Лабораторна робота №1
«Баєсівський підхід в криптоаналізі: побудова та дослідження детерміністичної та стохастичної вирішуючих функцій»

Пясецький Б.

Мета роботи: ознайомлення з принципами баєсовського 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.

1 Хід роботи

1. Описати алгоритм детерміністичної та стохастичної вирішуючих функцій.
2. Створити репозиторій в системі контролю Git.
3. Реалізувати алгоритм програмно. Подати результати побудови детерміністичної та стохастичної вирішуючих функцій у вигляді таблиць.
4. Обчислити середні витрати, провести порівняльний аналіз вирішуючих функцій.

Побудова детерміністичної та стохастичної вирішуючих функцій для моделей схем шифрування та криптоаналіз моделей шифрів виконувався для варіантів 6 та 17.

1.1 Алгоритм побудови вирішуючих функцій

Детерміністична вирішуюча функція на вході шифрованого текста (C) видає те значення відкритого текста (M), при якому умовна ймовірність ($P(M|C)$) максимальна.

Стохастична вирішуюча функція представлена як випадкова величина. Маємо випадкову величину яка приймає значення із множини відкритих текстів (M) та кожне значення приймає з ймовірністю $P(M|C)$. Тому результатом стохастичної вирішуючої функції буде максимальна умовна ймовірність.

1.2 Таблиця ймовірностей $P(M|C)$

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
0	0,00	0,04	0,00	0,04	0,00	0,04	0,00	0,28	0,04	0,04	0,04	0,08	0,04	0,08	0,04	0,04	0,04	0,00	0,08	0,08
1	0,00	0,00	0,24	0,08	0,00	0,08	0,04	0,08	0,08	0,04	0,00	0,00	0,00	0,00	0,04	0,16	0,08	0,04	0,00	0,04
2	0,20	0,03	0,00	0,23	0,03	0,00	0,00	0,07	0,00	0,03	0,00	0,03	0,10	0,10	0,03	0,07	0,00	0,00	0,03	0,03
3	0,20	0,00	0,13	0,00	0,03	0,07	0,00	0,07	0,03	0,03	0,03	0,00	0,00	0,23	0,03	0,00	0,00	0,10	0,03	0,00
4	0,00	0,04	0,04	0,00	0,00	0,04	0,12	0,04	0,04	0,08	0,36	0,00	0,08	0,00	0,00	0,00	0,00	0,12	0,04	0,00
5	0,20	0,03	0,00	0,00	0,00	0,00	0,13	0,03	0,03	0,00	0,00	0,03	0,03	0,00	0,07	0,07	0,00	0,03	0,13	0,20
6	0,45	0,03	0,00	0,00	0,00	0,00	0,00	0,05	0,05	0,03	0,00	0,03	0,03	0,00	0,05	0,03	0,10	0,15	0,00	0,03
7	0,20	0,03	0,07	0,00	0,07	0,03	0,20	0,00	0,03	0,00	0,07	0,03	0,03	0,00	0,03	0,00	0,03	0,03	0,07	0,07
8	0,00	0,00	0,00	0,04	0,32	0,04	0,00	0,04	0,00	0,00	0,04	0,04	0,04	0,04	0,12	0,08	0,04	0,08	0,00	0,08
9	0,00	0,08	0,04	0,04	0,00	0,00	0,16	0,00	0,32	0,00	0,00	0,08	0,00	0,16	0,04	0,04	0,00	0,00	0,00	0,04
10	0,20	0,10	0,00	0,07	0,07	0,10	0,03	0,03	0,03	0,00	0,00	0,03	0,00	0,03	0,00	0,20	0,00	0,03	0,00	0,07
11	0,45	0,00	0,05	0,05	0,08	0,00	0,05	0,00	0,00	0,05	0,00	0,00	0,03	0,03	0,00	0,03	0,18	0,00	0,00	0,03
12	0,20	0,30	0,00	0,03	0,00	0,03	0,00	0,00	0,03	0,03	0,07	0,03	0,00	0,03	0,00	0,03	0,03	0,10	0,03	0,03
13	0,20	0,03	0,00	0,03	0,10	0,03	0,00	0,03	0,00	0,00	0,00	0,07	0,07	0,00	0,27	0,03	0,07	0,00	0,00	0,07
14	0,65	0,00	0,02	0,04	0,00	0,00	0,00	0,04	0,02	0,04	0,02	0,02	0,00	0,04	0,00	0,00	0,04	0,04	0,04	0,02
15	0,20	0,00	0,07	0,00	0,10	0,03	0,03	0,07	0,03	0,00	0,07	0,03	0,23	0,07	0,00	0,00	0,03	0,00	0,03	0,00
16	0,00	0,04	0,04	0,04	0,00	0,00	0,04	0,00	0,12	0,08	0,08	0,00	0,04	0,00	0,08	0,00	0,00	0,04	0,32	0,08
17	0,45	0,00	0,00	0,02	0,00	0,20	0,00	0,00	0,02	0,05	0,02	0,05	0,05	0,00	0,02	0,05	0,00	0,00	0,05	0,00
18	0,20	0,07	0,10	0,03	0,00	0,03	0,07	0,00	0,00	0,27	0,07	0,07	0,03	0,00	0,00	0,00	0,07	0,00	0,00	0,00
19	0,20	0,03	0,07	0,07	0,07	0,07	0,00	0,03	0,00	0,03	0,03	0,20	0,03	0,03	0,03	0,03	0,03	0,03	0,00	0,00

