

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені Ігоря СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ
ІНСТИТУТ
Кафедра математичних методів захисту інформації

Комп'ютерний практикум №1
з курсу
Методи криптоаналізу 1

Підготували:
студенти 5 курсу
групи ФІ-22мн
Ковальчук О.М.
Коломієць А.Ю.

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

Мета лабораторної 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

Реалізувати алгоритми програмно 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) побудова оптимальних детерміністичної та стохастичної вирішуючих функцій зводиться до максимізації $P(M|C)$.

Обчислити середні втрати, провести порівняльний аналіз вирішуючих функцій.

Для варіанту №6

Таблиця 3 – Таблиця шифрування.

	M_0	M_1	M_2	M_3	M_4	M_5	M_6	M_7	M_8	M_9	M_{10}	M_{11}	M_{12}	M_{13}	M_{14}	M_{15}	M_{16}	M_{17}	M_{18}	M_{19}
K_0	14	12	1	2	8	17	7	0	9	18	4	19	15	3	13	10	11	6	16	5
K_1	13	12	11	0	15	10	5	4	16	17	7	18	19	2	8	1	6	3	14	9
K_2	17	12	19	8	11	1	5	0	16	3	15	6	13	10	9	2	18	14	4	7
K_3	18	6	7	19	13	0	4	10	9	17	16	14	2	8	1	5	15	12	3	11
K_4	6	0	16	14	3	4	11	2	10	18	15	17	5	9	13	19	1	8	7	12
K_5	17	9	11	10	7	3	5	8	16	4	18	13	15	0	19	1	14	12	2	6
K_6	7	18	15	10	11	8	9	13	1	14	4	2	17	12	3	5	6	19	0	16
K_7	11	10	14	19	8	1	4	5	7	16	12	9	0	2	6	17	18	3	15	13
K_8	11	7	3	1	19	10	9	6	4	12	0	15	18	14	5	8	13	16	17	2
K_9	3	16	15	13	19	18	11	1	9	2	8	10	4	14	6	17	12	5	7	0
K_{10}	15	9	3	18	8	10	5	14	6	0	16	12	2	19	13	11	7	4	17	1
K_{11}	6	4	19	12	15	17	10	14	3	11	18	8	7	9	2	13	0	1	5	16
K_{12}	19	13	18	1	10	3	9	2	17	14	12	7	16	15	0	6	11	4	5	8
K_{13}	12	18	3	17	11	15	9	6	14	1	4	13	2	0	16	8	19	7	5	10
K_{14}	11	19	18	16	2	12	4	15	1	6	7	5	13	9	17	0	8	3	14	10
K_{15}	2	10	4	14	7	19	18	3	15	11	17	0	6	9	5	1	13	12	16	8
K_{16}	6	10	3	9	13	7	16	19	5	18	4	17	11	15	8	2	1	14	12	0
K_{17}	17	12	7	11	15	13	18	3	0	4	19	9	8	2	16	1	6	10	5	14
K_{18}	10	5	9	2	13	19	1	15	6	16	3	18	17	11	8	12	14	4	0	7
K_{19}	5	2	18	11	10	17	15	1	12	19	14	0	4	3	7	9	6	8	16	13

Для варіанту №11

Таблиця 4 – Таблиця шифрування.

