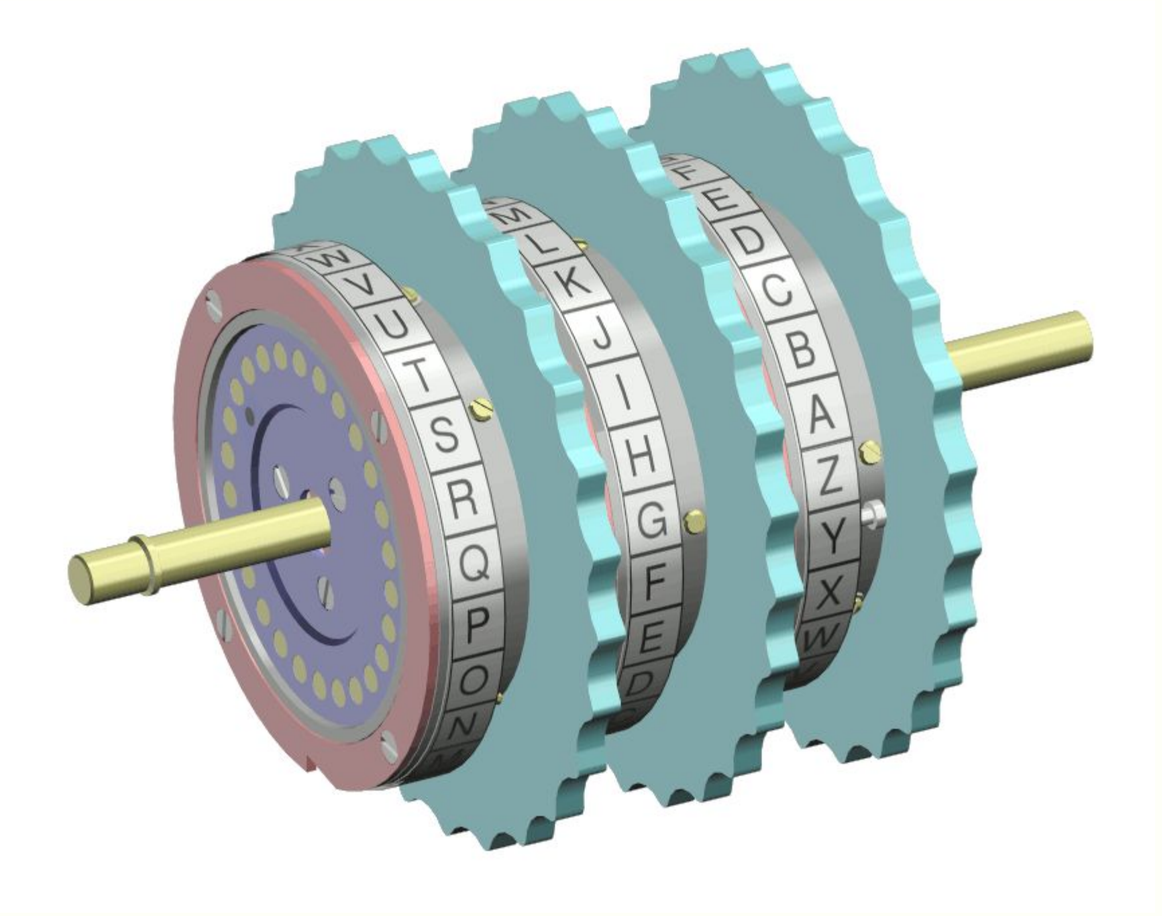
КЛАСИФІКАЦІЯ ПЕРЕСТАНОВОК ЗІ СПЕЦІАЛЬНИМИ ВЛАСТИВОСТЯМИ ТА ОЦІНКА ПОТУЖНОСТІ КЛАСІВ

Виконала: Бурлака Марія Костянтинівна

Керівник: в.о. завідувача кафедри ММЗІ ФТІ
Савчук Михайло Миколайович, д.ф.-м.н., доцент

Актуальність

- Підстановки, що досліджуються в роботі, є підключами найбільш поширених систем криптографічного захисту інформації у XX сторіччі - роторних шифрувальних машин
- Модифіковані системи роторного шифрування застосовуються і сьогодні
- Перестановки та підстановки є базовими криптографічними перетвореннями в сучасних системах захисту інформації, від якості яких залежить стійкість та ефективність систем захисту


Z
Y
X
W
V
U
T
S
R
Q
P
O
N
M
L
K
J
I
H
G
F
E
D
C
B
A
Z
Y
X
W
V
U
T
S
R
Q
P
O
N
M
L
K
J
I
H
G
F
E
D
C
B
A
Z
Y
X
W
V
U
T
S
R
Q
P
O
N
M
L
K
J
I
H
G
F
E
D
C
B
A

Мета, об'єкт та предмет дослідження

Мета дослідження:

- класифікація підстановок в ключах роторних шифрувальних машин в залежності від їх криптографічних характеристик
- експериментальне отримання статистичних оцінок потужностей класів для підстановок різного розміру

