**Лабораторная работа №1**

*Тема:* [*Классические шифры*](https://wiki.soiro.ru/%D0%9A%D0%BB%D0%B0%D1%81%D1%81%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B5_%D1%88%D0%B8%D1%84%D1%80%D1%8B)

*Введение:*В данной лабораторной работе вам необходимо программнореализовать два классических шифра. Это могут быть:

* [Шифр простой замены](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%BF%D1%80%D0%BE%D1%81%D1%82%D0%BE%D0%B9_%D0%B7%D0%B0%D0%BC%D0%B5%D0%BD%D1%8B);
* [Аффинный шифр](https://ru.wikipedia.org/wiki/%D0%90%D1%84%D1%84%D0%B8%D0%BD%D0%BD%D1%8B%D0%B9_%D1%88%D0%B8%D1%84%D1%80);
* [Шифр Хилла](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%A5%D0%B8%D0%BB%D0%BB%D0%B0);
* [Шифр Виженера](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%92%D0%B8%D0%B6%D0%B5%D0%BD%D0%B5%D1%80%D0%B0).

Данные шифры не отличаются высокой криптостойкостью, однако хорошо иллюстрируют приемы, которые могут применяться для шифрования сообщений. Дополнительную информацию вы можете посмотреть в [лекции](https://drive.google.com/open?id=1lWbQ5N0rG_I0m1B9Su00cNAiYbLVE7YF).

*Алфавит:* Во всех заданиях (в том числе и бонусных) используетсяодинаковыйалфавит:33заглавные русские буквы от «А» до «Я»(«АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ»).

*Шифр простой замены:* В качестве ключа задается вторая строкаподстановки: она должна содержать все символы алфавита, записанные в произвольном порядке по одному разу каждый.

*Аффинный шифр:* В качестве ключа задается ключевая пара,где = 1 и.

*Шифр Хилла:* В качестве ключа задается матрица 2 × 2, все элементыкоторой лежат в кольце , а определитель по модулю 33 не равен 0 и взаимно простой с 33. Матрица указывается построчно.Для шифрования следует умножать вектор с открытым текстом на матрицу-ключ, а для расшифрования – вектор с шифротекстом на обратную матрицу ключа.

*Шифр Виженера:* В качестве ключа задается строка произвольнойдлины*,* состоящая из символов алфавита.

*Условие лабораторной работы:* Ваша задача – реализация двухклассических шифров согласно вашему варианту (первый шифр смотрите в таблице № 1, второй – в таблице №2). Под реализацией следует понимать компьютерную программу, написанную на одном из доступных языков программирования: {С/С++, C#, Java, Python, R}, которая для каждого шифра принимает на вход открытый текст или шифротекст (и тот, и другой состоят из заглавных символов русского алфавита), ключ (формат которого описан выше) и указание, какую нужно проводить операцию (зашифрование или расшифрование). На выходе у вас должен быть шифротекст или открытый текст,в зависимости от выбранной операции. При этом ваша программа должна корректно обрабатывать ситуации некорректного ключа. Обратите внимание: в итоге ваша программа должна уметь зашифровывать и расшифровывать сообщения каждым из двух шифров, которые вы реализуете.

*Отчет:* Реализовав шифры, вам необходимо продемонстрировать ихработу, зашифровав открытый текст из таблицы №1 и расшифровав шифротекст из таблицы №2, согласно вашему варианту. Результаты операций необходимо поместить в текстовый файл, назвав его «Report.txt».

