

Университет ИТМО

Факультет ПИИКТ.

Кафедра ВТ.

Лабораторная работа №6 по дисциплине

Прикладная математика

Выполнили :

Шишкин Никита Дмитриевич

Давыдов Иван Денисович

Вариант 20

Группа Р3300

Преподаватель :

Тропченко Андрей Александрович

Санкт-Петербург

2019 год.

Часть 1.

Цель работы:

Ознакомится с моноалфавитными подстановками и используя частотный анализ дешифровать криптограмму, зашифрованную методом моноалфавитных подстановок.

Расшифрованный исходный текст:

ЫЪЗВЮРСЦПЫБВЮЦЙЦАЙХРВЮЪЮИПЙЬЮБЙГПВАМЮЪВБЙФАСРЙЬЮПЫЪБЙЬЮ
ИЗБА ЛЕСНИКА СОСТОЯЛА ИЗ ОДНОЙ КОМНАТЫ ЗАКОПТЕЛОЙ НИЗКОЙ И
ЮФЕЦАЙЬЮЗСЪЮФЙРВАСЬЮЮФСШС ЙШЙИЙБЮПВЮРВЛЕСЮРСТВРЙЮИПЙЦАЛЙ
ПУСТОЙ БЕЗ ПОЛАТЕЙ И ПЕРЕГОРОДОК НА ЛАВКЕ ЛЕЖАЛО ОДНОСТВО
РКПЙСЮШЕТКСЮЛЮЕ РЕЮЛВРХРВЦКЮ ШЕИВЮАШХФЙБЮИЛВЮЗЙРКЧЫЖЮ ЙШЧБ
ЛЬНОЕ РУЖЬЕ В УГЛУ ВАЛЯЛАСЬ ГРУДА ТРЯПОК ДВА БОЛЬШИХ ГОРШК
ВЮЦАЙХРЮЛЙЪРСЮФСУБЫЮРЕУЫПВЮ ЙШСРВЮПВЮЦАЙРСЮФСУВРКПЙЮЛЦФМЖ
А СТОЯЛИ ВОЗЛЕ ПЕЧКИ ЛУЧИНА ГОРЕЛА НА СТОЛЕ ПЕЧАЛЬНО ВСПЫХ
ЫЛВХЮЮФЙ ВЦВХЮПВЮЦВГЙЬЮЦСШСИПСКЮЪЗМЮЛЫЦСРВЮРОРКБВЮФШЫЛХЪ
ИВАЯ И ПОГАСАЯ НА САМОЙ СЕРЕДИНЕ ИЗБЫ ВИСЕЛА ЛЮЛЬКА ПРИВЯЗ

Ключ:

| | | | | | | | | | | | | | | | | | | |
|-------------------------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Нормативный алфавит (М) | А | Б | В | Г | Д | Е | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С |
| Алфавит шифрования (Е) | В | З | Л | _ | И | С | Т | Ъ | Ы | Ь | Б | Р | Г | П | Й | И | Ш | Ц |

| | | | | | | | | | | | | | | |
|-------------------------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Нормативный алфавит (М) | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ы | Ь | Э | Ю | Я | _ |
| Алфавит шифрования (Е) | А | Е | - | Ж | - | У | Ч | - | М | К | - | О | Х | Ю |

Краткий протокол криптоанализа:

Изначально имеем результаты статистического анализа данной криптограммы:

