

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

Звіт за темою:  
«Дослідження алгоритмів реалізації арифметичних  
операцій над великими числами»

Виконали студенти  
групи ФІ-32мн  
Баєвський Константин,  
Шифрін Денис,  
Кріпака Ілля

Київ — 2023

# 1 Мета практикуму

Практично ознайомитися із принципами баєсівського підходу в криптоаналізі, та безпосередньо 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 детерміністичну та стохастичну функції   | ✓        |
| Порахувати середні витрати для вирішуючих функцій | ✓        |

## 2 Хід роботи/Опис труднощів

Для виконання 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 визначили, що детерміністична та стохастична вийшли не однаковими, але обоє значень середньої похибки у обох функцій вийшли однаковими. У результаті отримали, що ніякій із функцій надати перевагу не можемо, вони обоє добре підходять для нашого розподілу.

### 3.1 Опис алгоритму

Для побудови детерміністичної функції та стохастичних функцій наведемо наступний алгоритм.

**Зауваження.** Одразу зазначимо, 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  $P(M|C)$  за формулою  $\frac{P(M, C)}{P(C)}$ .
- 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  $P(M|C)$  за формулою  $\frac{P(M, C)}{P(C)}$ .
- Із обчислених значень умовних ймовірностей вибираємо максимальні значення. Та у тих рядках, де максимальне значення повторюється  $s$  разів присвоюємо коміркам значення  $\frac{1}{s}$ .

## 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  | 0.0      | 0.094737 | 0.085714 | 0.09 | 0.0      | 0.0      | 0.0      | 0.0      | 0.09 | 0.1      | 0.0      | 0.27 | 0.245455 | 0.18 | 0.0      | 0.163636 | 0.171429 | 0.171429 | 0.0      | 0.085714 |
| 1  | 0.0      | 0.0      | 0.257143 | 0.18 | 0.342857 | 0.1      | 0.0      | 0.081818 | 0.09 | 0.1      | 0.171429 | 0.09 | 0.081818 | 0.0  | 0.0      | 0.081818 | 0.085714 | 0.0      | 0.0      | 0.085714 |
| 2  | 0.105882 | 0.189474 | 0.0      | 0.09 | 0.0      | 0.0      | 0.342857 | 0.0      | 0.09 | 0.0      | 0.171429 | 0.0  | 0.081818 | 0.18 | 0.105882 | 0.0      | 0.085714 | 0.171429 | 0.1      | 0.085714 |
| 3  | 0.0      | 0.0      | 0.085714 | 0.0  | 0.085714 | 0.1      | 0.085714 | 0.409091 | 0.09 | 0.0      | 0.085714 | 0.0  | 0.081818 | 0.0  | 0.0      | 0.245455 | 0.085714 | 0.085714 | 0.1      | 0.171429 |
| 4  | 0.094118 | 0.084211 | 0.038095 | 0.0  | 0.0      | 0.044444 | 0.07619  | 0.036364 | 0.04 | 0.044444 | 0.038095 | 0.04 | 0.072727 | 0.04 | 0.0      | 0.036364 | 0.0      | 0.0      | 0.133333 | 0.0      |
| 5  | 0.047059 | 0.0      | 0.114286 | 0.0  | 0.0      | 0.0      | 0.114286 | 0.0      | 0.08 | 0.044444 | 0.07619  | 0.04 | 0.0      | 0.04 | 0.094118 | 0.036364 | 0.07619  | 0.0      | 0.0      | 0.038095 |
| 6  | 0.094118 | 0.042105 | 0.038095 | 0.04 | 0.0      | 0.0      | 0.0      | 0.072727 | 0.04 | 0.177778 | 0.038095 | 0.0  | 0.0      | 0.0  | 0.094118 | 0.036364 | 0.038095 | 0.038095 | 0.044444 | 0.038095 |
| 7  | 0.047059 | 0.126316 | 0.038095 | 0.08 | 0.0      | 0.0      | 0.038095 | 0.0      | 0.04 | 0.044444 | 0.0      | 0.04 | 0.0      | 0.08 | 0.047059 | 0.145455 | 0.038095 | 0.0      | 0.044444 | 0.0      |
| 8  | 0.0      | 0.0      | 0.038095 | 0.0  | 0.114286 | 0.0      | 0.038095 | 0.036364 | 0.0  | 0.044444 | 0.07619  | 0.04 | 0.036364 | 0.12 | 0.047059 | 0.036364 | 0.0      | 0.07619  | 0.044444 | 0.038095 |
| 9  | 0.047059 | 0.0      | 0.038095 | 0.08 | 0.038095 | 0.044444 | 0.07619  | 0.0      | 0.04 | 0.0      | 0.038095 | 0.0  | 0.036364 | 0.08 | 0.094118 | 0.0      | 0.07619  | 0.07619  | 0.0      | 0.038095 |
| 10 | 0.0      | 0.084211 | 0.0      | 0.04 | 0.07619  | 0.133333 | 0.038095 | 0.036364 | 0.04 | 0.088889 | 0.0      | 0.0  | 0.036364 | 0.0  | 0.047059 | 0.072727 | 0.038095 | 0.038095 | 0.0      | 0.038095 |
| 11 | 0.0      | 0.126316 | 0.07619  | 0.08 | 0.114286 | 0.0      | 0.0      | 0.036364 | 0.0  | 0.044444 | 0.07619  | 0.0  | 0.036364 | 0.0  | 0.047059 | 0.0      | 0.0      | 0.038095 | 0.088889 | 0.038095 |
| 12 | 0.047059 | 0.084211 | 0.0      | 0.08 | 0.07619  | 0.088889 | 0.0      | 0.036364 | 0.04 | 0.0      | 0.038095 | 0.04 | 0.0      | 0.0  | 0.0      | 0.038095 | 0.114286 | 0.0      | 0.114286 | 0.0      |
| 13 | 0.047059 | 0.042105 | 0.0      | 0.0  | 0.0      | 0.133333 | 0.038095 | 0.072727 | 0.0  | 0.0      | 0.07619  | 0.12 | 0.0      | 0.0  | 0.047059 | 0.072727 | 0.0      | 0.0      | 0.133333 | 0.038095 |
| 14 | 0.094118 | 0.0      | 0.038095 | 0.0  | 0.038095 | 0.044444 | 0.038095 | 0.036364 | 0.0  | 0.0      | 0.038095 | 0.2  | 0.072727 | 0.0  | 0.0      | 0.0      | 0.114286 | 0.038095 | 0.044444 | 0.0      |
| 15 | 0.047059 | 0.042105 | 0.0      | 0.08 | 0.0      | 0.044444 | 0.038095 | 0.036364 | 0.08 | 0.0      | 0.0      | 0.04 | 0.109091 | 0.04 | 0.0      | 0.0      | 0.038095 | 0.07619  | 0.044444 | 0.07619  |
| 16 | 0.094118 | 0.042105 | 0.0      | 0.08 | 0.07619  | 0.0      | 0.038095 | 0.0      | 0.08 | 0.044444 | 0.07619  | 0.0  | 0.0      | 0.04 | 0.141176 | 0.0      | 0.0      | 0.0      | 0.088889 | 0.038095 |
| 17 | 0.141176 | 0.0      | 0.038095 | 0.04 | 0.0      | 0.044444 | 0.0      | 0.036364 | 0.08 | 0.088889 | 0.0      | 0.04 | 0.0      | 0.12 | 0.047059 | 0.0      | 0.07619  | 0.0      | 0.044444 | 0.038095 |
| 18 | 0.047059 | 0.042105 | 0.07619  | 0.04 | 0.038095 | 0.133333 | 0.038095 | 0.072727 | 0.04 | 0.044444 | 0.0      | 0.0  | 0.036364 | 0.08 | 0.0      | 0.036364 | 0.038095 | 0.0      | 0.0      | 0.038095 |
| 19 | 0.047059 | 0.0      | 0.038095 | 0.0  | 0.0      | 0.088889 | 0.0      | 0.0      | 0.04 | 0.133333 | 0.0      | 0.04 | 0.072727 | 0.0  | 0.188235 | 0.036364 | 0.0      | 0.07619  | 0.088889 | 0.0      |

