

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Московский Авиационный Институт»
(Национальный Исследовательский Университет)

Институт: №8 «Информационные технологии и прикладная
математика» Кафедра: 806 «Вычислительная математика и
программирование»

Лабораторная работа № 4 по
курсу
«Криптография»

Группа: М8О-306Б-20

Студент: И. П. Попов

Преподаватель: А. В. Борисов

Оценка:

Дата:

Москва, 2022

Задача

Сравнить:

1. два осмысленных текста на естественном языке,
2. осмысленный текст и текст из случайных букв,
3. осмысленный текст и текст из случайных слов,
4. два текста из случайных букв,
5. два текста из случайных слов.

Как сравнивать: считать процент совпадения букв в сравниваемых текстах – получить дробное значение от 0 до 1 как результат деления количества совпадений на общее число букв. Расписать подробно в отчете алгоритм сравнения и приложить сравниваемые тексты в отчете хотя бы для одного запуска по всем пяти подпунктам. Осознать какие значения получаются в этих пяти подпунктах. Привести свои соображения о том почему так происходит. Длина сравниваемых текстов должна совпадать. Привести соображения о том какой длины текста должно быть достаточно для корректного сравнения.

Ход работы

Алгоритм сравнения заключается в посимвольном сравнении текстов текстов латинского алфавита. Процент совпадения считается как отношения числа совпавших букв к числу символов в тексте.

Функция сравнения текстов:

```
public static double filesCompareByByte(Path path1, Path path2) throws IOException {
    long length = 0;
    long coincidence = 0;

    try (BufferedInputStream fis1 = new BufferedInputStream(new FileInputStream(path1.toFile()));
        BufferedInputStream fis2 = new BufferedInputStream(new FileInputStream(path2.toFile()))) {
        int ch1;
        int ch2;
        while ((ch1 = fis1.read()) != -1 && (ch2 = fis2.read()) != -1) {
            if (ch1 == ch2) coincidence++;
            length++;
        }
    }
    return (double) coincidence / length;
}
```

Финальная функция для вывода результатов:

```
public static void main(String[] args) throws IOException {
    System.out.println("Test 3");
    Path fileText1 = Path.of("src\\cripto\\symbols1000\\fileText1.txt");
    Path fileText2 = Path.of("src\\cripto\\symbols1000\\fileText2.txt");
    Path fileSymbols1 = Path.of("src\\cripto\\symbols1000\\fileSymbols1.txt");
    Path fileSymbols2 = Path.of("src\\cripto\\symbols1000\\fileSymbols2.txt");
    Path fileRandom1 = Path.of("src\\cripto\\symbols1000\\fileRandom1.txt");
    Path fileRandom2 = Path.of("src\\cripto\\symbols1000\\fileRandom2.txt");

    System.out.println("два осмысленных текста на естественном языке");
    System.out.println(filesCompareByByte(fileText1, fileText2));

    System.out.println("осмысленный текст и текст из случайных букв");
    System.out.println(filesCompareByByte(fileText1, fileSymbols2));

    System.out.println("осмысленный текст и текст из случайных слов");
    System.out.println(filesCompareByByte(fileSymbols1, fileRandom2));

    System.out.println("два текста из случайных букв");
    System.out.println(filesCompareByByte(fileSymbols1, fileSymbols2));

    System.out.println("два текста из случайных слов");
    System.out.println(filesCompareByByte(fileRandom1, fileRandom2));
}
```

Пример текстов

fileText1 (файл с осмысленным текстом 1)

```
Those hours, that with gentle work did frame
The lovely gaze where every eye doth dwell,
Will play the tyrants to the very same
And that unfair which fairly doth excel;
For never-resting time leads summer on
To hideous winter, and confounds him there;
Sap checked with frost, and lusty leaves quite gone,
Beauty o'er-snowed and bareness every where:
Then were not summer's distillation left,
A liquid prisoner pent in walls of glass,
Beauty's effect with beauty were bereft,
Nor it, nor no remembrance what it was:
But flowers distilled, though they with winter meet,
Leese but their show; their substance still lives sweet.

Then let not winter's ragged hand deface,
In thee thy summer, ere thou be distilled:
```

Make sweet some vial; treasure thou some place
With beauty's treasure ere it be self-killed.
That use is not forbidden usury,
Which happies those that pay the willing loan;
That's for thy self to breed another thee,
Or ten times happier, be it ten for one;
Ten times thy self were happier than thou art,

fileText2 (файл с осмысленным текстом 2)

Lo! in the orient when the gracious light
Lifts up his burning head, each under eye
Doth homage to his new-appearing sight,
Serving with looks his sacred majesty;
And having climbed the steep-up heavenly hill,
Resembling strong youth in his middle age,
Yet mortal looks adore his beauty still,
Attending on his golden pilgrimage:
But when from highmost pitch, with weary car,
Like feeble age, he reeleth from the day,
The eyes, 'fore duteous, now converted are
From his low tract, and look another way:
So thou, thyself outgoing in thy noon
Unlooked on diest unless thou get a son.