| СТАТИСТИКА | | СИМВОЛ — ЗАМЕНИТЬ НА | |
|------------|----------|--|--|
| Крип-ма | Рус. яз. | КРИПТОГРАММА | |
| Ю 0.149 | О 0.175 | ЫЪЗВЮРСЦПЫБВЮЦЙЦАЙХРВЮЪЮИПЙЬЮБЙГПВАМЮЪВБЙФАСРЙЬЮПЫЪБЙЬЮ | |
| В 0.101 | О 0.089 | | |
| Й 0.089 | Е 0.072 | ЮФЕЦАЙЬЮЗСЪЮФЙРВАСЬЮЮФСШС ЙШЙИЙБЮПВЮРВЛЕСЮРСТВРЙЮИПЙЦАЛЙ | |
| Р 0.068 | А 0.062 | | |
| С 0.061 | И 0.062 | РКПЙСЮШЕТКСЮЛЮЕ РЕЮЛВРХРВЦКЮ ШЕИВЮАШХФЙБЮИЛВЮЗЙРКЧЫЖЮ ЙШЧБ | |
| П 0.053 | Н 0.053 | | |
| Ы 0.051 | Т 0.053 | ВЮЦАЙХРЮЛЙЪРСЮФСУБЫЮРЕУЫПВЮ ЙШСРВЮПВЮЦАЙРСЮФСУВРКПЙЮЛЦФМЖ | |
| Б 0.046 | С 0.045 | | |
| Ц 0.043 | Р 0.040 | ЫЛВХЮЮФЙ ВЦВХЮПВЮЦВГЙЬЮЦСШСИПСКЮЪЗМЮЛЫЦСРВЮРОРКБВЮФШЫЛХЪ | |
| Ф 0.030 | В 0.038 | | |
| Ш 0.030 | Л 0.035 | | |
| А 0.028 | К 0.028 | | |
| Л 0.028 | М 0.026 | | |
| Е 0.025 | Д 0.025 | | |
| К 0.023 | П 0.023 | | |
| И 0.020 | У 0.021 | | |
| 0.020 | Я 0.018 | | |
| Ъ 0.020 | Ы 0.016 | | |

На основании статистики, произведем замену «Ю» - «_»

| СТАТИСТИКА | | СИМВОЛ <u>Ю</u> ЗАМЕНИТЬ НА | |
|------------|----------|--|--|
| Крип-ма | Рус. яз. | КРИПТОГРАММА | |
| Ю 0.149 | О 0.175 | ЫЪЗВЮРСЦПЫБВЮЦЙЦАЙХРВЮЪЮЙИПЬЮБЙГПВАМЮЪВЕЙФАСРЬЮПЫЪБЙЮЫ | |
| В 0.101 | О 0.089 | ----- | |
| Й 0.089 | Е 0.072 | ЮФЕЦАЙЪЮЗСЪЮФЙРВАСЪЮЮФСШС ЙШЙИБЮПВЮРВЛБСКРСТВРЙЮИПЦАЛЙ | |
| Р 0.068 | А 0.062 | ----- | |
| С 0.061 | И 0.062 | РКПЙСЮШЕТКСЮЛЮЕ РЕЮЛВРХРВЦКЮ ШЕИВЮАШХФЙБЮИЛВЮЗЙРКЧЫЖЮ ЙШЧБ | |
| П 0.053 | Н 0.053 | ----- | |
| Ы 0.051 | Т 0.053 | ВЮЦАЙХРЮЛЙЪРСКЮФСУБЮРЕУЫПВЮ ЙШСРВЮПВЮЦАЙРСКЮФСУВРКПЙЮЛЦФМЖ | |
| Б 0.046 | С 0.045 | ----- | |
| Ц 0.043 | Р 0.040 | ЫЛВХЮЮФЙ ВЦВХЮПВЮЦВГЙЮЮЦСШСИПСЮЪЗМЮЛЫЦСРВЮРОРКБВЮФШЫЛХЪ | |
| Ф 0.030 | В 0.038 | ----- | |
| Ш 0.030 | Л 0.035 | | |
| А 0.028 | К 0.028 | | |
| Л 0.028 | М 0.026 | | |
| Е 0.025 | Д 0.025 | | |
| К 0.023 | П 0.023 | | |
| И 0.020 | У 0.021 | | |
| 0.020 | Я 0.018 | | |
| Ъ 0.020 | Ы 0.016 | | |

Обратим внимание на символ «Ы». Он много раз встречается поодиночке, следовательно вполне вероятно, что это некий однобуквенный предлог, союз или местоимение, т.е. «В», «К», «О», «У», «С», «А», «И», «Я». Кроме того, заметим некое слово из двух букв «ЫЪ» и нескольких слов начинающихся с «Ы». Попробуем осуществить замену «Ы» - «И», а также «Ъ» - «З» (нет подходящих четырехбуквенных слов, начинающихся с «ИМ», «ИХ» и т.д.