	M_0	M_1	M_2	M_3	M_4	M_5	M_6	M_7	M_8	M_9	M_{10}	M_{11}	M_{12}	M_{13}	M_{14}	M_{15}	M_{16}	M_{17}	M_{18}	M_{19}
K_0	2	17	3	19	12	4	0	8	1	6	15	14	7	9	10	5	18	16	13	11
K_1	18	19	11	16	8	0	5	10	15	7	17	14	1	3	13	12	4	6	2	9
K_2	10	12	15	5	13	11	8	2	0	3	17	14	7	1	6	16	18	19	9	4
K_3	4	15	8	0	12	9	19	18	1	14	17	16	7	2	6	10	5	11	13	3
K_4	15	9	5	1	16	0	8	18	2	17	3	10	4	6	12	14	11	7	19	13
K_5	1	7	5	11	19	8	17	18	14	0	15	12	10	6	9	16	2	4	13	3
K_6	18	10	13	12	19	1	2	5	14	17	11	9	15	0	6	8	7	3	4	16
K_7	3	13	1	14	12	11	2	9	18	10	0	19	5	16	15	4	8	6	7	17
K_8	5	9	0	15	10	12	18	13	19	14	3	4	17	11	16	8	6	7	2	1
K_9	14	8	12	16	17	2	7	18	6	11	15	13	4	19	9	5	1	0	10	3
K_{10}	16	6	0	14	13	15	5	12	11	18	1	2	3	8	9	19	17	10	4	7
K_{11}	9	18	4	0	8	13	11	17	5	15	7	10	14	12	3	6	19	16	2	1
K_{12}	9	6	19	12	3	15	7	16	14	18	4	0	17	1	13	10	5	2	8	11
K_{13}	12	4	9	19	2	18	14	6	0	5	7	8	17	16	11	1	10	3	13	15
K_{14}	13	17	19	1	12	8	11	3	16	10	18	15	6	2	0	5	9	4	14	7
K_{15}	16	3	15	11	18	8	13	1	4	12	19	2	14	5	10	6	7	9	17	0
K_{16}	17	2	13	12	16	3	8	0	7	6	18	1	14	10	15	11	5	19	9	4
K_{17}	14	18	12	6	1	8	9	2	17	5	3	7	4	10	13	0	19	11	16	15
K_{18}	4	11	19	6	3	16	10	9	14	13	1	7	5	15	18	12	8	0	2	17
K_{19}	9	7	12	8	0	10	3	6	14	19	17	4	18	5	2	1	13	11	16	15

Хід роботи

Опис алгоритму побудови детерміністичної вирішуючої функції

Баєсівською вирішуючою функцією називається така детерміністична вирішуюча функція δ_B для якої виконується умова:

$$P(\delta_B|C) = \max_{M \in \mathcal{M}} P(M|C)$$

Баєсівською δ_B розв'язувальною функцією називається послідовність відображень:

$$\delta_B = \{\delta_B^{(n)} : Z_m^n \rightarrow Z_m^n, n = 1, 2, \dots\},$$

де $\forall C$ значення функції $M = \delta_B^{(n)}(C)$ визначається як таке M , для якого максимізується ймовірність

$$P(\delta_B^{(n)}(C)/C) = \max_{M \in Z_m^n} P(M/C).$$

.

Детерміністична вирішуюча функція є оптимальною тоді і лише тоді, коли вона є баєсівською. Детерміністична розв'язувальна функція буде оптимальною тоді і тільки тоді, якщо для кожного C значенням функції $\delta_B^{(n)}(C)$ буде такий відкритий текст M , при якому $P(M, C)$ і $P(M|C)$ досягають максимального значення, тобто

$$P(\delta_B^{(n)}(C)/C) = \max_{M \in Z^n} P(M/C) = P(\delta_B^{(n)}(C)/C)$$

Опис алгоритму побудови стохастичної вирішуючої функції

Для кожного ШТ C_k будемо послідовність $P(M_i | C_k)$, $i = 1, 2, \dots, m^n$. Для таких M_i , для яких

$$P(M_i|C_k) = \max_{M'} P(M'|C_k).$$

покладаємо $\delta_c^{(n)}(C_k, M_i) = \frac{1}{s}$, де s – число таких ВТ для даного C_k , на яких досягається максимум. Іншим елементам $\delta_c^{(n)}(C_k, M_i) = 0$ k -го рядку матриці (що відповідає ШТ C_k) приписуємо значення нуль.

Опис труднощів, що виникали, та шляхи їх розв'язання

Найбільші труднощі, що виникли під час виконання комп'ютерного практикуму – нестача знань володінням GitHub репозиторієм з терміналу Linux. Але дана перепона була подолана шляхом тренування в інтерактивному веб-середовищі. Також було важко працювати з об'єктами мови програмування Python3 такими, як DataFrame та Arrays. Були неоднозначності, щодо індексування комірок матриці таблиці, що призводили до постійного пошуку помилок у коді в індексації елементів.

