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

15 вересня 2025 р.
м. Київ

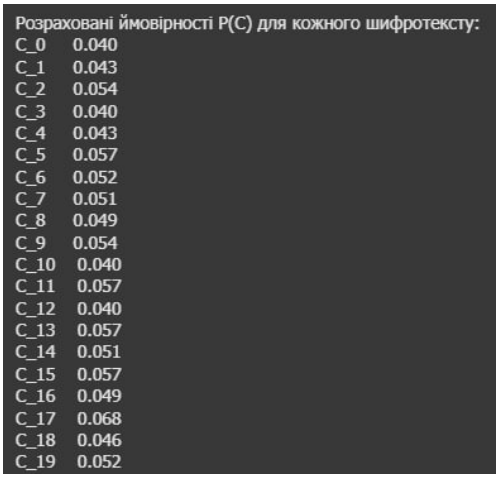
Комп'ютерний практикум № 1

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 порвіняльного 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



Таблиця спільних ймовірностей P(M, C):

	C_0	C_1	C_2	C_3	C_4	C_5	C_6	C_7 \
M_0	0.0044	0.00473	0.00594	0.0044	0.00473	0.00627	0.00572	0.00561
M_1	0.0044	0.00473	0.00594	0.0044	0.00473	0.00627	0.00572	0.00561
M_2	0.0044	0.00473	0.00594	0.0044	0.00473	0.00627	0.00572	0.00561
M_3	0.0044	0.00473	0.00594	0.0044	0.00473	0.00627	0.00572	0.00561
M_4	0.0044	0.00473	0.00594	0.0044	0.00473	0.00627	0.00572	0.00561
M_5	0.0012	0.00129	0.00162	0.0012	0.00129	0.00171	0.00156	0.00153
M_6	0.0012	0.00129	0.00162	0.0012	0.00129	0.00171	0.00156	0.00153
M_7	0.0012	0.00129	0.00162	0.0012	0.00129	0.00171	0.00156	0.00153
M_8	0.0012	0.00129	0.00162	0.0012	0.00129	0.00171	0.00156	0.00153
M_9	0.0012	0.00129	0.00162	0.0012	0.00129	0.00171	0.00156	0.00153
M_10	0.0012	0.00129	0.00162	0.0012	0.00129	0.00171	0.00156	0.00153
M_11	0.0012	0.00129	0.00162	0.0012	0.00129	0.00171	0.00156	0.00153
M_12	0.0012	0.00129	0.00162	0.0012	0.00129	0.00171	0.00156	0.00153
M_13	0.0012	0.00129	0.00162	0.0012	0.00129	0.00171	0.00156	0.00153
M_14	0.0012	0.00129	0.00162	0.0012	0.00129	0.00171	0.00156	0.00153
M_15	0.0012	0.00129	0.00162	0.0012	0.00129	0.00171	0.00156	0.00153
M_16	0.0012	0.00129	0.00162	0.0012	0.00129	0.00171	0.00156	0.00153
M_17	0.0012	0.00129	0.00162	0.0012	0.00129	0.00171	0.00156	0.00153
M_18	0.0012	0.00129	0.00162	0.0012	0.00129	0.00171	0.00156	0.00153
M_19	0.0012	0.00129	0.00162	0.0012	0.00129	0.00171	0.00156	0.00153

