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

Комп'ютерний практикум №1

з курсу методи криптоаналізу

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

Виконав студент
групи ФІ-42мн
Бєш Радомир Андрійович

Київ — 2024

# ВСТУП

**Мета:** 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.

**Постановка задачі**: реалізувати алгоритми програмно для варіанту №18 і подати результати побудови детерміністичної та стохастичної вирішуючих функцій у вигляді таблиць. Для цього необхідно:

1) порахувати розподіли $P(C)$ та $P(M, C)$;

2) ґрунтуючись на цих розподілах обчислити $P(M|C)$;

3) побудувати оптимальні детерміністичну та стохастичну вирішуючі функції;

4) обчислити середні втрати.

**Результати дослідження:**
https://github.com/Radomir21/2024-Cryptanalysis.

# 1 ХІД РОБОТИ

**Алгоритм 1.1** (**Детерміністична вирішуюча функція**).
Вхід: умовний розподіл $P(M|C)$.

Вихід: детерміністична вирішуюча функція $\delta_D$.

1) Знаходимо розподіл $P(C)$ за формулою:

$$P_C(c) = \sum_{i=1}^{M} \sum_{j=1}^{K} P_M(i) \cdot P_K(j) \cdot \mathbb{1}\{E(j,i) = c\} \tag{1.1}$$

2) Знаходимо розподіл $P(M, C)$ за формулою:

$$P_{M,C}(i,c) = \sum_{j} P_M(i) \cdot P_K(j) \cdot \mathbb{1}\{E(j,i) = c\} \tag{1.2}$$

3) Знаходимо умовний розподіл $P(M|C)$ за формулою:

$$P(M|C=c) = \frac{P(M, C=c)}{P(C=c)}, \quad \text{якщо } P(C=c) > 0 \tag{1.3}$$

4) Знаходимо детерміністичну функцію за формулою:

$$\delta_i = \arg\max_j \big(P(M_j|C=c_i)\big) \tag{1.4}$$

**Алгоритм 1.2** (**Стохастична вирішуюча функція**).
Вхід: $P(M)$, $P(C|M)$.

Вихід: стохастична матриця $\delta_S^n$.

1) Знаходимо матрицю без максимізації.

$$\texttt{matrix}_{i,j} = \begin{cases} P(C|M)_{i,j}, & \text{якщо } P(C|M)_{i,j} \geqslant \max(P(C|M)_i) \\ 0, & \text{інакше} \end{cases}$$

2) Обчислюємо суми ймовірностей для ненульових значень.

3) Максимізуємо щоб при кожному ненульовому значенні $\delta_S(C, M)$

ймовірність $P(M|C)$ була максимальною.

Таблиця ймовірностей і детерміністична та стохастична функції у вигляді таблиць знаходиться у файлі `results.txt` в репозиторії https://github.com/Radomir21/2024-Cryptanalysis.

**Середні втрати для вирішуючих функцій** становили $\delta_D$=0.5303999999999999 та $\delta_S$=0.5304 , тобто дали однакові значення.

**Опис труднощів, що виникли**. Великих труднощів з програмної реалізації не було, хоча вже на прикінці я зрозумів, що дану лабораторну роботу можна було зробити за декілька рядків коду, використовуючи всю силу `numpy` в пайтоні, як це я зробив для знаходження стохастичної матриці та функції втрат для стохастичної вирішуючої функції. Проте найбільша проблема для мене стала представлення результатів в цьому звіті. Я так і не знайшов гарного способу представити результати в LaTex, тому всі матриці знаходяться у репозиторію у файлі `results.txt`.

# ВИСНОВКИ

В ході виконання комп'ютерного практикуму було розглянуто принципи баєсівського підходу в криптоаналізі, побудова детерміністичної та стохастичної вирішуючих функцій для моделей схем шифрування та криптоаналіз моделей шифрів за допомогою програмної реалізації на `python`, також здійснення порівняльного аналізу вирішуючих функцій. Середні втрати детерміністичної і стохастичної вирішуючих функцій для варінату №18 показали однаковий результат, а саме 0.5304.