Таблиці ймовірностей $P(M/C)$

Для варіанту №6

	M_0	M_1	M_2	M_3	M_4	M_5	M_6	M_7	M_8	M_9	M_{10}	M_{11}	M_{12}	M_{13}	M_{14}	M_{15}	M_{16}	M_{17}	M_{18}	M_{19}
C_0	0.0000	0.0016	0.0000	0.0016	0.0000	0.0016	0.0000	0.0112	0.0016	0.0016	0.0016	0.0032	0.0016	0.0032	0.0016	0.0016	0.0016	0.0000	0.0032	0.0032
C_1	0.0000	0.0000	0.0096	0.0032	0.0000	0.0032	0.0016	0.0032	0.0032	0.0016	0.0000	0.0000	0.0000	0.0000	0.0016	0.0064	0.0032	0.0016	0.0000	0.0016
C_2	0.0096	0.0016	0.0000	0.0112	0.0016	0.0000	0.0000	0.0032	0.0000	0.0016	0.0000	0.0016	0.0048	0.0048	0.0016	0.0032	0.0000	0.0000	0.0016	0.0016
C_3	0.0096	0.0000	0.0064	0.0000	0.0016	0.0032	0.0000	0.0032	0.0016	0.0016	0.0016	0.0000	0.0000	0.0112	0.0016	0.0000	0.0000	0.0048	0.0016	0.0000
C_4	0.0000	0.0016	0.0016	0.0000	0.0000	0.0016	0.0048	0.0016	0.0016	0.0032	0.0144	0.0000	0.0032	0.0000	0.0000	0.0000	0.0000	0.0048	0.0016	0.0000
C_5	0.0096	0.0016	0.0000	0.0000	0.0000	0.0000	0.0064	0.0016	0.0016	0.0000	0.0000	0.0016	0.0016	0.0000	0.0032	0.0032	0.0000	0.0016	0.0064	0.0096
C_6	0.0288	0.0016	0.0000	0.0000	0.0000	0.0000	0.0000	0.0032	0.0032	0.0016	0.0000	0.0016	0.0016	0.0000	0.0032	0.0016	0.0064	0.0096	0.0000	0.0016
C_7	0.0096	0.0016	0.0032	0.0000	0.0032	0.0016	0.0096	0.0000	0.0016	0.0000	0.0032	0.0016	0.0016	0.0000	0.0016	0.0000	0.0016	0.0016	0.0032	0.0032
C_8	0.0000	0.0000	0.0000	0.0016	0.0128	0.0016	0.0000	0.0016	0.0000	0.0000	0.0016	0.0016	0.0016	0.0016	0.0048	0.0032	0.0016	0.0032	0.0000	0.0032
C_9	0.0000	0.0032	0.0016	0.0016	0.0000	0.0000	0.0064	0.0000	0.0128	0.0000	0.0000	0.0032	0.0000	0.0064	0.0016	0.0016	0.0000	0.0000	0.0000	0.0016
C_{10}	0.0096	0.0048	0.0000	0.0032	0.0032	0.0048	0.0016	0.0016	0.0016	0.0000	0.0000	0.0016	0.0000	0.0016	0.0000	0.0096	0.0000	0.0016	0.0000	0.0032
C_{11}	0.0288	0.0000	0.0032	0.0032	0.0048	0.0000	0.0032	0.0000	0.0000	0.0032	0.0000	0.0000	0.0016	0.0016	0.0000	0.0016	0.0112	0.0000	0.0000	0.0016
C_{12}	0.0096	0.0144	0.0000	0.0016	0.0000	0.0016	0.0000	0.0000	0.0016	0.0016	0.0032	0.0016	0.0000	0.0016	0.0000	0.0016	0.0016	0.0048	0.0016	0.0016
C_{13}	0.0096	0.0016	0.0000	0.0016	0.0048	0.0016	0.0000	0.0016	0.0000	0.0000	0.0000	0.0032	0.0032	0.0000	0.0128	0.0016	0.0032	0.0000	0.0000	0.0032
C_{14}	0.0576	0.0000	0.0016	0.0032	0.0000	0.0000	0.0000	0.0032	0.0016	0.0032	0.0016	0.0016	0.0000	0.0032	0.0000	0.0000	0.0032	0.0032	0.0032	0.0016
C_{15}	0.0096	0.0000	0.0032	0.0000	0.0048	0.0016	0.0016	0.0032	0.0016	0.0000	0.0032	0.0016	0.0112	0.0032	0.0000	0.0000	0.0016	0.0000	0.0016	0.0000
C_{16}	0.0000	0.0016	0.0016	0.0016	0.0000	0.0000	0.0016	0.0000	0.0048	0.0032	0.0032	0.0000	0.0016	0.0000	0.0032	0.0000	0.0000	0.0016	0.0128	0.0032
C_{17}	0.0288	0.0000	0.0000	0.0016	0.0000	0.0128	0.0000	0.0000	0.0016	0.0032	0.0016	0.0032	0.0032	0.0000	0.0016	0.0032	0.0000	0.0000	0.0032	0.0000
C_{18}	0.0096	0.0032	0.0048	0.0016	0.0000	0.0016	0.0032	0.0000	0.0000	0.0128	0.0032	0.0032	0.0016	0.0000	0.0000	0.0000	0.0032	0.0000	0.0000	0.0000
C_{19}	0.0096	0.0016	0.0032	0.0032	0.0032	0.0032	0.0000	0.0016	0.0000	0.0016	0.0016	0.0096	0.0016	0.0016	0.0016	0.0016	0.0016	0.0016	0.0000	0.0000