Music to hear, why hear'st thou music sadly?
Sweets with sweets war not, joy delights in joy:
Why lov'st thou that which thou receiv'st not gladly,
Or else receiv'st with pleasure thine annoy?
If the true concord of well-tuned sounds,
By unions married, do offend thine ear,
They do but sweetly chide thee, who confounds
In singleness the parts that thou shouldst bear.
Mark how one string, sweet husband to another,

fileSymbols1 (файл из случайных символов 1)

PPZTcBoAFRUodBoCRGuibkXonwfvIHcQbbdmNYydcnfXyexSjMdshEPilPvjuBodjtbhpcIIhQ
EOwqtKmIQsnsImYsrJfPPQjKGZWVgMdhhcIqgaEUJZIRRCsmVVREgvUQRGfDXobLUVAYhWMmCvE
gTJRjXqHvlsaeLpEPSRNpSgXEVixxGPeRXNpDNhWszkmjfuIXBkxrfCxakVFvvCLkMBkiKRBHFn
jGNPcNxfwFUCRDYLQsbJHGkQeVtSlsOpslQjqYAMYHWWlSCotzTwkUZNxRYrIgJZIUFGrCoAhSb
slqFaoVmmzVBRKFZrOLcVtrQVXpZJahIGYNIXCKLcHdvvvWCOqystYkpHtSNEHWiludJjQnXrem
BgdrPBoHogcLzSyyxLMXYGaaEXPuEMaZZtRNQjJdAHmeZrfIFufpLQjDawgexxGzIzqaGJHYkfG
egJhstxrryQTBiOIObCDQHtGuRqloyrXPFTGJBrSjxFGmCuDwrakqaCLHAMyrYhkcGzJjUbrsHh
FompnTJQADiAMNEbUMuhZiViHElvArKnOppmQfmBhsNGhHuwOqfzhmoleBfJdblSatGiXdtKRHn
aFIBEqHfPSTOSdHFaChStdIBUdUahPXHUSiXshwtjKAoaknmpIcJfQwuPeCZZIaXmfpSTBiYcbq
WlrnMHAqsrtTzVMBRChLZPiNsOrkvfWWxMztugjWkEXvHwoZmkjFwbAlekTbTdIqmFlPGyzEbNk
uxrwkBbTyliWuPbEAdUCXCaUirRscRwMouWAOQTYsSYMygZBIxFXsAGMlISJfKuHJMPNRSRSUm
VVERTJLdRPTvKbuzSoVVGobWcbgyohUezPmqVumkeflkyNEblQrfNEKYiahMYFqxkdpAKWmSJMu
FsdLsbHSPnNPrtcIJxOOWnmhQYnZamujcVarJZNPrKXFJUNrTTnyNdyncLrIYFpcEeIwRsIgcx
CkPzkNlUNoRSeTaWmwGldvWKf

fileSymbols2 (файл из случайных символов 2)