Об'єкт дослідження: ключі зашифрування у роторних машинах та їх модифікаціях

Предмет дослідження: криптографічні характеристики підстановок над алфавітами

Завдання

- Провести огляд та аналіз опублікованої літератури за тематикою
- Ввести поняття криптографічної характеристики перестановки та запропонувати класифікацію перестановок за їх характеристиками
- Створити програму для реалізації розбиття множини усіх перестановок різних розмірів на класи
- Методом статистичного моделювання оцінити потужності отриманих класів та ймовірність вибору випадкової перестановки с заданою характеристикою
- Перевірити якість оцінки потужності

Перестановки “без перепайок” та їх кількість

Означення. Перестановка $(i_0, i_1, \dots, i_{n-1})$ множини $\{0, 1, \dots, n-1\}$ є перестановкою “без перепайок”, якщо

$$\forall\ k, l \in \{0, 1, \dots, n-1\}: \quad k + i_k \pmod n \neq l + i_l \pmod n, \quad k \neq l$$

Відомі результати та їх автори

- Таблиця точних значень P_n для непарних n від 1 до 19 та оцінки P_n для n = 25, 35, 45, 55, ∞

  (Cooper C., Gilchrist R., Kovalenko[6] I.N., Novacovic D. - Deriving the number of good permutations with applications to cryptography)
- Доведено, що для n ≥ 75: $413.099e^{-0.9883n} \leq P_n \leq 267.384e^{-0.9825n}$

  (Кузнецов Н.Ю. Применение ускоренного моделирования к нахождению количества “хороших” перестановок)

Побудова характеристики $(\alpha_0, \alpha_1, \dots, \alpha_n)$ **перестановки** $(i_0, i_1, \dots, i_{n-1})$

Для заданої перестановки $(i_0, i_1, \dots, i_{n-1})$ множини $\{0, 1, \dots, n-1\}$ характеристика шукається наступним чином:

1. Знайти послідовність $(j_0, j_1, \dots, j_{n-1})$, де $j_m = m + i_m \pmod n$
2. Представити отриману послідовність у вигляді мультимножини $\{0^{k_0}, 1^{k_1}, \dots, (n-1)^{k_{n-1}}\}$
3. Знайти характеристику $(\alpha_0, \alpha_1, \dots, \alpha_n)$, де α_0 – кількість нулів серед чисел k_m, m=0,1,2,..,n-1, α_1 – кількість одиниць і так далі

Властивості характеристик перестановки

- Для $\{k_0, k_1, \dots, k_{n-1}\}$:

$$\sum_{i=1}^{n} k_i = n$$

- Для $(\alpha_0, \alpha_1, \dots, \alpha_n)$:

$$\sum_{i=1}^{n+1} i\alpha_i = n$$

Приклади характеристик перестановки

Перестановка без “паралельних перепайок”: $(0, n, 0, 0, \dots, 0)$

Перестановка з виродженою характеристикою: $(n-1, 0, \dots, 0, 1)$

Алгоритм генерування випадкової перестановки

Вхід: множина {0, 1, … , n-1}

1. Для всіх i від n-1 до 1:
    1. Обрати j ∈ {0, 1, … , i} - випадкове число
    2. Поміняти місцями i-тий та j-тий елементи

Вихід: випадкова перестановка

Алгоритм отримання статистичних оцінок потужностей класів

Вхід: множина $\{0, 1, \dots, n-1\}$

1. Встановити кількість експериментів N - велике число
2. Поки $N \geq 0$:
   1. Побудувати випадкову незалежну перестановку $(i_0, i_1, \dots, i_{n-1})$
   2. Для перестановки $(i_0, i_1, \dots, i_{n-1})$ знайти характеристику $(\alpha_0, \alpha_1, \dots, \alpha_n)$
   3. Якщо характеристика $(\alpha_0, \alpha_1, \dots, \alpha_n)$ не зустрічалася на попередніх ітераціях, встановити лічильник c = 1.
      Інакше - збільшити c на 1
3. Для кожного отриманого класу за допомогою точкової оцінки c побудувати довірчий інтервал для потужності класу, використовуючи метод Монте-Карло і апроксимацію біноміального розподілу пуассоновим та гауссовим розподілами

Вихід: інтервальні оцінки потужностей класів з різними характеристиками

Кількість перестановок “без перепайок”

n	К-ть перестановок	К-ть перестановок “без перепайок”	Точна імов-ть	Оцінка імов-ті
3	6	3	0.5	0.5
5	120	15	0.125	0.125
7	5040	133	0.0263889	0.0263889
9	362880	2025	0.00558036	0.00558036
11	39916800	37851	0.000948247	0.000948247

Порівняння кількості перестановок “без перепайок”

n	Отримана оцінка	Відома оцінка
11	0.0009506	0.000948247
13	0.0002991	0.000165467
15	0.0000498	0.0000278096
17	0.0000052	0.00000451522
19	0.0000016	0.000000720595
25	0	$2.73 \cdot 10^{-9}$
35	0	$2.25 \cdot 10^{-13}$
45	0	$1.75 \cdot 10^{-17}$
55	0	$1.32 \cdot 10^{-21}$