Для варіанту №11

	M_0	M_1	M_2	M_3	M_4	M_5	M_6	M_7	M_8	M_9	M_{10}	M_{11}	M_{12}	M_{13}	M_{14}	M_{15}	M_{16}	M_{17}	M_{18}	M_{19}
C_0	0.0000	0.0000	0.0032	0.0032	0.0016	0.0072	0.0056	0.0016	0.0032	0.0016	0.0016	0.0016	0.0000	0.0016	0.0016	0.0016	0.0000	0.0032	0.0000	0.0016
C_1	0.0096	0.0000	0.0016	0.0032	0.0016	0.0016	0.0000	0.0016	0.0072	0.0000	0.0032	0.0016	0.0056	0.0032	0.0000	0.0032	0.0016	0.0000	0.0000	0.0032
C_2	0.0336	0.0016	0.0000	0.0000	0.0016	0.0016	0.0032	0.0032	0.0016	0.0000	0.0000	0.0032	0.0000	0.0032	0.0016	0.0000	0.0016	0.0016	0.0104	0.0000
C_3	0.0096	0.0016	0.0056	0.0000	0.0032	0.0016	0.0016	0.0016	0.0000	0.0016	0.0048	0.0000	0.0016	0.0056	0.0016	0.0000	0.0000	0.0032	0.0000	0.0048
C_4	0.0192	0.0016	0.0016	0.0000	0.0000	0.0056	0.0000	0.0000	0.0016	0.0000	0.0016	0.0032	0.0048	0.0000	0.0000	0.0016	0.0056	0.0032	0.0032	0.0032
C_5	0.0096	0.0000	0.0032	0.0016	0.0000	0.0000	0.0072	0.0016	0.0016	0.0032	0.0000	0.0000	0.0032	0.0032	0.0000	0.0088	0.0048	0.0000	0.0000	0.0000
C_6	0.0000	0.0032	0.0000	0.0032	0.0000	0.0000	0.0000	0.0032	0.0016	0.0072	0.0000	0.0000	0.0016	0.0032	0.0048	0.0032	0.0016	0.0072	0.0000	0.0000
C_7	0.0000	0.0032	0.0000	0.0000	0.0000	0.0000	0.0032	0.0000	0.0016	0.0056	0.0032	0.0032	0.0088	0.0000	0.0000	0.0000	0.0032	0.0032	0.0016	0.0032
C_8	0.0000	0.0016	0.0016	0.0016	0.0072	0.0064	0.0048	0.0056	0.0000	0.0000	0.0000	0.0016	0.0000	0.0016	0.0000	0.0032	0.0032	0.0000	0.0016	0.0000
C_9	0.0288	0.0032	0.0016	0.0000	0.0000	0.0016	0.0016	0.0032	0.0000	0.0000	0.0000	0.0016	0.0000	0.0056	0.0048	0.0000	0.0016	0.0016	0.0032	0.0056
C_{10}	0.0096	0.0016	0.0000	0.0000	0.0016	0.0016	0.0016	0.0056	0.0000	0.0032	0.0000	0.0032	0.0016	0.0032	0.0072	0.0032	0.0016	0.0016	0.0016	0.0000
C_{11}	0.0000	0.0016	0.0056	0.0032	0.0000	0.0032	0.0000	0.0016	0.0016	0.0016	0.0016	0.0000	0.0000	0.0016	0.0016	0.0016	0.0016	0.0048	0.0000	0.0072
C_{12}	0.0096	0.0016	0.0048	0.0048	0.0104	0.0016	0.0000	0.0016	0.0000	0.0016	0.0000	0.0016	0.0000	0.0016	0.0016	0.0072	0.0000	0.0000	0.0000	0.0000
C_{13}	0.0096	0.0016	0.0032	0.0000	0.0032	0.0016	0.0016	0.0016	0.0000	0.0016	0.0000	0.0016	0.0000	0.0000	0.0088	0.0000	0.0016	0.0000	0.0104	0.0016
C_{14}	0.0192	0.0000	0.0000	0.0032	0.0000	0.0000	0.0016	0.0000	0.0080	0.0032	0.0000	0.0128	0.0048	0.0000	0.0000	0.0016	0.0000	0.0000	0.0016	0.0000
C_{15}	0.0096	0.0016	0.0032	0.0016	0.0000	0.0032	0.0000	0.0000	0.0056	0.0016	0.0088	0.0016	0.0016	0.0016	0.0032	0.0000	0.0000	0.0000	0.0000	0.0048
C_{16}	0.0192	0.0000	0.0000	0.0072	0.0032	0.0016	0.0000	0.0016	0.0016	0.0000	0.0000	0.0016	0.0000	0.0032	0.0016	0.0032	0.0000	0.0072	0.0032	0.0016
C_{17}	0.0096	0.0072	0.0000	0.0000	0.0016	0.0000	0.0016	0.0016	0.0016	0.0032	0.0104	0.0000	0.0048	0.0000	0.0000	0.0000	0.0016	0.0000	0.0016	0.0032
C_{18}	0.0432	0.0032	0.0000	0.0000	0.0016	0.0016	0.0064	0.0016	0.0032	0.0032	0.0000	0.0016	0.0000	0.0016	0.0000	0.0000	0.0072	0.0000	0.0000	0.0000
C_{19}	0.0000	0.0056	0.0048	0.0072	0.0032	0.0000	0.0016	0.0000	0.0016	0.0016	0.0016	0.0016	0.0000	0.0016	0.0000	0.0016	0.0032	0.0032	0.0016	0.0000