Таблица №1: Зашифровать текст согласно вашему варианту

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№ вар.** | **Шифр** | **Ключ** | **Открытый текст** |  |
| 1. | Простой замены | ЬИУЗРОЫЭБХГШТЦНЁКЖПЛВЩЧЙМЮ | КРИПТОГРАФИЯ |  |
| СЯЪДФАЕ |  |
|  |  |  |  |
| 2. | Аффинный | 2 14 | МАТЕМАТИКА |  |
| 3. | Хилла | 26 30 20 32 | КРИПТОЛОГИ |  |
| 4. | Виженера | ИЕЮ | ШИФРТЕКСТ |  |
| 5. | Простой замены | ГЛФЫЗШБЖХЁПВЧНКЪЭДЬРЕТСАМЮ | КОНФИДЕНЦИАЛЬНОСТЬ |  |
| ЦЩЯУИОЙ |  |
|  |  |  |  |
| 6. | Аффинный | 10 25 | КРИПТОАНАЛИЗ |  |
| 7. | Хилла | 6 14 2 7 | СТАТИСТИКА |  |
| 8. | Виженера | НЦР | ЦЕЛОСТНОСТЬ |  |
| 9. | Простой замены | СПГЁИФЦУЛХМКЩЫЪВОЮЭНДТЯЬЙЗ | ДОСТУПНОСТЬ |  |
| ШЖБЕЧАР |  |
|  |  |  |  |
| 10. | Аффинный | 17 24 | КРИПТОСИСТЕМА |  |
| 11. | Хилла | 25 25 18 22 | НАДЕЖНОСТЬ |  |
| 12. | Виженера | ЯЬА | ИНВОЛЮЦИЯ |  |
| 13. | Простой замены | БЯЖЬНВЩГЗПКШЪДОМЁЙЦИЧУЫЮАЭ | ФАЛЬСИФИКАЦИЯ |  |
| ЕТЛСХРФ |  |
|  |  |  |  |
| 14. | Аффинный | 31 25 | НАРУШЕНИЕ |  |
| Таблица №2: Расшифровать текст согласно вашему варианту | | | |  |
| **№ вар.** | **Шифр** | **Ключ** | **Шифротекст** |  |
| 1. | Аффинный | 29 29 | ЬЮИНЛЦЩЁ |  |
| 2. | Виженера | ЩДР | ЁДЮЭДБВС |  |
| 3. | Простой замены | ЪЗЙЩЛШУИРДЧЁСФЕТЦЭМАВПЯБЫЖ | ЪЗЭДЁТМ |  |
| ЮОХНЬГК |  |
|  |  |  |  |
| 4. | Хилла | 16 29 1 22 | ВКУРДХГЁ |  |
| 5. | Виженера | ЛБВ | ЛИКШЙПЛ |  |
| 6. | Хилла | 15 8 31 26 | ОЗЩНИЬЁЖ |  |
| 7. | Аффинный | 17 27 | ЛТМЯВФТДУ |  |
| 8. | Простой замены | ЧТАЮШДНЫСХФЬУЁЭЦВЕКЛИЪЯМЗО | ЮИЧФПАЧ |  |
| ЙГЖЩРБП |  |
|  |  |  |  |
| 9. | Хилла | 30 4 16 10 | БУЙЮЁХИЯ |  |
| 10. | Простой замены | ИЮЧЪЩЁЗМШСХУРЦЭЬЫНФДБТВЛГА | ЩМЁУТНБД |  |
| ПЯЕОЖКЙ |  |
|  |  |  |  |
| 11. | Виженера | ЩКЁ | ЖПРЛКЦВШ |  |
| 12. | Аффинный | 20 13 | ВМЬЫЙЭНХЯ |  |
| 13. | Хилла | 11 7 24 26 | ХУВСПЖЁБ |  |
| 14. | Виженера | ЁЭТ | ТЭАИЛДШЭА |  |

*Бонусное задание №1.* Применив[частотный анализ](https://ru.wikipedia.org/wiki/%D0%A7%D0%B0%D1%81%D1%82%D0%BE%D1%82%D0%BD%D1%8B%D0%B9_%D0%B0%D0%BD%D0%B0%D0%BB%D0%B8%D0%B7),дешифроватьшифротекст, полученное с помощью шифра простой замены:

Алфавит: **"АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ "(С пробелом)**