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

## 3.3 Детерміністична та стохастична матриці

У ході обчислень було отримано наступні функції.

|               | C1 ÷ | C2 ÷ | C3 ÷ | C4 ÷ | C5 ÷ | C6 ÷ | C7 ÷ | C8 ÷ | C9 ÷ | C10 ÷ | C11 ÷ | C12 ÷ | C13 ÷ | C14 ÷ | C15 ÷ | C16 ÷ | C17 ÷ | C18 ÷ | C19 ÷ | C20 ÷ | C21 ÷ |
|---------------|------|------|------|------|------|------|------|------|------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|
| 1 Ciphertexts |      | 0    | 1    | 2    | 3    | 4    | 5    | 6    | 7    | 8     | 9     | 10    | 11    | 12    | 13    | 14    | 15    | 16    | 17    | 18    | 19    |
| 2 Messages    |      | 17   | 2    | 1    | 1    | 1    | 10   | 2    | 3    | 0     | 6     | 1     | 0     | 0     | 0     | 19    | 3     | 0     | 0     | 4     | 3     |

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

Також сердене значення втрат вийшло таким:

- Для детерміністичної вирішуючої функції значення втрат становить: 0.786.
- Для стохастичної вирішуючої функції значення втрат становить: 0.78599.

| #   | 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  | 0.33 | 0   | 0   | 0.33 | 0   | 0   | 0   | 0   | 0.33 | 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  | 0.25 | 0.25 | 0.25 | 0.25 | 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    | 0.5  | 0.5  | 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 | 0.5  | 0    | 0.5  | 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 | 0.5  | 0    | 0.5  | 0    | 0   | 0  | 0  | 0  | 0  | 0  | 0    | 0   | 0   | 0    | 0   | 0   | 0   | 0   | 0    | 0   |
| C18 | 0    | 0    | 0    | 0    | 0.5 | 0  | 0  | 0  | 0  | 0  | 0    | 0   | 0   | 0.5  | 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.