Реакция программы:

| СТАТИСТИКА | | СИМВОЛ <u>Ъ</u> ЗАМЕНИТЬ НА З | |
|------------|----------|--|--|
| Крип-ма | Рус. яз. | КРИПТОГРАММА | |
| Ю 0.149 | О 0.175 | ЫЪЗВЮРСЦПЫБВЮЦЙЦАЙХРВЮЪЮЙИПЬЮБЙГПВАМЮЪВЕЙФАСРЬЮПЫЪБЙЮЫ | |
| В 0.101 | О 0.089 | ИЗ-- --И-- --ИЗ-- --З-- --ИЗ-- --И | |
| Й 0.089 | Е 0.072 | ЮФЕЦАЙЪЮЗСЪЮФЙРВАСЪЮЮФСШС ЙШЙИБЮПВЮРВЛБСКРСТВРЙЮИПЦАЛЙ | |
| Р 0.068 | А 0.062 | ----- | |
| С 0.061 | И 0.062 | -----З-----И----- | |
| П 0.053 | Н 0.053 | РКПЙСЮШЕТКСЮЛЮЕ РЕЮЛВРХРВЦКЮ ШЕИВЮАШХФЙБЮИЛВЮЗЙРКЧЫЖЮ ЙШЧБ | |
| Ы 0.051 | Т 0.053 | ----- | |
| Б 0.046 | С 0.045 | ВЮЦАЙХРЮЛЙЪРСКЮФСУБЮРЕУЫПВЮ ЙШСРВЮПВЮЦАЙРСКЮФСУВРКПЙЮЛЦФМЖ | |
| Ц 0.043 | Р 0.040 | -----И--З-- --И-- --И-- | |
| Ф 0.030 | В 0.038 | ЫЛВХЮЮФЙ ВЦВХЮПВЮЦВГЙЮЮЦСШСИПСЮЪЗМЮЛЫЦСРВЮРОРКБВЮФШЫЛХЪ | |
| Ш 0.030 | Л 0.035 | И-- И-----И-- ИЗ-- --И----- --И--З | |
| А 0.028 | К 0.028 | | |
| Л 0.028 | М 0.026 | | |
| Е 0.025 | Д 0.025 | | |
| К 0.023 | П 0.023 | | |
| И 0.020 | У 0.021 | | |
| 0.020 | Я 0.018 | | |
| Ъ 0.020 | Ы 0.016 | | |

Первое слово повторяется также в конце текста, но уже с другим окончанием. Слов из 4-х букв на «ИЗ» практически нет, скорее всего это слов «ИЗБА» или одна из его форм, сделаем замену «З» - «Б». Также заметим во втором ряду слово «Б-З», отсюда делаем очевидную замену «С» - «Е».

Теперь получаем это:

Длинное слово в середине второй строки должно быть словом «ПЕРЕГОРОДОК», а шестое слово в первой по смыслу (речь об избе) словом «КОМНАТЫ». Результат замен:

| СТАТИСТИКА | | СИМВОЛ <u>М</u> ЗАМЕНИТЬ НА <u>Ы</u> |
|------------|----------|--|
| Крип-ма | Рус. яз. | КРИПТОГРАММА |
| Ю 0.149 | О 0.175 | |
| В 0.101 | О 0.089 | ЫЪЗВЮРСЦПЫВВЮЦЦАЙХРВЮЪЮИПИЬЮБЙГПВАМЪВВЙФАСРЬЮПЪБЬЮЪ |
| И 0.089 | Е 0.072 | ИЗБА -Е-НИКА -О-ТО--А ИЗ ОДНОЙ КОМНАТЫ ЗАКОПТЕ-ОЙ НИЗКОЙ И |
| Р 0.068 | А 0.062 | ЮФЕЦАЙЪЮЗСЪЮЙРВАСЪЮЮФСШ ЙШЙИЬЮПВЮРВЛБСЮРСТВРЙЮИПИЦАЛЙ |
| С 0.061 | И 0.062 | П--ТОЙ БЕЗ ПО-АТЕЙ И ПЕРЕГОРОДОК НА -А-КЕ -Е-А-О ОДНО-Т-О |
| П 0.053 | Н 0.053 | РКПЙСЮШЕТКСЮЛЮ РЕЮЛВРХРВЦЮ ШЕИВЮАШХФЙБЮИЛВЮЗЙРКЧЫЖУ ЙШЧБ |
| Ы 0.051 | Т 0.053 | --НОЕ Р---Е - -Г-- -А---А-- ГР-ДА ТР-ПОК Д-А БО--И- ГОР-К |
| Б 0.046 | С 0.045 | ВЮЦАЙХРЮЛЙЪРСЮФСУБЮРЕУНПВЮ ЙШСРВЮПВЮЦАЙРСЮФСУВРКПЙЮЛЦФМЖ |
| Ц 0.043 | Р 0.040 | А -ТО--И -ОЗ-Е ПЕ-КИ ---ИНА ГОРЕ-А НА -ТО-Е ПЕ-А--НО --ПЫ- |
| Ф 0.030 | В 0.038 | ЫЛВХЮЮФЙ ВЦВХЮПВЮЦВГЙЮЦСШНПСЮЪЭМОЛЫЦСРВЮРОРКВБЮФШЛХЪ |
| Ш 0.030 | Л 0.035 | И-А- И ПОГА-А- НА -АМОЙ -ЕРЕДИНЕ ИЗБЫ -И-Е-А ----КА ПРИ--З |
| А 0.028 | К 0.028 | |
| Л 0.028 | М 0.026 | |
| Е 0.025 | Д 0.025 | |
| К 0.023 | П 0.023 | |
| И 0.020 | У 0.021 | |
| О 0.020 | Я 0.018 | |
| Ъ 0.020 | Ы 0.016 | |

Все последующие замены тривиальны и не представляют никаких сложностей.

Часть 2.

Цель работы:

Ознакомится с многопетлевыми полиалфавитными подстановками и дешифровать криптограмму, зашифрованную методом многопетлевым шрифтом. Определить период шифра предлагаемой криптограммы. Получить составной ключ, вычислить первичные ключи.

Расшифрованный исходный текст:

ФУРЬСМХХВДЮЦКЛЙЗАГР ЖДЭААКЭПХУЪЕЭЛУНТШВЖЦТБЬЙЭВЖЩК
ИДЕТ ПАРОВОЗ СПРАШИВАЕТСЯ ОТЧЕГО ОН ДВИЖЕТСЯ МУЖИК Г
ЧЮЬПЙДЛЗУАШЭПВЧЪЪТФХРЬСВШУУЖ ЙЪЗЕЩКЧЮЬПЙДЛЧУАШХКБУЭЕ
ОВОРИТ ЭТО ЧЕРТ ДВИЖЕТ ЕГО ДРУГОЙ ГОВОРИТ ЧТО ПАРОВО
ЧЛЧППГЭВЧЕРУДЦРОЗЖЛЫДНТРВЙШЛШЫРДДЕЫС ЛЙГНЪЧЬЛПЙИЬВЙ
З ИДЕТ ОТТОГО ЧТО В НЕМ ДВИЖУТСЯ КОЛЕСА ТРЕТИЙ УТВЕР
ННЪУСАЙЮОАБИОАЪТЫЧФОЧСПЯЕУДЫВЪБФРЭЯЩЪНБАЧЖМЖТЖЩЧ ЦВ
ЖДАЕТ ЧТО ПРИЧИНА ДВИЖЕНИЯ ЗАКЛЮЧАЕТСЯ В ДЫМЕ ОТНОСИ
ГЮШОНПГНВСУОВЭЯГЪЖМЧКЮНГШЬЖЙЯШКХРДМЕУЪОВЪ ЯПДЩЕЮЦДИМ
МОМ ВЕТРОМ МУЖИК НЕОПРОВЕРЖИМ ДЛЯ ТОГО ЧТОБЫ ЕГО ОПР
ЗЙОЛСМФДЗ ОУЭФЙИЧИЩКЛЩЭШСКЭЖЖЛЦЫЗЖЪОЙЖНДНЕЛЧУАШУПГД
ОВЕРГНУТЬ НАДО ЧТОБЫ КТО НИБУДЬ ДОКАЗАЛ ЕМУ ЧТО НЕТ