1. ЮЭ ЪУНЁЧЁЩЭ ПЭЯОНР УНЁЧЁЩЭ ЭПЯОЬЬИУНЁЧЁЩЧНЮЯЧСЭТЬИУНТЪМНЁЧЁЩЭ БЁУЬЧМНЭАЮЯОРЪМЛА МНЬОНЁЧЁЩЭ БЁЧЪЙЬБЛНВОПЯЧЩБНЬОНЁЧЁЩЭРЭЦУНЁЧЁЩЭРЭЦНЮЯЧНЮЭЫЭЖЧНЁЧЁЩЭ РОЪЙЬЭСЭНОЮЮОЯОАОН РОЪЧРОУАНЁЧЁЩЧНРНЁЧЁЩЭ ЭЯАЧЯЭРЭЕЬИШНЭАТУЪНЁЧЁЩЭ ЭЯАЧЯЭРЖЧЩЧН НЧ ЮЭЪЙЦЭРОЬЧУЫНЁЧЁЩЭ ЭЯАЧЯЭРЭЕЬЭШНЫОЁЧЬИНЁЧЁЩЭ ЭЯАЧЯБЛАНЁЧЁЩЧНЮЯЧСЭТЬИУНТЪМНЁЧЁЩЭ БЁУЬЧМНЭАНЬУЮЯЧСЭТЬИГНТЪМНЁЧЁЩЭ БЁУЬЧМНЁЧЁЩЧНЮЯЧСЭТЬИУНТЪМНЁЧЁЩЭ БЁУЬЧМНЮЭ АБЮОЛАНРНЁЧЁЩЭЁЪЧВЭРОЪЙЬИШНЭАТУЪНРНЁЧЁЩЭЁЪЧВЭРОЪЙЬЭЫНЭАТУЪУНЁЧЁЩЭЁЪЧВЭРЖЧЩЧНЬОНЁЧЁЩЭЁЪЧВЭРОЪЙЬИГНОЮЮОЯОАОГНЁЧЁЩЭЁЪЧВБЛАНЁЧЁЩЧНЭАНЬУЁЧЁЩЭ БЁЧАУЪЙЬИГНЁЧЁЩЭЭАЯЭ АЩЭРНЁЧЁЩЧНЮЯЭЁУТЁЧУНЁЧЁЩЭЁЪЧВЭРОЬЧУНЮЭЮОТОЛАНРНЁЧЁЩЭТЯЭПЧАУЪЙЬИШНЭАТУЪНЁЧЁЩЭТЯЭПЧЪЙЖЧЩЧНЬОНЁЧЁЩЭТЯЭПЧЪЩОГНТЯЭПМАНЁЧЁЩЧНТЭНЁЧЁЩЭТЯЭПЧЪЙЬЭСЭН Э АЭМЬЧМНРИПЯО ИРОМНЬУЁЧЁЩЭТЯЭПЬИУНЁЧЁЩЧНЬОНЁЧЁЩЭ РОЪЩБНСТУНЁЧЁЩЭ РОЪЙЖЧЩЧН ХЧСОЛАНЬУЁЧЁЩЭТЯЭПЬИУНЁЧЁЩЧНРНЁЧЁЩЭЮУЕЧНЁЧЁЩЭТЯЭПЬИУНЁЧЁЩЧНРИ БЁЧРОЛА МНРНЁЧЁЩЭ БЁЧЪЩОГ
2. ЙЬДЮЙЁДЩЁЫГЙДМЁЗЁЩЁЫУДМЁЗЁЩЁЫЁЩЁЫУДЙЬДЮЙЁДРПКАЧВЙДЙЩЁЗАЬИЙЩЁДМЁЗЁЩЁЫЁЩЁЫЁЩДМЁЗЁЩЁЫЁЩЁЫЁЩЬЫУДЙЬДЮЙЁДЯВШГЙДАРЙЧЙФДМЁЗЁЩЁЫЁЩЁЫЁЩЬЫЁЩДМЁЗЁЩЁЫЁЩЁЫЁЩЬЫЁЛРЯУДЙЬДЮЙЁДЕЬЕЧЩРЫГЙДМЁЗЁЩЁЫЁЩЁЫЁЩЬЫЁЛРЯЁЩДМЁЗЁЩЁЫЁЩЁЫЁЩЬЫЁЛРЯЁЛЁШУДЙЬДЮЙЁДЖЁЬЫЧЬЙДМЁЗЁЩЁЫЁЩЁЫЁЩЬЫЁЛРЯЁЛЁШЁЩДМЁЗЁЩЁЫЁЩЁЫЁЩЬЫЁЛРЯЁЛЁШЁЛЧЪРДЙЬДЮЙЁДЩЬЫЬЙДШЁЗФШКДИДМЁЗЁЩЁЫЁЩЁЫЁЩЬЫЁЛРЯЁЛЁШЁЛЧЪЧ РДЧЕЙРМЁЗЁЩЁЫЁЩЁЫЁЩЬЫЁЛРЯЁЛЁШЁЛЧЪРДЙЬДЮЙЁДЩУЫЧЬЙДИЬШГДПЧДЧЕЙРМЁЗЁЩЁЫЁЩЁЫЁЩЬЫЁЛРЯЁЛЁШЁЛЧЪЁЩДЮЩЧПРЧЕЙРМЁЗЁЩЁЫЁЩЁЫЁЩЬЫЁЛРЯЁЛЁШЁЛЧЪР
3. ЭЬДМЬВЯЬДОКРЯЗУВЬЦШДЖАРАНЬДЭАЦЖЬЦЮУФДЦЭЬЖЬВЬДОЭДНЛЬСНЧДЦДРЬТРЧЛОГДЛДМОНДДПРОЛЬВУЛЬВДЩХТЬГАЭДЛДПОВУЮАЕЭУЖАЦХЯЪДЗХОВЯДПОЦЮЯПВАЭУАДЛДХОЮОРЯЪДКЧВОДЛЬСЭОДНВЫДЭАМОДАИБДУДПОЮОГЯДЖЮОДОЭЬДКЧВЬДПРУКАСУИАГДРАЦПЯКВУХЬЭЁАЛДЛДПАРЛЧФДРЬТДХРЬЮХОЦЮШДРАЗАЭУФДМЬВЯЬДУДОЮЦЯЮЦЮЛУАДПОЫЦЭАЭУФДЭЬДЯЦЮЭОГДЩХТЬГАЭАДПРУЛАВУДХДЮОГЯДЖЮОДОЭДЭАДКЧВДПРУЭЫЮДДЖАРАТДМОНДЭЬДЯЦЮЭОГДЩХТЬГАЭАДОЭДОХЬТЬВЦЫДЛДЮОФДСАДЦУЮЯЬЁУУДУДЛДОЮЖЬЫЭУУДОЮДЭАПОЭУГЬЭУЫДЩХТЬГАЭЬЮОРЬДЗЛЧРЭЯВДЛДЭАМОДЮРЫПХОФДДТЬЮАГДОЭДОЮПРЬЛУВДХОЗУДЭЬДРАЁАЭТУЪДЦЛОЪДРЬКОЮЯДЛДНЛЯЕДЖЬЦЮЫЕДДУДОЭЬДКЧВЬДОНОКРАЭЬДХОЗУДДЭОДТЬЮАГДЯЮАРЫЭЬДУДЭАДПОПЬВЬДЛДПЬРУСЦХЯЪДЬХЬНАГУЪДЭЬДХОЭХЯРЦДГЬЮАГЬЮУЖАЦХУЕДРЬКОЮДЛДДМОНЯДЦЛЫИАЭЭУХУАТЯУЮДДЛЭОЛШДПРУКЧЛЗУФДЛДРОНЭОФДМОРОНДМЬВЯЬДДУТНЬВДЫХОКЧДЭЬПУЦЬЭЭЧАДОЮЁОГДЩЛЬРУЦЮЬДТВОКЭЧАДПЬГ ВАЮЧДТЬДЭУХОВЫМЬКРУЩВАГДМЬВЯЬДТЬХРАПУВЬЦШДЦВЬЛЬДОЦЮРОЯГЭОМОДПУЦЬЮАВЫДЦЬЮУРУЖАЦХУЕДПЬГ ВАЮОЛДДЭАДЛЧНАРСЬЛДПОТОРЬДУДЭАДЛУНЫДУЭОМОДЛЧЕОНЬДДМЬВЯЬЦЮЬРЗУФДПОХОЭЖУВДСУТЭШДЦЬГОЯКУФЦЮЛОГ
4. ДИГЕЙЫУЗЫДДХЁВТДЕТДШТУЗРЮГДФДЩГЯГЕГУЁЗХГДУЯРПДИЙЁЮХЁЯБ ТДФПЁЗФТЯИЫДИТЗТЦДРИЖЁЯБПЧГ АЦДВЯЫДЖЗРХЁЙЁФЯГЕРЫДЕРЙЗЁХЯРЬГЗРЕТДФДЗГПЧЯБЙТЙГДЙЗТХГВРРДЖЁХРУЯЁДЖЫЙБДКГЯЁФГЮДФДЙЁ ДКРИЯГД ЯТВЛРЦДУЗТЙДЕЁУГЯЫДС РЯБДЧЖЗЫ ЁДРДЕГФЁП ЧЙР ЁДЕГДПТ ГКТЫДУЁЯГГДЕГПЕТКРЙГЯБЕАГДТФТЗРРДЕЁУГЯБДЖЗЁВЁЯОТЯДИЙЗЁРЙБДПТФЁВАДИЁИЗГВЁЙЁКРФЛРИБДЕТДЧЯЧКЛГЕРРДИЙТУРЯБЕЁИЙРДФПЗАФКТЙАЩДФГМГИЙФДЮЁЙЁЗАГДЁЕДЗТПЗТУТЙАФТЯДФДДХЁВЧДЕЁУГЯБДЖЁЯЧКРЯДЖТЙГЕЙДЕТДВРЕТ РЙДДИ ГИБДЕРЙЗЁХЯРЬГЗРЕТДИЁДИЖЁИЁУЕА РДФЖРЙАФТЙБДГХЁДФГМГИЙФТ РДЗГЮЯТ РЗЧЫДИФЁЭДЁЙЮЗАЙРГДЁЕДЖЗЁФЁВРЯДЖЧУЯРКЕАГДВГ ЁЕИЙЗТЬРРДЕЁФЁХЁДФПЗАФКТЙЁХЁДФГМГИЙФТДРДКРЙТЯДЯГЮЬРРДЁДЙЁ ДЮТЮДЁЕЁДЗТУЁЙТГЙДФДЗГПЧЯБЙТЙГДЮДРПЁУЗГЙГЕРЪДЕЁУГЯЫДЕТКТЯРДЖЗЁЫФЯЫЙБДРЕЙГЗГИДФИЭДУЁЯБЛГДРДУЁЯБЛГДЯЪВГЦДВРЕТ РЙДУАЯДПТЖТЙГЕЙЁФТЕДФДИЛТДРДФГЯРЮЁУЗРЙТЕРРДРДЛРЗЁЮЁДРИЖЁЯБПЁФТЯИЫДФДХЁЗЕЁВЁУАФТЪМГЦДЖЗЁ АЛЯГЕЕЁИЙРДРДИЙЗЁРЙГЯБИЙФГДЙЗТЕИЖЁЗЙЕАЩДИГЙГЦДЕТД ГОВЧЕТЗЁВЕЁ ДЧЗЁФЕГДФДДХЁВЧДЕЁУГЯБДРПЁУЗЭЯДХЗГ ЧКРЦДИЙЧВГЕБДУЁЯГГДИЙТУРЯБЕАЦДРД ЁМЕАЦДКГ ДВРЕТ РЙДТДФДДХЁВЧДПТЖТЙГЕЙЁФТЯДУТЯЯРИЙРЙДЖЗГВЛГИЙФГЕЕРЮДЮЁЗВРЙТ

