

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені Ігоря СІКОРСЬКОГО»
Навчально-науковий фізико-технічний інститут
Кафедра математичних методів захисту інформації**

**Звіт до
комп'ютерного практикуму №1**

Оформлення звіту:
Дигас Богдан, ФІ-52мн
Юрчук Олексій, ФІ-52мн

17 вересня 2025 р.
м. Київ

Комп'ютерний практикум № 1

1.1 Вступні відомості

Мета роботи: 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:

1. Створіть репозиторій у системі контролю версій Git/GitHub;
2. Реалізуйте алгоритми програмно та представите результати побудови детермінованих та стохастичних вирішальних функцій у вигляді таблиць. Для цього необхідно:
 - (а) обчислити розподіли $P(C)$ та $P(M, C)$;
 - (б) на основі цих розподілів обчислити $P(M|C)$;
 - (в) побудова оптимальних детермінованих та стохастичних вирішальних функцій зводиться до максимізації $P(M|C)$.
3. Розрахуйте середні втрати, проведіть порівняльний аналіз функцій прийняття рішень.
4. Підготувати звіт для комп'ютерного практикуму.

1.2 Результати виконання роботи. Варіант 15

```
=== PROBABILITY DATA ===
Opened text probability: 0.11 0.11 0.11 0.11 0.11 0.03 0.03 0.03 0.03 0.03 0.03 0.03 0.03 0.03 0.03 0.03 0.03 0.03 0.03
Secret keys probability: 0.14 0.14 0.04 0.04 0.04 0.04 0.04 0.04 0.04 0.04 0.04 0.04 0.04 0.04 0.04 0.04 0.04 0.04 0.04
=== Cipher algorithm Info ===
Row 0: 2 11 13 15 5 8 2 19 13 9 5 11 15 18 5 1 6 17 13 6
Row 1: 14 17 17 9 7 16 6 15 8 6 19 18 19 4 16 8 11 16 17 19
Row 2: 17 4 15 17 4 6 13 4 18 15 12 10 7 15 10 18 15 19 6 12
Row 3: 12 8 11 13 2 11 12 8 4 13 1 9 13 13 8 0 17 13 7 9
Row 4: 3 16 9 19 17 3 1 17 17 0 7 15 14 10 17 7 3 8 18 1
Row 5: 15 3 10 11 13 17 7 18 3 1 17 6 2 2 18 16 9 10 11 16
Row 6: 4 12 2 12 1 14 5 16 1 12 8 13 12 11 19 4 19 3 16 5
Row 7: 5 15 8 2 15 10 0 6 16 2 2 17 6 16 13 2 13 2 2 17
Row 8: 0 0 18 3 12 19 15 10 10 19 16 1 9 12 15 11 5 12 19 18
Row 9: 6 14 14 18 0 7 10 7 5 14 13 7 16 3 4 19 16 5 8 11
Row 10: 9 6 6 1 6 5 8 2 9 18 4 8 0 5 0 17 12 14 15 4
Row 11: 16 19 19 14 14 18 3 1 19 4 14 5 5 17 14 6 14 7 9 8
Row 12: 1 5 3 4 3 4 9 3 2 3 18 19 3 9 11 5 2 0 14 15
Row 13: 7 2 12 6 19 1 16 5 6 7 15 4 4 0 1 14 0 18 4 14
Row 14: 13 7 7 8 10 12 18 11 11 8 3 2 8 6 9 10 4 1 3 7
Row 15: 19 1 1 16 18 0 19 0 7 16 0 16 18 14 2 9 18 9 0 13
Row 16: 18 10 5 7 9 2 14 12 12 10 9 3 1 8 12 15 7 6 5 2
Row 17: 11 18 0 5 16 13 11 13 14 11 10 14 11 19 6 3 10 15 10 10
Row 18: 10 13 16 0 8 15 17 14 0 17 11 12 17 1 7 12 8 11 12 0