Деякі класи перестановок довжини 11

$(\alpha_0,\alpha_1, \dots , \alpha_{12})$	Точне значення	ДІ, побудований засобами Python	ДІ для біноміальної моделі	ДІ для нормальної моделі	ДІ для моделі Пуассона
(4, 4, 2, 1, 0, 0, 0, 0, 0, 0, 0, 0)	8252200	[8237749, 8257785]	[8239302, 8256233]	[8236124, 8256157]	[8234899, 8257393]
(5, 3, 2, 0, 1, 0, 0, 0, 0, 0, 0, 0)	2017070	[2011495, 2022333]	[2012364, 2021468]	[2011493, 2022331]	[2011354, 2022482]
(2, 8, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)	464035	[460456, 465754]	[460881, 465333]	[460453, 465753]	[460441, 465776]
(7, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)	65340	[63559, 65552]	[63721, 65394]	[63559, 65548]	[63562, 65557]
(0, 11, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)	37851	[36715, 38229]	[36836, 38113]	[36712, 38228]	[36715, 38236]
(7, 3, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)	2420	[2259, 2647]	[2290, 2620]	[2257, 2645]	[2260, 2653]
(10, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)	11	[3, 32]	[5, 37]	[0, 32]	[4, 41]

Характеристики перестановок довжини 26 та 33

$(\alpha_0,\alpha_1, \dots , \alpha_{27})$	ДІ для біноміальної моделі	ДІ для нормальної моделі	ДІ для моделі Пуассона
(9,10,5,2,0,...,0)	$[2.723086 \cdot 20^{25}, 2.73363 \cdot 20^{25}]$	$[2.722078 \cdot 20^{25}, 2.73463 \cdot 20^{25}]$	$[2.72186 \cdot 20^{25}, 2.73486 \cdot 20^{25}]$
(7,14,3,2,0,0,...,0)	$[6.06225 \cdot 20^{24}, 6.11344 \cdot 20^{24}]$	$[6.05733 \cdot 20^{24}, 6.11828 \cdot 20^{24}]$	$[6.05713 \cdot 20^{24}, 6.11859 \cdot 20^{24}]$
(3,20,3,0,0,0,...,0)	$[1.40603 \cdot 20^{21}, 1.01765 \cdot 20^{22}]$	$[7.92611 \cdot 20^{21}, 1.03027 \cdot 20^{21}]$	$[7.96474 \cdot 20^{21}, 1.0383 \cdot 20^{21}]$
(17,1,5,1,0,1,0,1,0,...)	$[2.06861 \cdot 20^{18}, 1.91316 \cdot 20^{20}]$	$[0, 1.19373 \cdot 20^{20}]$	$[1.02105 \cdot 20^{18}, 2.24699 \cdot 20^{20}]$

$(\alpha_0,\alpha_1, \dots , \alpha_{34})$	ДІ для біноміальної моделі	ДІ для нормальної моделі	ДІ для моделі Пуассона
(11,13,7,2,0,...,0)	$[3.96965 \cdot 10^{35} , 3.98856 \cdot 10^{35}]$	$[3.96784 \cdot 10^{35} , 3.9035 \cdot 10^{35}]$	$[3.96758 \cdot 10^{35} , 3.9063 \cdot 10^{35}]$
(10,17,3,2,1,0,...,0)	$[4.56102 \cdot 10^{34} , 4.62664 \cdot 10^{35}]$	$[4.55469 \cdot 10^{34} , 4.63278 \cdot 10^{35}]$	$[4.55467 \cdot 10^{34} , 4.63305 \cdot 10^{35}]$
(9, 19, 2, 2, 1, 0, . . . , 0)	$[7.470017 \cdot 10^{33}, 7.73807 \cdot 10^{33}]$	$[7.44393 \cdot 10^{33}, 7.76230 \cdot 10^{33}]$	$[7.44469 \cdot 10^{33} , 7.76406 \cdot 10^{33}]$
(9,21,0,2,0,0,1,0,...,0)	$[1.71074 \cdot 10^{30} , 9.12880 \cdot 10^{30}]$	$[1.71074 \cdot 10^{30} , 9.12880 \cdot 10^{30}]$	$[1.40972 \cdot 10^{30} , 1.01320 \cdot 10^{31}]$

Висновки

- Введено поняття характеристики перестановки, що узагальнює поняття перестановки “без паралельних перепайок”
- Розроблено алгоритм та програма для побудови класів перестановок довільного порядку за їх характеристиками
- Методом статистичного моделювання отримано точечні та інтервальні оцінки потужності класів для перестановок довжини 11, 26, 30, 31, 32, 33, 45 та 55 з різними характеристиками. Перевірена якість оцінок.
- Показано, що ймовірність випадково вибрати перестановку з високими криптографічними властивостями швидко зменшується з ростом порядку перестановки

Дякую за увагу!