Составной ключ:

«МПЛКТЮХЕФВРЧЧЪЭЪЗЙЬО_БУМАБУЩЖКТЕЫШР»

Краткий протокол криптоанализа:

Определим период шифра, сначала воспользуемся методом Казиски:

| Номер | Период | Вес |
|-------|--------|-----|
| 1 | 35 | 22 |
| 2 | 1 | 15 |
| 3 | 2 | 6 |
| 4 | 3 | 2 |
| 5 | 4 | 1 |

Наибольший вес имеет период 35. Проверим ИС:

Индекс соответствия данной криптограммы: 0.0250

Значение ИС, также указывает на длину ключа >10, окончательно берем 35.

В каждой группе периода заменим самый часто встречающийся символ на «_».

Результат:

| СТАТИСТИКА (1) | | (F8) Ключ: МПЛКТГГЕФВРЧЧЪЭЪЗШЬО> | СИМВОЛ <u>Ю</u> ЗАМЕНИТЬ НА |
|----------------|----------|--|-----------------------------|
| Крипт-ма | Рус. яз. | КРИПТОГРАММА | |
| Л 0.179 | О 0.175 | ФУРЬСМХХВДЮЮЦКЛЙЗАГР ЖДЭЯААКЭПХУЪЕЭЛУНТШВЖЦТВЬЙЭВЖЩК | |
| С 0.103 | Е 0.072 | ИДЕТ ЙТРОВОЗ СПРАЙИВТЭТСЯНОТЧЕГО Я ДВИЖ ГСЯ МУЖИК Г | |
| Ъ 0.060 | А 0.062 | ЧЮЪПЙДЛЭУАШЭПВЧЪЪТФХРЬСВШУУЖ ЙЪЗЕЩКЧЮЪПЙДЛЧУАШХКБУЭ | |
| Ю 0.060 | И 0.062 | ВОБ Т Э О ЧЕРТ ЦФИЖЕТ ХО ДРУГОЙ Г ВОБ Т Ч О ПАРОВ | |
| Щ 0.060 | Н 0.053 | ЧЛЧППГЭВЧЕРУДЦРОЗЖЛЫДНТРВЙЩЛШЫРДДЕНС ЛЙГНЪЧЪЛПЙИЬБЙ | |
| Ш 0.051 | Т 0.053 | Щ ИДЕТЬ ТТОГО ЧТО Ф НЧГ ДВЦЖУТСЯ К ЭЕСА ТКЧТИЙ УТВЕР | |
| О 0.043 | С 0.045 | ННЬУСАЙЮОАБИОАЪТЫЧФОЧСПЯЕУДЫВЪБФРЭЯЩЪНБАЧЖМЖТЖШЧ ЦВ | |
| М 0.043 | Р 0.040 | ЖЦАЕГЧЧТОНПРИЧИНАСЦВИЖЕНВР ЗАКЛЮЧАЕТВЯ ФЧДЫМУ ОТНОСИ | |
| Э 0.043 | В 0.038 | ГЮШОНПГНВСУОВЭЯГЪЖМЧКЮНГШЬЖЙЯШКХРДМЕУЪОБЬ ЯПДЩЕЮЦДИМ | |
| Я 0.034 | Л 0.035 | Ю М ВЕТК М МУЖИК НЕ ПР ЪЕРЖЦМ ДЛЯ Т ХО ЧТОЪМ ЕГО ОПР | |
| Ч 0.026 | К 0.028 | ЗЙОЛСМФДЗ ОУЭФЙИЧИШКЛЩЭШСКЭЖЖЛЦЫЗЖЪОЙЖНДНЕЛЧУАШУПГД | |
| К 0.026 | М 0.026 | ОВЧРГЯКТЬ НАДО ЧТОУМ КТО ЗЪБУДЬ ДОКАЗТЛ ЧГУ Ч О НЕТ | |
| Ц 0.026 | Д 0.025 | | |
| Ь 0.026 | П 0.023 | | |
| Р 0.017 | У 0.021 | | |
| Т 0.017 | Я 0.018 | | |
| В 0.017 | Ы 0.016 | | |
| Х 0.017 | З 0.016 | | |
| Ы 0.017 | Ь 0.014 | | |
| Й 0.009 | Ъ 0.014 | | |
| Ж 0.009 | Б 0.014 | | |
| А 0.009 | Г 0.013 | | |