Row 19: 8 9 4 10 11 9 4 9 15 5 6 0 10 7 3 13 1 4 1 3
```

```

P(C): 0.0364 0.0428 0.0476 0.0476 0.054 0.0396 0.0492 0.046 0.0604 0.046 0.0396 0.054 0.0508 0.0588 0.0444 0.0556 0.0508 0.0812 0.046 0.0492
P(M, C) :
Row 0: 0 0.0044 0.0044 0 0 0.0044 0.0044 0 0.0044 0.0044 0 0.0044 0 0.0044 0 0.0044 0 0.0044 0.0044 0.0044
Row 1: 0 0 0 0.0044 0 0.0044 0.0044 0.0044 0.0044 0 0.0044 0 0.0154 0.0044 0.0044 0.0044 0.0044 0.0044 0.0044
Row 2: 0 0 0 0.0044 0 0.0044 0.0044 0 0 0.0044 0 0.0044 0.0044 0 0.0044 0 0.0044 0.0044 0.0044 0.0044
Row 3: 0.0044 0.0044 0.0044 0 0.0044 0 0.0044 0.0044 0.0044 0.0044 0 0.0044 0.0044 0.0044 0 0 0.0044 0 0
Row 4: 0.0044 0.0044 0 0.0044 0 0 0.0044 0.0044 0.0044 0.0044 0 0 0.0044 0.0044 0.0154 0.0044 0.0044 0.0044
Row 5: 0 0.0012 0.0012 0.0012 0 0 0.0012 0.0012 0 0.0012 0.0012 0.0012 0 0.0012 0 0.0012 0 0.0012 0.0012 0
Row 6: 0 0.0012 0.0012 0.0012 0.0012 0.0012 0.0012 0 0 0.0012 0 0.0012 0.0012 0.0012 0.0012 0 0.0012 0 0 0.0012
Row 7: 0.0012 0 0.0012 0 0 0.0042 0.0012 0 0.0012 0 0.0012 0 0 0.0012 0 0.0012 0.0012 0.0012 0 0
Row 8: 0.0042 0.0012 0 0.0012 0 0.0012 0 0 0.0012 0.0012 0.0012 0.0012 0 0 0.0012 0.0012 0 0.0012 0.0012
Row 9: 0.0012 0 0 0.0012 0.0012 0.0012 0.0042 0.0012 0.0012 0 0.0012 0.0012 0 0.0012 0.0012 0 0.0012 0 0.0012 0.0012
Row 10: 0.0012 0.0012 0.0012 0 0.0012 0.0012 0.0012 0.0012 0 0.0012 0.0012 0 0.0012 0 0.0012 0.0012 0 0.0012 0.0012 0
Row 11: 0 0.0012 0 0.0012 0.0012 0.0012 0.0012 0.0012 0.0012 0.0012 0.0012 0 0 0 0.0012 0 0.0042 0.0012 0.0012 0.0012
Row 12: 0.0012 0.0042 0.0012 0.0012 0.0012 0.0012 0.0012 0 0 0.0012 0 0.0012 0 0.0012 0.0012 0 0 0.0012 0.0012
Row 13: 0.0012 0.0012 0.0042 0 0.0012 0.0012 0.0012 0.0012 0.0012 0 0 0 0.0012 0 0.0012 0.0012 0 0.0012 0.0012
Row 14: 0 0.0012 0.0012 0.0012 0.0012 0 0.0012 0.0012 0.0012 0.0012 0.0012 0.0012 0.0012 0.0012 0.0042 0 0 0 0.0012 0
Row 15: 0.0012 0.0012 0.0012 0 0 0 0.0012 0 0 0.0012 0 0 0.0012 0.0012 0 0.0012 0 0.0012 0.0012
Row 16: 0 0.0012 0.0012 0.0012 0 0.0012 0.0012 0.0012 0.0012 0.0012 0.0012 0.0012 0 0.0012 0 0.0012 0 0 0.0042 0
Row 17: 0.0012 0 0 0.0012 0 0.0012 0.0012 0 0 0.0012 0.0012 0 0.0012 0.0012 0.0012 0.0012 0 0.0042 0.0012
Row 18: 0.0012 0.0012 0 0 0 0 0.0012 0.0012 0 0.0042 0.0012 0.0012 0.0042 0.0012 0.0012 0.0012 0.0012 0 0
Row 19: 0.0012 0.0012 0 0.0012 0.0012 0.0012 0.0012 0.0012 0.0042 0.0012 0.0012 0.0012 0 0.0012 0 0.0012 0 0 0 0