Рис. 1: Таблиця ймовірностей $P(M|C)$ для 6 варіанту

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
0	0,00	0,13	0,00	0,02	0,04	0,02	0,02	0,02	0,00	0,02	0,20	0,04	0,00	0,00	0,22	0,04	0,02	0,00	0,22	0,02
1	0,07	0,00	0,04	0,02	0,00	0,02	0,02	0,04	0,00	0,02	0,00	0,00	0,23	0,23	0,04	0,02	0,02	0,02	0,00	0,23
2	0,58	0,00	0,00	0,02	0,00	0,01	0,15	0,00	0,01	0,00	0,00	0,01	0,01	0,01	0,00	0,01	0,01	0,02	0,00	0,14
3	0,12	0,06	0,00	0,00	0,21	0,02	0,00	0,38	0,02	0,02	0,00	0,03	0,02	0,02	0,02	0,02	0,00	0,07	0,00	0,00
4	0,00	0,07	0,04	0,02	0,00	0,04	0,02	0,02	0,04	0,25	0,02	0,02	0,00	0,00	0,42	0,00	0,00	0,02	0,00	0,04
5	0,12	0,06	0,02	0,19	0,19	0,00	0,00	0,03	0,03	0,02	0,00	0,02	0,02	0,00	0,02	0,03	0,02	0,00	0,21	0,02
6	0,06	0,12	0,00	0,00	0,19	0,19	0,00	0,03	0,03	0,00	0,03	0,03	0,00	0,02	0,02	0,00	0,00	0,19	0,03	0,03
7	0,12	0,12	0,00	0,02	0,00	0,18	0,02	0,00	0,02	0,00	0,02	0,03	0,02	0,03	0,00	0,22	0,20	0,00	0,02	0,00
8	0,73	0,00	0,00	0,01	0,02	0,02	0,00	0,10	0,00	0,00	0,03	0,00	0,00	0,03	0,01	0,01	0,01	0,00	0,03	0,00
9	0,07	0,00	0,02	0,02	0,00	0,00	0,04	0,02	0,00	0,00	0,02	0,04	0,04	0,02	0,02	0,02	0,44	0,00	0,23	0,02
10	0,00	0,13	0,02	0,00	0,02	0,02	0,02	0,02	0,24	0,00	0,00	0,00	0,04	0,02	0,02	0,22	0,02	0,22	0,02	0,00
11	0,00	0,07	0,02	0,00	0,02	0,23	0,02	0,02	0,21	0,02	0,00	0,00	0,04	0,02	0,04	0,23	0,00	0,02	0,04	0,02
12	0,00	0,00	0,04	0,02	0,02	0,00	0,06	0,00	0,02	0,02	0,24	0,22	0,00	0,02	0,00	0,02	0,02	0,04	0,02	0,24
13	0,00	0,55	0,01	0,02	0,00	0,01	0,04	0,00	0,13	0,19	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,02	0,01
14	0,00	0,07	0,21	0,25	0,06	0,02	0,00	0,06	0,00	0,21	0,04	0,00	0,00	0,02	0,00	0,00	0,02	0,00	0,00	0,06
15	0,06	0,70	0,01	0,02	0,01	0,00	0,10	0,00	0,01	0,00	0,01	0,01	0,00	0,01	0,02	0,00	0,02	0,02	0,00	0,01
16	0,00	0,00	0,02	0,00	0,04	0,02	0,22	0,02	0,04	0,00	0,02	0,02	0,24	0,22	0,04	0,04	0,00	0,04	0,02	0,00
17	0,13	0,00	0,42	0,00	0,00	0,04	0,00	0,00	0,00	0,04	0,04	0,22	0,07	0,02	0,00	0,00	0,02	0,00	0,02	0,00
18	0,06	0,06	0,02	0,00	0,04	0,02	0,02	0,02	0,02	0,04	0,22	0,00	0,20	0,20	0,02	0,02	0,04	0,00	0,00	0,02
19	0,00	0,07	0,04	0,25	0,02	0,02	0,00	0,02	0,02	0,00	0,02	0,23	0,02	0,02	0,02	0,00	0,04	0,23	0,00	0,00

