Министерство образования Российской Федерации

МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ им. Н.Э. БАУМАНА

Факультет: Информатика и системы управления
Кафедра: Информационная безопасность (ИУ8)

Криптографические методы защиты информации

Домашняя работа №1

Преподаватель: Поляков М.В.
Студент: Макрецкий П.А.
Группа: ИУ8-85

Москва, 2024

СОДЕРЖАНИЕ

ЗАДАНИЕ

1. Дешифровать текст, зашифрованный аффинным шифром:

   BXWMFFGZWEGRXWJGSMBURWIFQIZIMHRXMVWBGESKVSBGB
   KBGIZEGRXWJCXWJWWMEXHWBBWJGZMZMHRXMVWBGSQMR
   RWNBIGBSZKQWJGEWAKGTMHWZBWZEJURBWNKSGZOMSGQR
   HWQMBXWQMBGEMHFKZEBGIZMZNEIZTWJBWNVMEYBIMHWB
   BWJBXWFIJQKHMKSWNQWMZSBXMBWMEXHWBBWJWZEJURBS
   BIIZWIBXWJHWBBWJMZNVMEYMOMGZQWMZGZOBXWEGRXWJ
   GSWSSWZBGMHHUMSBMZNMJNSKVSBGBKBGIZEGRXWJCGBXM
   JKHWOITWJZGZOCXGEXHWBBWJOIWSBICXGEXMSSKEXGBXMS
   BXWCWMYZWSSWSIFMHHSKVSBGBKBGIZEGRXWJSWMEXHWB
   BWJGSWZEGRXWJWNCGBXBXWFKZEBGIZBXWEGRXWJSRJGQM
   JUCWMYZWSSEIQWSFJIQBXWFMEBBXMBGFBXWEJURBMZMHU
   SBEMZNGSEITWJVUQWMZSIFFJWAKWZEUMZMHUSGSVJKBWFIJ
   EWOKWSSGZOIJIBXWJCGSWBXWRHMGZBWLBIFBCIEGRXWJBW
   LBEXMJMEBWJSBXWZBXWYWUEMZVWIVBMGZWNVUSIHTGZO
   MSGQKHBMZWIKSWAKMBGIZSGZEWCWYZICMMZNQMJWJWHM
   BGTWHURJGQWBXGSEMZVWKSWNBIJMRGNHUNGSEMJNQMZUF
   MHSWYWUSGZMZMKBIQMBWNSUSBWQBXWSMQWBURWIFBJM
   ZSFIJQMBGIZKSWNGZMFFGZWEGRXWJSGSKSWNGZHGZWMJEIZ
   OJKWZBGMHOWZWJMBIJSMBURWIFRSWKNIJMZNIQZKQVWJOW
   ZWJMBIJBXGSOWZWJMBIJGSZIBMEJURBIOJMRXGEMHHUSWEKJ
   WRSWKNIJMZNIQZKQVWJOWZWJMBIJFIJBXWSMQWJWMSIZBX
   MBBXWMFFGZWEGRXWJGSZIBSWEKJW

2. Дешифровать текст, зашифрованный шифром Вижинера. Найти длину ключевого слова и само слово

   VYCPYTKECRBDJVPXLOVPNTHTOFLDTZRYYQXHKTQJUGVZRJM
   WQEAXIVGIUWXFGVYRAZGKRTKWPRLPEDJRZTMWUDYEISFKM

XMGPLKTKWEVOJBJCCCCMSPTPNIHGUSHBBIRQXFDNVKPMVG
DYIBQCCDJGQVZMCTBFTMCOSTKCSUOEBRDTZGKRTKHJVDDK
AWCYJLSFDCPGGVYYIXOEYJTMHGICCVFAGRHMCQECDMVGIJT
MHGIYCWPCTIPZOKEKTTBKEEIASEZNWXFKJCHLSPKGPEZARQI
TBFRPSLIDJRXMIVZMCVWRYCGPWVYYGNZGXMKXFPZLVPVKT
FAXHVVPVHSUKMLAWEYYHLIEYGIAOUKFTPSCBLTLGGJMUTZN
JSQLHKKSIBCPTGEASTJCPVVNVRIXFKJCCVWRYCGXRYZRWMV
GWSCVHKFLIASEZNWXFUGPXFOTPUTTYPVQHVCOVQUKCOKFT
YOEKRWTHKWRWXQTPNITBCCWHMQCEBXLQQMCGUMOVYCL
CHWPTJIGEANTBCCWHBGDISIXTQIATZIGJQXGUQIMIASTNGHXH
JVNATWPKCMMCHKUDVWRYCGMSZKAWTFCTRTKGVYCCMVG
BCNVOPSCDUHCZLTWPAJMAOWPXYHBAWCRPGSQLQTJICKGDG
GKEATPSMEMLTOPUKPKSTVJPMWXVJNIFKDCIAWUTYCUSWJCS
MCTRNXWZAUGHVOTUKPGMHRJHXYGPQXGOPRSIHACKCSLMU
KCBMVGJYBXHAGCDYHTRLHYCTDYIBCPLQTWWPRDUBBGTGE
ASTJGHNGGUGCEWPVYGVCPXPJXBVZYAZSPVPPMCTJYIRDGFD
ELSWUMGTBFFKCNADVPVXBGIYIHFVYGHZSPVPPMCTZQCHHCT
PNIHQXPPIVKTYAEMUVAJKSRJCJWCTRLSHAPLKQXFIVLTKOVFP
UHFVYCHTAGICPLCPKFPMHJVYUYWPVAXIVGIGHGCVJCRNF

3. Дан отрывок из литературного произведения. Часть этого текста (непрерывным блоком) была зашифрована шифром Хилла с матрицей размерности 3. Найти матрицу.