```

```

P(M | C) :
Row 0: 0 0.102804 0.092437 0 0 0.111111 0.0894309 0 0.0728477 0.0956522 0 0.0814815 0 0.0748299 0 0.0791367 0 0.0541872 0.0956522 0.0894309
Row 1: 0 0 0 0.0814815 0 0.0894309 0.0956522 0.0728477 0.0956522 0 0.0814815 0 0.0346847 0.0791367 0.0866142 0.0541872 0.0956522 0.0894309
Row 2: 0 0 0 0.0814815 0 0.0894309 0.0956522 0 0.111111 0 0.0866142 0.0748299 0 0.0791367 0 0.0541872 0.0956522 0.0894309
Row 3: 0.120879 0.102804 0.092437 0 0.0814815 0 0.0956522 0.0728477 0.0956522 0 0.0814815 0.0866142 0.0748299 0 0 0.0541872 0 0
Row 4: 0.120879 0.102804 0.092437 0 0 0.0956522 0.0728477 0.0956522 0.111111 0 0 0.0990991 0.0791367 0.30315 0.0541872 0.0956522 0.0894309
Row 5: 0 0.0280374 0.0252101 0.0252101 0 0 0.0243902 0.026087 0.030303 0.0222222 0 0.026087 0 0.026087 0 0.0755396 0.023622 0.0147783 0.026087 0
Row 6: 0 0.0280374 0.0252101 0.0252101 0.0222222 0.030303 0 0 0.0198675 0 0.0222222 0.023622 0.0204082 0.027027 0 0.023622 0 0 0.0243902
Row 7: 0.032967 0 0.0252101 0 0 0.106061 0.0243902 0 0.0198675 0 0.030303 0 0 0.0204082 0 0.0215827 0.023622 0.0147783 0 0
Row 8: 0.115385 0.0280374 0 0.0252101 0 0.030303 0 0 0.026087 0.030303 0.0222222 0.023622 0 0 0.0215827 0.023622 0 0.026087 0.0243902
Row 9: 0.032967 0 0 0.0252101 0.0222222 0.030303 0.0853659 0.026087 0.0198675 0 0.030303 0.0222222 0 0.0204082 0.027027 0 0.023622 0 0.026087 0.0243902
Row 10: 0.032967 0.0280374 0.0252101 0 0.0222222 0.030303 0.0243902 0.026087 0.0198675 0.026087 0 0 0.023622 0 0.027027 0.0215827 0 0.0147783 0.026087 0.0243902
Row 11: 0 0.0280374 0 0.0252101 0.0222222 0.030303 0.0243902 0.026087 0.0198675 0.026087 0 0 0 0.027027 0 0.0826772 0.0147783 0.026087 0.0243902
Row 12: 0.032967 0.0981308 0.0252101 0.0252101 0.0222222 0.030303 0 0 0.026087 0 0.0222222 0 0 0.027027 0.0215827 0 0 0.026087 0.0243902
Row 13: 0.032967 0.0280374 0.0882353 0 0.0222222 0.030303 0.0243902 0.026087 0 0 0.023622 0 0.027027 0.0215827 0.023622 0 0.026087 0.0243902
Row 14: 0 0.0280374 0.0252101 0.0252101 0.0222222 0 0.0243902 0.026087 0.0198675 0.026087 0.030303 0.0222222 0.023622 0.0714286 0 0 0 0.026087 0
Row 15: 0.032967 0.0280374 0.0252101 0 0 0 0.026087 0 0.026087 0 0 0.0204082 0.027027 0 0.023622 0 0.026087 0.0243902
Row 16: 0 0.0280374 0.0252101 0.0252101 0 0.030303 0.0243902 0.026087 0.0198675 0.026087 0.030303 0 0.023622 0 0.027027 0.0215827 0 0 0.0913043 0
Row 17: 0.032967 0 0 0.0252101 0 0.030303 0.0243902 0 0 0.030303 0.0222222 0 0.0204082 0.027027 0.0215827 0.023622 0 0.0913043 0.0243902
Row 18: 0.032967 0.0280374 0 0 0 0 0.026087 0.0198675 0 0.106061 0.0222222 0.023622 0.0714286 0.027027 0.0215827 0.023622 0.0147783 0 0
Row 19: 0.032967 0.0280374 0 0.0252101 0.0222222 0.030303 0.0243902 0.026087 0.0695364 0.026087 0.030303 0.0222222 0 0.0204082 0 0.0215827 0 0 0 0

