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

Попов Артем , Стасюкевич Анатолій

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.

1 Хід роботи

1. Реалізувати алгоритми програмно і подати результати побудови детерміністичної та стохастичної вирішуючих функцій у вигляді таблиць порахувати розподіли P(C), P(M,C)). Обчислити P(M|C);

2. Побудувати оптимальні вирішуючі функції, максимізувавши розподіл P(M|C);

3. Обчислити середні втрати, провести порівняльний аналіз вирішуючих функцій.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
1	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	0.04
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	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05

Рис. 1: prob_02.csv

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
1	19	13	3	16	5	10	8	1	12	14	7	2	17	11	15	18	6	0	4	9
2	15	13	17	5	2	9	7	11	3	18	0	12	8	10	6	19	1	16	4	14
3	3	4	5	12	16	14	9	10	7	11	1	13	6	18	0	2	17	19	8	15
4	3	13	19	6	9	1	2	16	14	10	5	8	18	12	17	0	11	4	15	7
5	11	7	5	12	18	1	8	14	2	6	17	9	16	10	15	13	4	19	0	3
6	5	0	1	12	9	11	4	19	7	15	14	8	6	18	13	2	3	10	16	17
7	10	18	13	11	0	17	1	14	9	15	3	5	16	12	4	2	6	19	7	8
8	6	4	15	16	10	1	8	17	2	18	11	19	3	14	0	9	5	13	12	7
9	13	0	11	14	9	10	19	4	17	12	18	7	15	5	6	1	2	3	8	16
10	16	6	15	19	2	4	14	11	9	3	1	10	17	5	0	18	12	8	7	13
11	11	7	19	18	9	2	5	10	3	15	14	16	1	17	0	12	8	6	13	4
12	11	9	0	19	17	13	12	2	10	6	18	1	5	4	8	7	15	3	16	14
13	5	9	0	7	12	11	18	17	3	13	1	16	15	8	6	2	10	14	19	4
14	12	10	17	8	3	9	4	13	0	1	15	18	19	2	6	14	5	16	7	11
15	16	15	8	13	0	11	18	17	19	12	3	4	5	9	6	10	2	1	7	14
16	16	10	17	2	0	9	19	1	5	7	4	12	13	8	18	11	6	14	15	3
17	1	13	17	15	3	14	2	10	16	7	5	6	18	8	0	19	12	9	4	11
18	17	18	7	10	14	12	3	9	15	1	19	8	2	4	11	6	13	5	16	0
19	8	2	6	4	0	7	17	19	10	14	16	9	13	3	1	12	11	18	5	15
20	17	15	8	11	2	1	10	4	12	5	18	6	16	3	7	19	9	13	14	0

