Ступникова Екатерина Петровна, 2 курс, направление ИТМ

Лабораторная работа № 1

Скитала

Цель работы

Реализовать современными средствами алгоритм шифрования, используемый в древней Спарте. Ознакомиться с особенностями и принципами блочного шифрования.

Задание

1. Реализовать современными средствами алгоритм шифрования, используемый в древней Спарте.
2. Реализовать обратную операцию расшифровки.
3. Улучшить алгоритм шифрования так, чтобы можно было зашифровать строки текста размером меньше, чем n*m, дополняя их пробелами.
4. Улучшить алгоритм шифрования так, чтобы можно было зашифровать строки текста размером больше n*m.
5. Модифицировать код так, чтобы он работал теперь с содержимым текстовых файлов. Один содержит исходный текст, второй – зашифрованный, третий – результат расшифровки.
6. Зашифровать таким образом 5 разных файлов с текстом с разными ключами с ограничением 12 <= n*m <= 36.
7. Дешифровать их, не зная ключа, путем перебора возможных размерностей матриц n*m и просмотра результатов дешифрования вручную.

Результаты выполнения задания

Программа была реализована с использованием языка программирования Java.

Полный код проекта доступен в репозитории: https://github.com/stupnikova-katya/scytale

Для запуска программы необходимо выполнить ru.scytale.Main#main(String[] args).

В ходе последовательного выполнения пунктов 1-6 были созданы 5 файлов с зашифрованным текстом.

«Алиса в стране чудес»

Зашифрованный фрагмент	**Дешифрованный фрагмент**
С кдгарджуеиж -онккаа,чид неЕансеьлт?ис яАи ?дтееимс лтнееай д с в змсо, л онтпыорш еккдоаемкли сткяьо ,нв чтгаодеретниеек т,нс аяач исгнрдаедииайс?са ктАиенйлг ьлп Лриьртюоаиллсл, Ксчэчтоо инэсатхвоое дрпинртоеб уогдкдьее а-нннаоидм,тл аьакш ииоеен ибм ооораеян ыти а ико квпеслотах,мо чнзтанода ютнисВмхоиот д пинртио…ки тоио дгиед лан ,ен иквкакки твсстгяоа рнсноривед гооогй о.н евМя нссонтртоаржнаннноое й,з асМпуиит тазьтасьбясл,яу дДаштжк еип омб уесргпауин вепи,рт еьЕд,сс лтчиатося л.му очВжидетртьу сг рибо упндауесжтте ьнп пС ртлырижу осскир,ша ьзуем?ше ьлП орл?ыи г Анс? куЭ-ж.то.ок.,, ТдВар эвлтсоое.м -иДт оодб еров чису тдзреласон е-еркзеадчкеа юивт ссвтя,ьь к Нооо н зитд оежлсиварузетнг ыанхха . б	Скажи-ка дружок, где начинается день? А? Если идти над землей вместе с солнышком, то как определить, где кончается вторник, а где начинается среда? Английский писатель Льюис Кэрролл считал, что это происходит наверное где-нибудь над океаном, а они такие большие моря и океаны и все так плохо знают, что там над ними происходит… Вот никто и не видел никогда, как вторник становится средой. Много неясного в странной стране, Можно запутаться и заблудиться, Даже мурашки бегут по спине, Если представить, что может случиться. Вдруг будет пропасть и нужен прыжок, Струсишь ли сразу? Прыгнешь ли смело? А? Э... Так-то, дружок, В этом-то все и дело. Добро и зло в стране чудес - как и везде встречаются, Но только здесь они живут на разных берегах.

«Война и Мир»

Зашифрованный фрагмент	**Дешифрованный фрагмент**
Ндтаоо ряколрг аидю у сб.нс ояВ,те ьрв о рядатез босестртаеарзвш,ле я свш вио хнд елбсеыяслт, ь щдрева,аз ирт аовзл а жевдзыоышй.е бЭкетаро о бмдынвлыа й о,ог брвхв,ма атсна н оыдбмулибо, вудикадавнмноио, , и с сно нйоо,бй л зокамораросряшычемкйиа мсбито.ал Сым миои г нрсеовумокнилюинжмоем ,ер танрсеитсчопимы ирк еорнрунякывамымиц асимт иап,ра ыломьн, мрс иеитр едплирьтенызым е сжутдроуоя длуо лммыбяма июб.ще ирТмеоизлсаькитоне лон неп оохддочиовнбеяастяньныси яюи н неви и хдвоееттсеьнл ы,не цснани.а	На краю дороги стоял дуб. Вероятно, в десять раз старше берез, составлявших лес, он был в десять раз толще, и в два раза выше каждой березы. Это был огромный, в два обхвата дуб, с обломанными, давно, видно, суками и с обломанной корой, заросшей старыми болячками. С огромными своими неуклюже, несимметрично растопыренными корявыми руками и пальцами, он старым, сердитым и презрительным уродом стоял между улыбающимися березами. Только он один не хотел подчиняться обаянию весны и не хотел видеть ни весны, ни солнца.