	C_8	C_9	C_10	C_11	C_12	C_13	C_14	C_15 \
M_0	0.00539	0.00594	0.0044	0.00627	0.0044	0.00627	0.00561	0.00627
M_1	0.00539	0.00594	0.0044	0.00627	0.0044	0.00627	0.00561	0.00627
M_2	0.00539	0.00594	0.0044	0.00627	0.0044	0.00627	0.00561	0.00627
M_3	0.00539	0.00594	0.0044	0.00627	0.0044	0.00627	0.00561	0.00627
M_4	0.00539	0.00594	0.0044	0.00627	0.0044	0.00627	0.00561	0.00627
M_5	0.00147	0.00162	0.0012	0.00171	0.0012	0.00171	0.00153	0.00171
M_6	0.00147	0.00162	0.0012	0.00171	0.0012	0.00171	0.00153	0.00171
M_7	0.00147	0.00162	0.0012	0.00171	0.0012	0.00171	0.00153	0.00171
M_8	0.00147	0.00162	0.0012	0.00171	0.0012	0.00171	0.00153	0.00171
M_9	0.00147	0.00162	0.0012	0.00171	0.0012	0.00171	0.00153	0.00171
M_10	0.00147	0.00162	0.0012	0.00171	0.0012	0.00171	0.00153	0.00171
M_11	0.00147	0.00162	0.0012	0.00171	0.0012	0.00171	0.00153	0.00171
M_12	0.00147	0.00162	0.0012	0.00171	0.0012	0.00171	0.00153	0.00171
M_13	0.00147	0.00162	0.0012	0.00171	0.0012	0.00171	0.00153	0.00171
M_14	0.00147	0.00162	0.0012	0.00171	0.0012	0.00171	0.00153	0.00171
M_15	0.00147	0.00162	0.0012	0.00171	0.0012	0.00171	0.00153	0.00171
M_16	0.00147	0.00162	0.0012	0.00171	0.0012	0.00171	0.00153	0.00171
M_17	0.00147	0.00162	0.0012	0.00171	0.0012	0.00171	0.00153	0.00171
M_18	0.00147	0.00162	0.0012	0.00171	0.0012	0.00171	0.00153	0.00171
M_19	0.00147	0.00162	0.0012	0.00171	0.0012	0.00171	0.00153	0.00171

	C_16	C_17	C_18	C_19
M_0	0.00539	0.00748	0.00506	0.00572
M_1	0.00539	0.00748	0.00506	0.00572
M_2	0.00539	0.00748	0.00506	0.00572
M_3	0.00539	0.00748	0.00506	0.00572
M_4	0.00539	0.00748	0.00506	0.00572
M_5	0.00147	0.00204	0.00138	0.00156
M_6	0.00147	0.00204	0.00138	0.00156
M_7	0.00147	0.00204	0.00138	0.00156
M_8	0.00147	0.00204	0.00138	0.00156
M_9	0.00147	0.00204	0.00138	0.00156
M_10	0.00147	0.00204	0.00138	0.00156
M_11	0.00147	0.00204	0.00138	0.00156
M_12	0.00147	0.00204	0.00138	0.00156
M_13	0.00147	0.00204	0.00138	0.00156
M_14	0.00147	0.00204	0.00138	0.00156
M_15	0.00147	0.00204	0.00138	0.00156
M_16	0.00147	0.00204	0.00138	0.00156
M_17	0.00147	0.00204	0.00138	0.00156
M_18	0.00147	0.00204	0.00138	0.00156
M_19	0.00147	0.00204	0.00138	0.00156

Таблиця умовних ймовірностей P(M|C):

	C_0	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9	C_10	C_11
M_0	0.11	0.11	0.11	0.11	0.11	0.11	0.11	0.11	0.11	0.11	0.11	0.11
M_1	0.11	0.11	0.11	0.11	0.11	0.11	0.11	0.11	0.11	0.11	0.11	0.11
M_2	0.11	0.11	0.11	0.11	0.11	0.11	0.11	0.11	0.11	0.11	0.11	0.11
M_3	0.11	0.11	0.11	0.11	0.11	0.11	0.11	0.11	0.11	0.11	0.11	0.11
M_4	0.11	0.11	0.11	0.11	0.11	0.11	0.11	0.11	0.11	0.11	0.11	0.11
M_5	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03
M_6	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03
M_7	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03
M_8	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03
M_9	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03
M_10	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03
M_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
M_12	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03
M_13	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03
M_14	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03
M_15	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03
M_16	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03
M_17	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03
M_18	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03
M_19	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03

	C_12	C_13	C_14	C_15	C_16	C_17	C_18	C_19
M_0	0.11	0.11	0.11	0.11	0.11	0.11	0.11	0.11
M_1	0.11	0.11	0.11	0.11	0.11	0.11	0.11	0.11
M_2	0.11	0.11	0.11	0.11	0.11	0.11	0.11	0.11
M_3	0.11	0.11	0.11	0.11	0.11	0.11	0.11	0.11
M_4	0.11	0.11	0.11	0.11	0.11	0.11	0.11	0.11
M_5	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03
M_6	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03
M_7	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03
M_8	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03
M_9	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03
M_10	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03
M_11	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03
M_12	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03
M_13	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03
M_14	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03
M_15	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03
M_16	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03
M_17	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03
M_18	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03
M_19	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03

1.3 Побудова вирішуючих функцій

Означення 1.