Рис. 2: table_02.csv

```
0, 0.155556, 0, 0.28, 0, 0.28, 0.14, 0, 0.155556, 0, 0.127273, 0.381818, 0.155556, 0.107692, 0, 0.127273, 0.381818, 0.28, 0, 0.155556,
0.28, 0, 0.155556, 0, 0.28, 0, 0.14, 0.28, 0, 0.28, 0.254545, 0, 0, 0.430769, 0, 0.254545, 0, 0, 0.28, 0,
0.08, 0.0444444, 0, 0.04, 0, 0.08, 0.04, 0.04, 0.0888889, 0, 0, 0.0363636, 0, 0.0307692, 0, 0.0727273, 0, 0.16, 0, 0.0888889,
0, 0, 0.0444444, 0, 0.04, 0.04, 0.04, 0.04, 0.0444444, 0, 0.0363636, 0.0727273, 0.133333, 0.0307692, 0.05, 0.0363636, 0.0727273, 0, 0.04, 0.0888889,
0.16, 0, 0.133333, 0.08, 0, 0.04, 0, 0, 0, 0.16, 0.0363636, 0, 0.0444444, 0, 0.05, 0, 0.0363636, 0.04, 0.04, 0,
0, 0.177778, 0.0444444, 0, 0.04, 0, 0, 0.04, 0, 0.12, 0.0727273, 0.109091, 0.0444444, 0.0307692, 0.1, 0, 0, 0.04, 0, 0,
0, 0.0444444, 0.0888889, 0.04, 0.08, 0.04, 0, 0.04, 0.133333, 0.04, 0.0363636, 0, 0.0444444, 0, 0.05, 0, 0, 0.04, 0.08, 0.0888889,
0, 0.0888889, 0.0444444, 0, 0.08, 0, 0, 0, 0, 0.04, 0.109091, 0.0727273, 0, 0.0307692, 0.1, 0, 0.0363636, 0.12, 0, 0.0888889,
0.04, 0, 0.0888889, 0.12, 0, 0.04, 0, 0.08, 0, 0.08, 0.0727273, 0, 0.0888889, 0, 0.05, 0.0363636, 0.0363636, 0.04, 0, 0.0444444,
0, 0.0888889, 0, 0.04, 0, 0.04, 0.08, 0.08, 0, 0, 0.0363636, 0.0363636, 0.0888889, 0.0307692, 0.1, 0.109091, 0, 0, 0.08, 0,
0.04, 0.133333, 0, 0.08, 0.04, 0.08, 0, 0.04, 0, 0, 0, 0.0363636, 0, 0, 0.1, 0.0363636, 0.0363636, 0.04, 0.12, 0.0444444,
0, 0.0444444, 0.0444444, 0, 0.04, 0.04, 0.08, 0.04, 0.133333, 0.08, 0.0363636, 0, 0.0888889, 0.0307692, 0, 0, 0.0727273, 0, 0.04, 0.0444444,
0, 0.0444444, 0.0444444, 0.04, 0, 0.08, 0.08, 0, 0.0444444, 0, 0, 0, 0, 0.0615385, 0, 0.0727273, 0.109091, 0.08, 0.08, 0.0444444,
0, 0, 0.0444444, 0.08, 0.08, 0.08, 0, 0, 0.133333, 0.04, 0.0727273, 0.0363636, 0.0888889, 0, 0.05, 0, 0, 0.04, 0.08, 0,
0.2, 0.0444444, 0, 0, 0.04, 0, 0.2, 0.04, 0.0444444, 0, 0, 0.0363636, 0, 0.0307692, 0, 0.0727273, 0, 0.04, 0.04, 0,
0.04, 0.0444444, 0.177778, 0, 0, 0, 0.04, 0.04, 0, 0.04, 0.0363636, 0.0363636, 0.0888889, 0.0307692, 0.05, 0, 0, 0, 0.08, 0.133333,
0, 0.0444444, 0.0888889, 0.04, 0.04, 0.08, 0.12, 0, 0.0444444, 0.04, 0.0363636, 0.0727273, 0.0888889, 0.0307692, 0, 0.0363636, 0, 0.04, 0, 0,
0.04, 0.0444444, 0, 0.08, 0.04, 0.04, 0.04, 0, 0.0444444, 0.04, 0.0363636, 0, 0, 0.0615385, 0.1, 0, 0.0727273, 0, 0.04, 0.133333,
0.04, 0, 0, 0, 0.12, 0.04, 0, 0.16, 0.0888889, 0, 0, 0, 0.0444444, 0.0307692, 0.05, 0.0727273, 0.109091, 0, 0, 0.0444444,
0.08, 0, 0, 0.08, 0.08, 0, 0, 0.08, 0.0444444, 0.04, 0, 0.0727273, 0, 0.0307692, 0.15, 0.0727273, 0.0363636, 0.04, 0, 0,
```

Рис. 3: P(M|C)

1.1 Вхідні данні (вар.2) та Розподіл P(M|C)

1.2 Результати детерміністичної та стохастичної функції

Шифротекст	Відкритий текст	Ймовірність
0	1	0.5
1	5	0.5
2	15	0.5
3	0	1
4	1	0.5
5	0	1
6	14	0.5
7	1	0.5
8	0	1
9	1	0.5
10	1	0.5
11	0	1
12	0	0.5
13	1	0.5
14	19	1
15	1	0.5
16	0	1
17	0	1
18	1	0.5
19	0	1

Табл. 1: Результат стохастичної функції для 2 варіанта

1.3 Результати детерміністичної функції

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

Табл. 2: Результат детерміністичної функції для 2 варіанта

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. Як бачимо, результат застосування детерміністичної та стохастичної функції однаковий;

3. Значення середніх витрат для детерміністичної та стохастичної вирішуючих функцій однакове та дорівнює для 2 варіантадетерміністична ф-я) витрати = 0.263 (1.0 - витрати = 0.737);

   для 6 варіанта (детерміністична ф-я) витрати = 0.3296 (1.0 - витрати = 0.6704); (

4. Проаналізувавши значення бачимо, що краще використовувати детерміністичну вирішуючу функцію. Оскільки її легше реалізувати, ніж стохастичну вирішуючу функцію та результат майже не відрізняється.