	0.0	0.0	0.036364	0.0	0.030769	0.0	0.072727	0.0	0.04	0.04	0.0
15	0.04	0.044444	0.177778	0.0	0.0	0.0	0.04	0.04	0.0	0.04	0.036364	0.036364	0.088889	0.030769	0.05	0.0	0.0	0.0	0.08	0.133333
16	0.0	0.044444	0.088889	0.04	0.04	0.08	0.12	0.0	0.044444	0.04	0.036364	0.072727	0.088889	0.030769	0.0	0.036364	0.0	0.04	0.0	0.0
17	0.04	0.044444	0.0	0.08	0.04	0.04	0.04	0.0	0.044444	0.04	0.036364	0.0	0.0	0.061538	0.1	0.0	0.072727	0.0	0.04	0.133333
18	0.04	0.0	0.0	0.0	0.12	0.04	0.0	0.16	0.088889	0.0	0.0	0.0	0.044444	0.030769	0.05	0.072727	0.109091	0.0	0.0	0.044444
19	0.08	0.0	0.0	0.08	0.08	0.0	0.0	0.08	0.044444	0.04	0.0	0.072727	0.0	0.030769	0.15	0.072727	0.036364	0.04	0.0	0.0

Рисунок 1 – Таблиця умовних ймовірностей для обчислення вирішуючих функцій.

3. 3 Детерміністична та стохастична матриці

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
Ciphertexts	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
Messages	1	5	15	0	1	0	14	1	0	1	1	0	0	1	19	1	0	0	1	0

Рисунок 2 – Детерміністична вирішуюча ф-я у вигляді відображень (ШТ→ВТ).

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
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	1.0	0	0	0	0	0	0	0	0	0.0	0.0	0	0	0	0.0
2	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
3	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
4	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
5	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
6	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
7	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
8	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
9	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
10	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
11	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
12	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
13	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
14	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
15	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
16	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
17	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
18	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
19	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

Рисунок 3 – Стохастична вирішуюча функція.

Також було отримано наступні середні значення втрат:

– Для детерміністичної функції: 0.737

– Для стохастичної функції: 0.737.

4 Висновки

В даному практикумі за допомогою програмної реалізації практично ознайомилися з баєсівським підходом в криптоаналізі, проаналізували та описали побудову алгоритмів. Також за допомогою програмної реалізації побудували детерміністичну та стохастичну функції для заданих розподілів.