Рис. 2: Таблиця ймовірностей $P(M|C)$ для 6 варіанту

1.3 Результати детерміністичної та стохастичної функції

Шифротекст	Відкритий текст
0	7
1	2
2	3
3	13
4	10
5	0
6	0
7	0
8	4
9	8
10	0
11	0
12	1
13	14
14	0
15	12
16	18
17	0
18	9
19	0

Рис. 3: Результат детерміністичної функції для 6 варіанта

Шифротекст	Відкритий текст
0	14
1	12
2	0
3	7
4	14
5	18
6	4
7	15
8	0
9	16
10	8
11	5
12	10
13	1
14	2
15	1
16	12
17	2
18	10
19	3

Рис. 4: Результат детерміністичної функції для 17 варіанта

Шифротекст	Відкритий текст	Ймовірність
0	7	1
1	2	1
2	3	1
3	13	1
4	10	1
5	0, 19	0,5
6	0	1
7	0, 6	0,5
8	4	1
9	8	1
10	0, 15	0,5
11	0	1
12	1	1
13	14	1
14	0	1
15	12	1
16	18	1
17	0	1
18	9	1
19	0, 11	0,5

Рис. 5: Результат детермінистичної функції для 6 варіанта

Шифротекст	Відкритий текст	Ймовірність
0	14, 18	0,5
1	12, 13,19	0,333333333
2	0	1
3	7	1
4	14	1
5	18	1
6	4, 5, 17	0,333333333
7	15	1
8	0	1
9	16	1
10	8	1
11	5, 15	0,5
12	10, 19	0,5
13	1	1
14	3	1
15	1	1
16	12	1
17	2	1
18	10	1
19	3	1

Рис. 6: Результат детермінистичної функції для 17 варіанта

1.4 Середні витрати

Значення середніх витрат для детермінистичної вирішуючої функції:

1. Варіант 06 : 0,6704;
2. Варіант 17 : 0,6116;

Значення середніх витрат для стохастичної вирішуючої функції:

1. Варіант 06 : 0,6704;
2. Варіант 17 : 0,6116;

1.5 Опис труднощів

Основні труднощі виникали на етапі ознайомлення із теоретичною частиною, а саме з усвідомленням реалізації стохастичної вирішуючої функції.

2 Висновки

1. Ми ознайомились з принципами баєсівського підходу в криптоаналізі, побудували детерміністичну та стохастичну вирішуючу функцію для моделей схем шифрування та криптоаналіз моделей шифрів за допомогою програмної реалізації.
2. Результат застосування детерміністичної та стохастичної функції майже однакові.
3. Значення середніх витрат для детерміністичної та стохастичної вирішуючих функцій однакове та дорівнює 0,6704 для 6 варіанта; 0,6116 для 17 варіанта.

4. Проаналізувавши значення бачимо, що краще використовувати детерміністичну вирішуючу функцію, оскільки вона легше реалізовується, ніж стохастичну вирішуючу функцію, а результат, який вони дають, майже не відрізняється.