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

Звіт за темою:
«Баєсівський підхід в криптоаналізі: побудова і дослідження детерміністичної та стохастичної вирішуючих функцій»

Виконали студенти
групи ФІ-32мн
Кріпака Ілля,
Шашенок Микита

Київ — 2023

1 Мета практикуму

Практично ознайомитися із принципами баєсівського підходу в криптоаналізі,та безпосерденьо побудувати детерміністичну та стохастичну матриці для заданих розподілів.

1.1 Постановка задачі та варіант

Треба виконати	**Зроблено**
Описати побудову алгоритму	✓
Порахувати таблицю ймовірностей $P(M\|C)$	✓
Показати детермінитичну та стохастичну функції	✓
Порахувати середні витрати для вирішуючих функцій	✓

2 Хід роботи/Опис труднощів

Для виконанння лабораторної роботи була обрана мова програмування Python та бібліотека для роботи з таблицями Pandas, написані функції для отримання розподілу шифротекстів та сумісного розподілу відкритих текстів та шифротекстів.

З цього було отримано відповідні таблиці ймовірностей, яких вже були побудовані детерміністичну та стохастичні функції, а також обраховані середні втрати.

Під час виконання роботи виникли труднощі з певною невідповідністю формату даних при їх завантаженні у код, тому на початку було застосовано деякий препроцесінг з вхідними даними та отримано зручні для роботи таблиці.

3 Результати дослідження

У ході роботи було визначено, що детерміністична та стохастична вийшли однаковими, але було серденє значення похибки у обох функцій вийшли різними. У результаті отримали, що детерміністична функція є кращою для нашого варіанту.

3.1 Опис алгоритму

Для побудови детерміністичної функції та стохастичних функцій наведемо наступний алгоритм.

Зауваження. Одразу зазанчимо, що алгоритми подібні та відрізняються лише у останньому кроці. Для послідовності опису наведемо повні кроки.

Алгоритм .1. 1. Алгоритм із побудови детерміністичної вирішуючої функції.

- Обчислюємо $P(C)$ за формулою: $\forall C : P(C) = \sum_{(M,k):E_k(M)=C} P(M,k)$.
- Обчислюємо $P(M,C)$ за формулою: $\forall (M,C) : P(M,C) = \sum_{k:E_k(M)=C} P(M,k)$.
- Обчислюємо $P(C|M)$ за формулою $\dfrac{P(M,C)}{P(C)}$.
- Із обчислених значень умовних ймовірностей вибираємо максимальні значення. Та присвоюємо 1 до тих комірок у матриці де зустріли його.

2. Алгоритм із побудови стохастичної вирішуючої функції.

   - Обчислюємо $P(C)$ за формулою: $\forall C : P(C) = \sum_{(M,k):E_k(M)=C} P(M,k)$.
   - Обчислюємо $P(M,C)$ за формулою: $\forall (M,C) : P(M,C) = \sum_{k:E_k(M)=C} P(M,k)$.
   - Обчислюємо $P(C|M)$ за формулою $\dfrac{P(M,C)}{P(C)}$.
   - Із обчислених значень умовних ймовірностей вибираємо макимальні значення. Та у тих рядках, де максимальне значення повторюється s разів присвоюємо коміркам значення $\dfrac{1}{s}$.

3.2 Таблиця ймовірностей

Таблиця ймовірностей набула наступної форми.