Исправим замены в словах, чтобы получить корректный составной ключ.

Итоговый результат:

| СТАТИСТИКА (1) | | (F8) Ключ: МПЛКТЮХЕФВРЧЧЪЭЪЗЙЬО> | СИМВОЛ Н ЗАМЕНИТЬ НА М |
|----------------|----------|--|------------------------|
| Крип-ма | Рус. яз. | КРИПТОГРАММА | |
| Л 0.179 | О 0.175 | ФУРЬСМХХБДЮЦКЛЙЗАГР ЖДЭАААКЭПХУЪЕЭЛУНТШВЖЦТБЪЙЭБЖЩК | |
| С 0.103 | О 0.089 | ИДЕТ ПАРОВОЗ СПРАШИВАЕТСЯ ОТЧЕГО ОН ДВИЖЕТСЯ МУЖИК Г | |
| Ф 0.094 | Е 0.072 | ЧЮБПЙДЛЭУАШЭПБЧЪТФХРЬСВШУУЖ ЙЪЭЕЩКЧЮБПЙДЛЧУАШХКБУЭЕ | |
| Ъ 0.060 | А 0.062 | ОВОРИТ ЭТО ЧЕРТ ДВИЖЕТ ЕГО ДРУГОЙ ГОВОРИТ ЧТО ПАРОВО | |
| Ю 0.060 | И 0.062 | ЧЛЧППГЭВЧЕРУДЦРОЗЖЛЫДНТРВЙЩЛШЫРДДЕЫС ЛЙГНЪЧЪЛПЙИЪБЙ | |
| Щ 0.060 | Н 0.053 | З ИДЕТ ОТТОГО ЧТО В НЕМ ДВИЖУТСЯ КОЛЕСА ТРЕТИЙ УТВЕР | |
| Ш 0.051 | Т 0.053 | ННЬУСАЙЮОАБИОАЪТЫЧФОЧСПЯЕУДЫВЪВФРЭАЩЪНБАЧЖМЖТЖШЧ ЦВ | |
| О 0.043 | С 0.045 | ЖДАЕТ ЧТО ПРИЧИНА ДВИЖЕНИЯ ЗАКЛЮЧАЕТСЯ В ДЫМЕ ОТНОСИ | |
| М 0.043 | Р 0.040 | ГЮШОНПГНВСУОВЭЯГЪЖМЧКЮНГШЪЖЙЯШКХРДМЕУЪОБЪ ЯПДШЕЮЦДИМ | |
| Э 0.043 | В 0.038 | МОМ ВЕТРОМ МУЖИК НЕОПРОВЕРЖИМ ДЛЯ ТОГО ЧТОБЫ ЕГО ОПР | |
| Я 0.034 | Л 0.035 | ЗЙОЛСМФДЗ ОУЭФЙИЧИЩКЛЩЭШСКЭЖЖЛЦЫЗЖЪОЙЖНДНЕЛЧУАШУПГД | |
| Ч 0.026 | К 0.028 | ОВЕРГНУТЬ НАДО ЧТОБЫ КТО НИБУДЬ ДОКАЗАЛ ЕМУ ЧТО НЕТ | |
| К 0.026 | М 0.026 | | |
| Ц 0.026 | Д 0.025 | | |
| Б 0.026 | П 0.023 | | |
| Р 0.017 | У 0.021 | | |
| Т 0.017 | Я 0.018 | | |
| В 0.017 | Ы 0.016 | | |
| Х 0.017 | З 0.016 | | |
| Ы 0.017 | Ь 0.014 | | |
| Й 0.009 | Ъ 0.014 | | |
| Ж 0.009 | Б 0.014 | | |
| А 0.009 | Г 0.013 | | |