Знайдені детерміністична та стохастична функції у вигляді таблиць

Для варианту №6

Таблиця 5 – Детерміністична 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}	C_{13}	C_{14}	C_{15}	C_{16}	C_{17}	C_{18}	C_{19}
<i>Deterministic function</i>	7	2	3	13	10	0	0	0	4	8	0	0	1	14	0	12	18	0	9	0

Для варіанту №11

Таблиця 6 – Детерміністична 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}	C_{13}	C_{14}	C_{15}	C_{16}	C_{17}	C_{18}	C_{19}
<i>Deterministic function</i>	5	0	0	0	0	0	9	12	4	0	0	19	4	18	0	0	0	10	0	3

Для варіанту №6

Таблиця 7 – Стохастична функція.

[illegible]

Для варіанту №11

Таблиця 8 – Стохастична функція.

	M_0	M_1	M_2	M_3	M_4	M_5	M_6	M_7	M_8	M_9	M_{10}	M_{11}	M_{12}	M_{13}	M_{14}	M_{15}	M_{16}	M_{17}	M_{18}	M_{19}
C_0	0.0	0.0	0.0	0.0	0.0	1.0	0.0	0.0	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_1	1.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	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_2	1.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	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_3	1.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	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_4	1.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	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_5	1.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	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_6	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.5	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.5	0.0	0.0
C_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	1.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
C_8	0.0	0.0	0.0	0.0	1.0	0.0	0.0	0.0	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_9	1.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	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_{10}	1.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	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_{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	0.0	0.0	0.0	0.0	0.0	0.0	0.0	1.0
C_{12}	0.0	0.0	0.0	0.0	1.0	0.0	0.0	0.0	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}	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	1.0	0.0
C_{14}	1.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	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_{15}	1.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	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_{16}	1.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	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_{17}	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	1.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
C_{18}	1.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	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_{19}	0.0	0.0	0.0	1.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0

Середні втрати для вирішуючих функцій

Для варіанту №6

Детерміністична вирішуюча функція: 0.6703999999999999

Стохастична вирішуюча функція: 0.6703999999999999

Для варіанту №11

Детерміністична вирішуюча функція: 0.7128

Стохастична вирішуюча функція: 0.7128

ВИСНОВКИ

Аналізуючи значення середніх втрат для детерміністичної та стохастичної вирішуючих функцій можемо прийти до висновку, що вони дають однакову точність. Але яка вирішуюча функція краща: детерміністична чи стохастична? Стохастична краща, бо вона зберігає усі найбільш імовірні ВТ, а детерміністична обирає одну із всіх, а решту відкидає.