*Бонусное задание №2.* Применив[метод Касиски](https://ru.wikipedia.org/wiki/%D0%9C%D0%B5%D1%82%D0%BE%D0%B4_%D0%9A%D0%B0%D1%81%D0%B8%D1%81%D0%BA%D0%B8),дешифроватьсообщение, полученное с помощью шифра Виженера.

ЙССГЯ ИИХТЯ ЙЧРАШ ЭЗПНХ БТЕЕЬ ЛХЯБЬ ЁЛНОА ЛЛРАЫ ЛРЛТМ ОГФНХ ЗМЛМТ ЁПЯЯЭ ЛРОЕУ НДРОЭ ЛСТРЯ ЁХШОФ ЁПЛЗВ ПДУИЮ КТМГД АИРОГ ООСЙВ ВРЯИЩ ЮЯОПБ ВКЖЕС ЛЖГТЮ ЛСЗУФ ЭЫЛСЬ ВЗСВР ЯЬЛЕЯ БСГЗР БФЦГЯ ЖЗСВХ ИМЗГЯ БТРИЙ ВЦЮЧГ ЛЕЮИШ ЮИЁНД ПАЦНЩ ДИРИЪ ОЁВЗР КСЮХВ МТХЕБ ВНДОУ ЭЦФТТ ЭТРПЯ ЗМРУЬ КТЕЫЪ ЛФОЕР КЖСРЯ БХЕОЩ ТУУЕФ ЗТЕИА ЛХЗЛЩ ИХВНР ОБОЛЩ ЯДРОТ ЛРССГ НТЕЕА ЛЕОИШ ЛХХИЯ ПЫГРЬ ОЦСНР ЯВЙНЯ ЖОГРЯ ИМРЕ

*Особенности бонусных заданий:*

1. Бонусное задание №1 состоит из 4-ех вариантов. Каждый вариант может быть засчитан только одному студенту, первому отправившему преподавателю ответ. Один студент не может сделать более 1 (одного)

варианта задания. При сдаче бонусного задания студент должен продемонстрировать весь процесс применения частотного анализа. При возникновении у преподавателя сомнений в самостоятельности выполнения студентов задания, оно может быть не засчитано. Допускается ручное, программное или программно-ручное решение.

1. Бонусное задание №2 может выполнить неограниченное число студентов. Для этого задания требуется программная реализация метода Касиски, то есть необходимо получить программу, на вход в которую поступает только шифротекст, зашифрованный шифром Виженера, а на выходе программа возвращает открытый текст и ключ. Подробности метода можете также посмотреть [здесь](https://drive.google.com/open?id=1lfPczBKSfewHpVoxJfgc-kvR_Mj2rf4M).