Получен составной ключ: «МПЛКТЮХЕФВРЧЧЪЭЪЗЙЬО_БУМАБУЩЖКТЕЫШР»

Предположим, что он получен из двух первичных ключей, тогда их длины могут быть равны 7 и 5.

Составной ключ - $K_1 K_2 \dots K_{30}$

Первый первичный ключ - $K_{1,1} K_{1,2} \dots K_{1,7}$

Второй первичный ключ - $K_{2,1} K_{2,2} \dots K_{2,5}$

Система уравнений:

$$K_{1,1} + K_{2,1} = 12("М")$$

$$K_{1,3} + K_{2,5} = 2("В")$$

$$K_{1,2} + K_{2,2} = 15("П")$$

$$K_{1,4} + K_{2,1} = 16("Р")$$

$$K_{1,3} + K_{2,3} = 11("Л")$$

$$K_{1,5} + K_{2,2} = 23("Ч")$$

$$K_{1,4} + K_{2,4} = 10("К")$$

$$K_{1,6} + K_{2,3} = 23("Ч")$$

$$K_{1,5} + K_{2,5} = 18("Т")$$

$$K_{1,7} + K_{2,4} = 26("Ъ")$$

$$K_{1,6} + K_{2,1} = 30("Ю")$$

$$K_{1,1} + K_{2,5} = 29("Э")$$

$$K_{1,7} + K_{2,2} = 21("Х")$$

$$K_{1,2} + K_{2,1} = 26("Ъ")$$

$$K_{1,1} + K_{2,3} = 5("Е")$$

$$K_{1,3} + K_{2,2} = 7("З")$$

$$K_{1,2} + K_{2,4} = 20("Ф")$$

$$K_{1,4} + K_{2,3} = 9(\text{"Й"})$$

$$K_{1,5} + K_{2,4} = 28(\text{"Ъ"})$$

$$K_{1,6} + K_{2,5} = 14(\text{"О"})$$

$$K_{1,7} + K_{2,1} = 32(\text{"_"})$$

$$K_{1,1} + K_{2,2} = 1(\text{"Б"})$$

$$K_{1,2} + K_{2,3} = 19(\text{"У"})$$

$$K_{1,3} + K_{2,4} = 12(\text{"М"})$$

$$K_{1,4} + K_{2,5} = 0(\text{"А"})$$

$$K_{1,5} + K_{2,1} = 1(\text{"Б"})$$

$$K_{1,6} + K_{2,2} = 19(\text{"У"})$$

$$K_{1,7} + K_{2,3} = 25(\text{"Щ"})$$

$$K_{1,1} + K_{2,4} = 6(\text{"Ж"})$$

$$K_{1,2} + K_{2,5} = 10(\text{"К"})$$

$$K_{1,3} + K_{2,1} = 18(\text{"Т"})$$

$$K_{1,4} + K_{2,2} = 5(\text{"Е"})$$

$$K_{1,5} + K_{2,3} = 27(\text{"Ы"})$$

$$K_{1,6} + K_{2,4} = 24(\text{"Ш"})$$

$$K_{1,7} + K_{2,5} = 16(\text{"Р"})$$

Решив систему относительно $K_{1,1}$, мы можем подобрать 2 первичных ключа:

Первый - «ЭКВАТОР».

Второй - «РЕЙКА».