qbBnoWxDlZgWyBrwbGxhfdQggJPHpSGbWwjAzExcussyItowOHRqubPetTWpcmYnrcfJztbtSfBf
JyGhWOBJSXeZTJKjvEnWujKxChQqfdVWKZMMeZampqCifcVIZpxZMDUpdyhIkWgeJVfkKwxWXWG
EADocvHozWtdomsCsMOjDNZwuVgqzupJsQdMyiidJkYrjmZEdxnXznKUOXxMatcfLPMJjbGfGME
aAyYWVzfjdpUsYNQKSpnjZErmNzcMgXxYcuzbbUByZsjUzrCsXBUvEVHZmuHbRDUDeCuxveIsUa
lqKbriVLyegEvPnLKGKHUNSMdxZwsYlHpWWsgpZjubQuLRIZKwnGwkwRfPovPvPOOajNlDtjzN
KFDclqyDVubEQgpOBicnjYDdqIEeoysIRiUxYuvhfbibAYqVNeCWBgFiOuWOMdlsvaEvcSPUCI
rLXmCJQjCUXUCnNXnERKuQdqmaCTApSjrrbBzYMORSueQoYUAgldragGSrmRLXfenVRkmnIWkKE
ttuGVIVWjgDZsCcXAtMuVYSrEvnBVqNAJRcYqntagjyLAElMomRWiiAeucqNHqIgvUxvTwRQJK
wjGgnuwlJBBeEKFsAxjzvMhlFntcOGtRJZXucMFxWhoXWZUvLurxlsZUdsMzZvreNLqGrKsOzJA
lCMEmEYpKnihLTSQiZZYdIJuLrAVcIsxbVwWXXSLbsEPepuKSAUdjggVdXPlzEgECIyhSdaqfOBi
kSgJbAKAVhdLzOyyUjeqMXHPsdGegwcVMfHTFCwPMMgsqQLwPytMBFibLPBOzayyCkjjzdkENQnG
SDhFyeHXeCXMrISLWhQIPwuyvtQbvYPEDaCfnJpxXxjvEySXDkxiuEgWEQLREgxsJQJXAYOodY
xdCffYtSJFWtJSGuanDRplLFCDNdEhntKRgxdhChbbavytOeuZDbAvfOloZNPZjapRStoXeaExA
ibnfOJgfdyxoIWiWjaYuAjWcd

fileRandom1 (файл из случайных слов 1)

ludicrous recollection homely degradation triumph veal bug impractical
glitter bold slab playmate denounce refrain ban agenda rye fastest form
lifting entrust button acoustic tunnel light declining matinee haunt lichen
appalled leaning snare broadcast desolation exaggerate thumb exclusionary
censure strew mimetic plain disembark allocation treasure terrified
convincing addictive sweat premature attacker uninsured exchange trigger
prenatal deplete looter sedan ferocious internal synthesizer innuendo
repulsive reunite docile particle flattery smash rev deserted fund-raising
global holocaust balding utter prize pulse uncomplicated spurious
trustworthy oppression holy tumble landowner underdeveloped heyday esteem
nostril explosives snatch endure pride icy cartoonist roomy globular
exquisite brake deference crossover cube deal brace hormonal mortal beating
titan serbian sadness magician archaic pointless vilify hiss textual rock
enriched obnoxious zulu down shining governmental whale embarrassment

fileRandom2 (файл из случайных слов 2)

spark contradict intercede divided ultraviolet horrible carbon
inspirational stimulate standardize corporal interlocking countryside
unmistakable shed windfall ghostly chloride aggregation view takeoff tailor
masculine recurrence patriarchy pellet sheath wrong lime gale delightful
enigma strike payer mater headliner chemistry evolve paranoia troublemaker
choppy dill imbue block app dislodge squeak backing successive permeate
wily trove polished elated chicken vine antagonist seafood pistol manage
complement weigh try underwear idle ascending urge governing host float
aryan inhuman finder backpack paternity marked maker no-brainer drawback
laurel shut controller ethanol thrust luncheon slalom certified scorecard
prompt perfume deem imprint conceptual pedal holiness moderate asparagus
dominion yearly time-honored enclosed realistic shoot villa box discord
vampire hallowed circumvent staple dunk snack syringe pragmatist challenge
attainable half flex heroine tar enmity musical eyebrow laser

Результат работы

Тест1 (100 символов)

два осмысленных текста на естественном языке

0.058823529411764705

осмысленный текст и текст из случайных букв

0.01

осмысленный текст и текст из случайных слов

0.02

два текста из случайных букв

0.02

два текста из случайных слов

0.05263157894736842

Test 2 (500 символов)

два осмысленных текста на естественном языке

0.05415860735009671

осмысленный текст и текст из случайных букв

0.016

осмысленный текст и текст из случайных слов

0.008

два текста из случайных букв

0.02

два текста из случайных слов

0.07168458781362007

Test 3 (1000 символов)

два осмысленных текста на естественном языке

0.06555772994129158

осмысленный текст и текст из случайных букв

0.016

осмысленный текст и текст из случайных слов

0.017

два текста из случайных букв

0.017

два текста из случайных слов

0.0631111111111112

Выводы

В ходе этой лабораторной работы мною был проведен эксперимент по сравнению осмысленных текстов, текстов из случайных слов и текстов из случайных букв в различных их комбинациях. Наибольший процент совпадений показали осмысленные тексты, так как в них вероятность следования символа В за символом А больше (как части одинаковых слов, слогов и тд), нежели в остальных текстах. Наименьший процент совпадений, показали тексты из случайных слов, что не удивительно, ведь там нет никаких зависимостей между буквами.