```

1.3 Побудова вирішуючих функцій

Означення 1.

Оптимальна (баєсівська) детерміністична функція [в межах лабораторної роботи] визначається наступним чином:

$$\delta_B = \left\{ \delta_B^{(n)} : \mathcal{M} \rightarrow \mathcal{C} \right\},$$

де $P(\delta_B^{(optim)} | C) = \max_{m \in M} P(M_i | C)$.

Тобто фактично детерміністична функція дорівнює довільному шифротексту, який дорівнює максимальному значенню в i -тому рядку таблиці.

Означення 2.

Стохастична розв'язувальна функція δ_D є оптимальною тоді і тільки тоді, коли $\forall n$ з нерівності $\delta_c^{(n)}(C, M) > 0$ випливає, що $P(M|C) = \max_{M'} P(M'|C)$. Тобто

$$\delta_D^{(optim)}(C, m) = \begin{cases} \frac{1}{G}, & \text{if } P(M|C) = \max_{M'} P(M'|C) \\ 0, & \text{otherwise} \end{cases},$$

де G – максимальна кількість відкритих текстів M , які мають найбільшу [однакову] ймовірність для обраного шифротексту C .

```

Optimal deterministic decision is :
5 14 10 0 16 15 5 5 0 6 0 16 1 2 13 0 18 18 10 8
Optimal stochastic decision is :
Row 0: 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Row 1: 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0
Row 2: 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0
Row 3: 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Row 4: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0
Row 5: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0
Row 6: 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0
Row 7: 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0
Row 8: 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Row 9: 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0
Row 10: 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Row 11: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0
Row 12: 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Row 13: 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Row 14: 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0
Row 15: 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Row 16: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0
Row 17: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0
Row 18: 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0
Row 19: 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0

```

```

Average deterministic decision loss is : 0.553556
Average stochastic decision loss is : 0.553556

```

1.4 Висновки:

Подивившись на отримані результати середніх втрат можна впасти в ступор, оскільки вони виявилися однаковими. На нашу думку це може бути пов'язано з недостатньою точністю обрахунків. Маємо припущення, що стохастична (а.к.а. випадкова) вирішуюча функція мала б відповідати більшій кількості потенційних ВТ до відповідно обраного ШТ, порівняно зі строго детерміністичною. Вона також могла показувати як зашкально добрий результат, так і навпаки (жартуємо, будь-яку випадковість можна передбачити). Варто зазначити, що при збільшенні кількості вхідних даних, стохастична вирішуюча функція (яка являє собою багаторозмірну матрицю) буде займати багатенько пам'яті, що може сповільнити процес виконання програми.