«Сказка о Царе Солтане»

Зашифрованный фрагмент	**Дешифрованный фрагмент**
Вр ел оле м яИритноге акеаруткб потнжс оон; иевлдя бтб нгеОе евах дхрхое ру у.рлНатпс аьазыааКбщидт кбелкисНол пивяаритя я, акотсНнмооЧ яааосвув, кмтуди зо р одяа:рнйалтя оо та вГдвзовнуо ылгыйрасеюсо,ин п тй ськкза;Пт роав Пипт яКбу раптолшсина,рюк сил а пт яПт аравтраксите.ию тсьл стзаво;яГоо ес звнви тКьи ехгин дзт вс	Ветер на море гуляет И кораблик подгоняет; Он бежит себе в волнах На раздутых парусах. Корабельщики дивятся, На кораблике толпятся, На знакомом острову Чудо видят наяву: Город новый златоглавый, Пристань с крепкою заставой; Пушки с пристани палят, Кораблю пристать велят. Пристают к заставе гости; Князь Гвидон зовет их в гости, Их он кормит и поит

«Анна Каренина»

Зашифрованный фрагмент	**Дешифрованный фрагмент**
КниЩайнетец я иркбжК боылонал осатеО ьдьтнвмц .а зар увж вз.ыапуи елеюмУси в ип веб ее тыбхеселол,мееть иеашчох реебсшиер ь хс,бшч т оеесеил,м еиаяяд д г.аоаки жжлннМат,оо ло штогчюиа отн,нциасс уе ккбю моиащновхлапиеллхо ию,чвб б тсывлевтуврн иж выК,епу и ею уеаидз двсвипсиьемртл сеер:вез т ирнпиЛньыаие иос лг,т пео чжо таесеотдг нйъарВс.е,арк з фоиПое ивчянЛн авиеанллев ае ыгаесз,ос еи тпщмечыоенинлв и аюьКяяяб и в октилоо в ивмпыб о емыпдкр семзо ез грмрнроаеьыавмждоеит удл ие ияК ертмии бщт пмунико до рмусисаежке гюднмки.уя нн зияеКн соЛябнтнезыаоевьл р ингр наоичои,влтнч о,о егел ш о алед жеуглнетчоя иннеоК.яя,	Княжне Кити Щербацкой было восьмнадцать лет. Она выезжала первую зиму. Успехи ее в свете были больше, чем обеих ее старших сестер, и больше, чем даже ожидала княгиня. Мало того, что юноши, танцующие на московских балах, почти все были влюблены в Кити, уже в первую зиму представились две серьезные партии: Левин и, тотчас же после его отъезда, граф Вронский. Появление Левина в начале зимы, его частые посещения и явная любовь к Кити были поводом к первым серьезным разговорам между родителями Кити и ее будущности и к спорам между князем и княгинею. Князь был на стороне Левина, говорил, что он ничего не желает лучшего для Кити.

«Мастер и Маргарита»

Зашифрованный фрагмент	**Дешифрованный фрагмент**
Слц ж нжлонеуесиаос а ыо ооьндЛсйГрй,ибл т оа ыаэагр оелн вйы цпеадонмоцпеим Т аелне. акваеиса л,члрйкяаа топррзл рк ееeаапоуртр уьоооаоупт кл плдя ыь ыоун,рсювшл ервкмвакХвоси ортмгрд.Птоа ооа уь л е ж ы дянеуеблпргтве.Пхтиоолн еоиныкпаоисоц апдкйкй оот таиикгрыодвл всооысоиа трн кпщ лдй уо еюе,млвиврбюо,иаа ылдв л,рсяипдиа он онмяд еб еы тлыпаблесоб ыл,вшан ееи ыл апркрсо,гесоиетк д хдлиьдедрг:юс в оои жня еуа иа,вдщявВфле,исвр-аем ееозпаня–вЯф.Ада фу лапнсаьп е оелс освеозпдо оор-аанйдрге еж апдк.Т екпаоийыбл аспнц ыирсыаы окамдрг,п ря оои избаормно алгвеен оисгаиснен онл е всооывекр трн с аавн,сеишенаы пшви а рзнквЕшлпади рааи.Тлыбгмлм оп ооояцвсол акпе тяиз апаоицм,пкндкйаи оиувсо рмны вивеенепооаы ар,рлстешты асиуы рм акнтепяон тае рйяоорв.Под клоклмта л иоер,ааобгаавоу оонл трюкгот онеонгрумлинсоо еин евялгоаипра пдша орвеоол,пкы щеклмт,кпд иоер онои ыо оы жюЛсйГр.Здс н	Солнце уже снижалось над Лысой Горой, и была эта гора оцеплена двойным оцеплением. Та кавалерийская ала, что перерезала прокуратору путь около полудня, рысью вышла к Хевровским воротам города. Путь для нее уже был приготовлен. Пехотинцы каппадокийской когорты отдавили в стороны скопища людей, мулов и верблюдов, и ала, рыся и поднимая до неба белые столбы пыли, вышла на перекресток, где сходились две дороги: южная, ведущая в Вифлеем, и северо-западная – в Яффу. Ала понеслась по северо-западной дороге. Те же каппадокийцы были рассыпаны по краям дороги, и заблаговременно они согнали с нее в стороны все караваны, спешившие на праздник в Ершалаим. Толпы богомольцев стояли за каппадокийцами, покинув свои временные полосатые шатры, раскинутые прямо на траве. Пройдя около километра, ала обогнала вторую когорту молниеносного легиона и первая подошла, покрыв еще километр, к подножию Лысой Горы. Здесь она спешилась. Командир рассыпал алу на взводы, и они