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

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

де $P\left(\delta_B^{(optim)} | C\right) = \max\limits_{m \in M} P(M_i|C)$.
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* $P(M|C) = \max\limits_{M'} P(M'|C)$. *Тобто*

$$\delta_D^{optim}(C, m) = \begin{cases} \frac{1}{|M|}, \ \textit{if } P(M|C) = \max\limits_{M'} P(M'|C) \\ 0, \ \textit{otherwise} \end{cases}$$

Оптимальна детермінована функція рішення δ(C):

C_0	M_0
C_1	M_0
C_2	M_0
C_3	M_0
C_4	M_0
C_5	M_0
C_6	M_0
C_7	M_0
C_8	M_0
C_9	M_0
C_10	M_0
C_11	M_0
C_12	M_0
C_13	M_0
C_14	M_0
C_15	M_0
C_16	M_0
C_17	M_0
C_18	M_0
C_19	M_0

Як результат роботи - видало перший ліпший M_i (за критеріями підходить декілька)

Матриця стохастичної функції рішення δ_S:

	C_0	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9	C_10	C_11
M_0	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05
M_1	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05
M_2	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05
M_3	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05
M_4	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05
M_5	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05
M_6	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05
M_7	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05
M_8	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05
M_9	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05
M_10	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05
M_11	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05
M_12	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05
M_13	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05
M_14	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05
M_15	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05
M_16	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05
M_17	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05
M_18	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05
M_19	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05

	C_12	C_13	C_14	C_15	C_16	C_17	C_18	C_19
M_0	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05
M_1	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05
M_2	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05
M_3	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05
M_4	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05
M_5	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05
M_6	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05
M_7	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05
M_8	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05
M_9	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05
M_10	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05
M_11	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05
M_12	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05
M_13	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05
M_14	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05
M_15	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05
M_16	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05
M_17	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05
M_18	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05
M_19	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05

Покращена стохастична функція:

	C_0	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9	C_10	C_11	C_12
M_0	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	
M_1	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	
M_2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	
M_3	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	
M_4	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	
M_5	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	
M_6	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	
M_7	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	
M_8	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	
M_9	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	
M_10	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	
M_11	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	
M_12	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	
M_13	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	
M_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	
M_15	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	
M_16	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	
M_17	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	
M_18	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	
M_19	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	

	C_13	C_14	C_15	C_16	C_17	C_18	C_19
M_0	0.2	0.2	0.2	0.2	0.2	0.2	0.2
M_1	0.2	0.2	0.2	0.2	0.2	0.2	0.2
M_2	0.2	0.2	0.2	0.2	0.2	0.2	0.2
M_3	0.2	0.2	0.2	0.2	0.2	0.2	0.2
M_4	0.2	0.2	0.2	0.2	0.2	0.2	0.2
M_5	0.0	0.0	0.0	0.0	0.0	0.0	0.0
M_6	0.0	0.0	0.0	0.0	0.0	0.0	0.0
M_7	0.0	0.0	0.0	0.0	0.0	0.0	0.0
M_8	0.0	0.0	0.0	0.0	0.0	0.0	0.0
M_9	0.0	0.0	0.0	0.0	0.0	0.0	0.0
M_10	0.0	0.0	0.0	0.0	0.0	0.0	0.0
M_11	0.0	0.0	0.0	0.0	0.0	0.0	0.0
M_12	0.0	0.0	0.0	0.0	0.0	0.0	0.0
M_13	0.0	0.0	0.0	0.0	0.0	0.0	0.0
M_14	0.0	0.0	0.0	0.0	0.0	0.0	0.0
M_15	0.0	0.0	0.0	0.0	0.0	0.0	0.0
M_16	0.0	0.0	0.0	0.0	0.0	0.0	0.0
M_17	0.0	0.0	0.0	0.0	0.0	0.0	0.0
M_18	0.0	0.0	0.0	0.0	0.0	0.0	0.0
M_19	0.0	0.0	0.0	0.0	0.0	0.0	0.0

```
Середні втрати для детермінованої функції: 0.890000000
```

```
Середні втрати для стохастичної функції: 0.890000000
```

1.4 Висновки:

Подивившись на отримані результати середніх втрат можна впасти в ступор, оскільки вони виявилися однаковими. На нашу думку це може бути бути пов’язано з недостатньою точністю обрахунків. Маємо припущення, що стохастична (a.k.a. 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.