÷	0 ÷	1 ÷	2 ÷	3 ÷	4 ÷	5 ÷	6 ÷	7 ÷	8 ÷	9 ÷	10 ÷	11 ÷	12 ÷	13 ÷	14 ÷	15 ÷	16 ÷	17 ÷	18 ÷	19 ÷
0	0.000000	0.004500	0.004500	0.004500	0.00000	0.000000	0.000000	0.000000	0.004500	0.004500	0.00000	0.013500	0.013500	0.009000	0.000000	0.009000	0.009000	0.00900	0.000000	0.004500
1	0.000000	0.000000	0.013650	0.009100	0.01820	0.004550	0.000000	0.004550	0.004550	0.004550	0.00910	0.004550	0.004550	0.000000	0.000000	0.004550	0.004550	0.00000	0.000000	0.004550
2	0.004600	0.009200	0.000000	0.004600	0.00000	0.000000	0.018400	0.000000	0.004600	0.000000	0.00920	0.000000	0.004600	0.009200	0.004600	0.000000	0.004600	0.00920	0.004600	0.004600
3	0.000000	0.000000	0.004650	0.000000	0.00465	0.004650	0.004650	0.023250	0.004650	0.000000	0.00465	0.000000	0.004650	0.000000	0.000000	0.013950	0.004650	0.00465	0.004650	0.009300
4	0.004000	0.004000	0.002000	0.000000	0.00000	0.002000	0.004000	0.002000	0.002000	0.002000	0.00200	0.002000	0.004000	0.002000	0.000000	0.002000	0.000000	0.00000	0.006000	0.000000
5	0.002050	0.000000	0.006150	0.000000	0.00000	0.000000	0.006150	0.000000	0.004100	0.002050	0.00410	0.002050	0.000000	0.002050	0.004100	0.002050	0.004100	0.00000	0.000000	0.002050
6	0.004200	0.002100	0.002100	0.002100	0.00000	0.000000	0.000000	0.004200	0.002100	0.008400	0.00210	0.000000	0.000000	0.000000	0.004200	0.002100	0.002100	0.00210	0.002100	0.002100
7	0.002150	0.006450	0.002150	0.004300	0.00000	0.000000	0.002150	0.000000	0.002150	0.002150	0.00000	0.002150	0.000000	0.004300	0.002150	0.008600	0.002150	0.00000	0.002150	0.000000
8	0.000000	0.000000	0.002200	0.000000	0.00660	0.000000	0.002200	0.002200	0.000000	0.002200	0.00440	0.002200	0.002200	0.006600	0.002200	0.002200	0.000000	0.00440	0.002200	0.002200
9	0.002250	0.000000	0.002250	0.004500	0.00225	0.002250	0.004500	0.000000	0.002250	0.000000	0.00225	0.000000	0.002250	0.004500	0.004500	0.000000	0.004500	0.00450	0.000000	0.002250
10	0.000000	0.004600	0.000000	0.002300	0.00460	0.006900	0.002300	0.002300	0.002300	0.004600	0.00000	0.000000	0.002300	0.000000	0.002300	0.004600	0.002300	0.00230	0.000000	0.002300
11	0.000000	0.007050	0.004700	0.004700	0.00705	0.000000	0.000000	0.002350	0.000000	0.002350	0.00470	0.000000	0.002350	0.000000	0.002350	0.000000	0.000000	0.00235	0.004700	0.002350
12	0.002400	0.004800	0.000000	0.004800	0.00480	0.004800	0.000000	0.002400	0.002400	0.000000	0.00240	0.002400	0.000000	0.000000	0.000000	0.000000	0.002400	0.00720	0.000000	0.007200
13	0.002450	0.002450	0.000000	0.000000	0.00000	0.007350	0.002450	0.004900	0.000000	0.000000	0.00490	0.007350	0.000000	0.000000	0.002450	0.004900	0.000000	0.00000	0.007350	0.002450
14	0.004100	0.000000	0.002050	0.000000	0.00205	0.002050	0.002050	0.002050	0.000000	0.000000	0.00205	0.010250	0.004100	0.000000	0.000000	0.000000	0.006150	0.00205	0.002050	0.000000
15	0.002055	0.002055	0.000000	0.004110	0.00000	0.002055	0.002055	0.002055	0.004110	0.000000	0.00000	0.002055	0.006165	0.002055	0.000000	0.000000	0.002055	0.00411	0.002055	0.004110
16	0.004120	0.002060	0.000000	0.004120	0.00412	0.000000	0.002060	0.000000	0.004120	0.002060	0.00412	0.000000	0.000000	0.002060	0.006180	0.000000	0.000000	0.00000	0.004120	0.002060
17	0.006195	0.000000	0.002065	0.002065	0.00000	0.002065	0.000000	0.002065	0.004130	0.004130	0.00000	0.002065	0.000000	0.006195	0.002065	0.000000	0.004130	0.00000	0.002065	0.002065
18	0.002070	0.002070	0.004140	0.002070	0.00207	0.006210	0.002070	0.004140	0.002070	0.002070	0.00000	0.000000	0.002070	0.004140	0.000000	0.002070	0.002070	0.00000	0.000000	0.002070
19	0.002075	0.000000	0.002075	0.000000	0.00000	0.004150	0.000000	0.000000	0.002075	0.006225	0.00000	0.002075	0.004150	0.000000	0.008300	0.002075	0.000000	0.00415	0.004150	0.000000

Рис. 1: Таблиця умовних ймовірностей для обчислення вирішуючих функцій.

3.3 Детерміністична та стохастична матриці

У ході обчислень було отримано наступні функції.

÷	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	17	2	1	1	1	13	2	3	3	6	2	0	0	2	19	3	0	2	13	3

Рис. 2: Детерміністична вирішуюча функція зображена у формі відображень. (ШТ → ВТ)

Також серденє значення втрат вийшло таким:

- Для детерміністичної вирішуючої функції значення втрат становить: 0.8376049.
- Для стохастичної вирішуючої функції значення втрат становить: 0.936809.

#	M0	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12	M13	M14	M15	M16	M17	M18	M19
C0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
C1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
C2	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
C3	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
C4	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
C5	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
C6	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
C7	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
C8	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
C9	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
C10	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
C11	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
C12	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
C13	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
C14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
C15	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
C16	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
C17	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
C18	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
C19	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Рис. 3: Стохастична вирішуюча функція.

4 Висновки

За допомогою реалізації практикуму "Баєсівський підхід в криптоаналізі: побудова і дослідження детерміністичної та стохастичної вирішуючих функцій" дізналися на практиці як повинен відбуватися баєсівський підхід у криптоаналізі. Також були долучені до створення такого собі «маленького» прикладу із побудови вирішуючих функцій для заданого розподілу повідомлень.