пшлсеьоасеиаь.Кмни асп оадррсыалаун зоы л аввд,и н цпл с оиоеиивепонженвскгдои еыооо ом,отввсхла саи воонмтлк дбды оьооинпде анг оъмн еос фсо оои Яфкйдрг.	оцепили все подножие невысокого холма, оставив свободным только один подъем на него с Яффской дороги.

В ходе работы были использованы следующие пары ключей:

1. 2,6
2. 2,7
3. 2,8
4. 2,9
5. 2,10
6. 2,11
7. 2,12
8. 2,13
9. 2,14
10. 2,15
11. 2,16
12. 2,17
13. 2,18
14. 3,4
15. 3,5
16. 3,6
17. 3,7
18. 3,8
19. 3,9
20. 3,10
21. 3,11
22. 3,12
23. 4,3
24. 4,4
25. 4,5
26. 4,6

27. 4,7
28. 4,8
29. 4,9
30. 5,3
31. 5,4
32. 5,5
33. 5,6
34. 5,7
35. 6,2
36. 6,3
37. 6,4
38. 6,5
39. 6,6
40. 7,2
41. 7,3
42. 7,4
43. 7,5
44. 8,2
45. 8,3
46. 8,4
47. 9,2
48. 9,3
49. 9,4
50. 10,2
51. 10,3
52. 11,2
53. 11,3
54. 12,2
55. 12,3
56. 13,2
57. 14,2
58. 15,2
59. 16,2
60. 17,2
61. 18,2

Для получения пар ключей был реализован метод ru.scytale.utils.FileUtils#getNumsOfMatrixInFile. А полный список пар всех ключей находится в файле src/resources/KEYS.txt.

Сведения для дешифруемых текстов в виде скриншотов:

```
Название файла: text1.txt
Количество символов: 6697
Время, занятое на перебор ключей алгоритмом: 30с.
Правильный вариант ключа: 8 3
Номер правильного варианта ключа среди перебираемых: 45
```

```
Название файла: text2.txt
Количество символов: 3073
Время, занятое на перебор ключей алгоритмом: 20с.
Правильный вариант ключа: 8 3
Номер правильного варианта ключа среди перебираемых: 45
```

```
Название файла: text3.txt
Количество символов: 17377
Время, занятое на перебор ключей алгоритмом: 20с.
Правильный вариант ключа: 4 8
Номер правильного варианта ключа среди перебираемых: 28
```

```
Название файла: text4.txt
Количество символов: 5905
Время, занятое на перебор ключей алгоритмом: 14с.
Правильный вариант ключа: 4 6
Номер правильного варианта ключа среди перебираемых: 26
```

```
Название файла: text5.txt
Количество символов: 4609
Время, занятое на перебор ключей алгоритмом: 6с.
Правильный вариант ключа: 2 9
Номер правильного варианта ключа среди перебираемых: 4
```

Сведения для дешифруемых текстов в виде сводной таблицы:

Название файла	**Количество символов**	**Время, занятое на перебор ключей алгоритмом**	**Правильный вариант ключа**	**Номер правильного варианта ключа среди перебираемых**
text1.txt	6697	30 с	8 3	45
text2.txt	3073	20 с	8 3	45
text3.txt	17377	20 с	4 8	28
text4.txt	5905	14 с	4 6	26
text5.txt	4609	6 с	2 9	4

Ответы на контрольные вопросы:

1. Отправителю и получателю шифрованных сообщений необходимо знать только ключ (n * m) для успешного шифрования/дешифрования сообщения. Ни длина текста, ни количество блоков, на которое он будет потом разбит, для пользователей не имеет значения.
2. Варианты ключей, где одно из значений пары было равно единице, были отброшены, так как такой ключ не влияет на результат шифрования (текст остается неизменным).

Выводы

Я изучила алгоритм шифрования Скитала, узнала основные принципы работы блочных шифров, реализовала данный алгоритм в программе с использованием

языка программирования Java и провела эксперимент с перебором возможных ключей для дешифрования текстов.