   Call me Ishmael. Some years ago—never mind how long precisely—having little or no money in my purse, and nothing particular to interest me on shore, I thought I would sail about a little and see the watery part of the world. It is a way I have of driving off the spleen and regulating the circulation. Whenever I find myself growing grim about the mouth; whenever it is a damp, drizzly November in my soul; whenever I find myself involuntarily pausing before coffin warehouses, and bringing up the rear of every funeral I meet; and

especially whenever my hypos get such an upper hand of me, that it requires a strong moral principle to prevent me from deliberately stepping into the street, and methodically knocking people's hats off—then, I account it high time to get to sea as soon as I can. This is my substitute for pistol and ball. With a philosophical flourish Cato throws himself upon his sword; I quietly take to the ship. There is nothing surprising in this. If they but knew it, almost all men in their degree, some time or other, cherish very nearly the same feelings towards the ocean with me. There now is your insular city of the Manhattoes, belted round by wharves as Indian isles by coral reefs—commerce surrounds it with her surf. Right and left, the streets take you waterward. Its extreme downtown is the battery, where that noble mole is washed by waves, and cooled by breezes, which a few hours previous were out of sight of land. Look at the crowds of water-gazers there. Circumambulate the city of a dreamy Sabbath afternoon. Go from Corlears Hook to Coenties Slip, and from thence, by Whitehall, northward. What do you see?—Posted like silent sentinels all around the town, stand thousands upon thousands of mortal men fixed in ocean reveries. Some leaning against the spiles; some seated upon the pier-heads; some looking over the bulwarks of ships from China; some high aloft in the rigging, as if striving to get a still better seaward peep. But these are all landsmen; of week days pent up in lath and plaster—tied to counters, nailed to benches, clinched to desks. How then is this? Are the green fields gone? What do they here? But look! here come more crowds, pacing straight for the water, and seemingly bound for a dive. Strange! Nothing will content them but the extremest limit of the land; loitering under the shady lee of yonder warehouses will not suffice. No. They must get just as nigh the water as they possibly can without falling in. And there they stand—miles of them—leagues. Inlanders all, they come from lanes and alleys, streets and avenues—north, east, south, and west. Yet here they all unite. Tell me, does the magnetic virtue of the needles of the compasses of all those ships attract them thither? Once more.

Say you are in the country; in some high land of lakes. Take almost any path you please, and ten to one it carries you down in a dale, and leaves you there by a pool in the stream. There is magic in it. Let the most absent-minded of men be plunged in his deepest reveries—stand that man on his legs, set his feet a-going, and he will infallibly lead you to water, if water there be in all that region. Should you ever be athirst in the great American desert, try this experiment, if your caravan happen to be supplied with a metaphysical professor. Yes, as every one knows, meditation and water are wedded for ever.But here is an artist. He desires to paint you the dreamiest, shadiest, quietest, most enchanting bit of romantic landscape in all the valley of the Saco. What is the chief element he employs? There stand his trees, each with a hollow trunk, as if a hermit and a crucifix were within; and here sleeps his meadow, and there sleep his cattle; and up from yonder cottage goes a sleepy smoke. Deep into distant woodlands winds a mazy way, reaching to overlapping spurs of mountains bathed in their hill-side blue. But though the picture lies thus tranced, and though this pine-tree shakes down its sighs like leaves upon this shepherd’s head, yet all were vain, unless the shepherd’s eye were fixed upon the magic stream before him. Go visit the Prairies in June, when for scores on scores of miles you wade knee-deep among Tiger-lilies—what is the one charm wanting?—Water—there is not a drop of water there! Were Niagara but a cataract of sand, would you travel your thousand miles to see it? Why did the poor poet of Tennessee, upon suddenly receiving two handfuls of silver, deliberate whether to buy him a coat, which he sadly needed, or invest his money in a pedestrian trip to Rockaway Beach? Why is almost every robust healthy boy with a robust healthy soul in him, at some time or other crazy to go to sea? Why upon your first voyage as a passenger, did you yourself feel such a mystical vibration, when first told that you and your ship were now out of sight of land? Why did the old Persians hold the sea holy? Why did the Greeks give it a separate deity, and own brother of Jove? Surely

all this is not without meaning. And still deeper the meaning of that story of Narcissus, who because he could not grasp the tormenting, mild image he saw in the fountain, plunged into it and was drowned. But that same image, we ourselves see in all rivers and oceans. It is the image of the ungraspable phantom of life; and this is the key to it all.

Шифртекст:

YDFRBCNXICSDDORSHMCZROVCLZYSRAMYMFVCOGTQXPCGUJ
CHESEVYRWXCQWLKULRNWPQHYDFWQKJKNOJGYOZXJAVPCJ
KNGPMTOJZGYUUGMBCSQZONFTROMAFEPRJKNKHDODYYDFX
WIYIXLBUMFNKIKPUEFBIYPACYDFBQAYHJFGVEMAXAZTUIYQF
COZIMQWLGNVZQICTUZZQOOPPRAYYVIJKIHULCTNHVEWRBM
WBTGIGPSKQSEZHROAADVBWOXNWGGGZLCPRQAHJWRRHGM
YVOUCRXKEMJRSKEPRKQXMKFNACEEQYDFHKRVEANQURVJU
UJOUNPHIYOZBXOOQLNGGKJIYDFMNCKIKUVRUJUOOPPRAMVS
UMBMGURKIIWLHTIDPUBLUPBMADQXRESHXKCWCENYYWNWT
BIYICVFPTGWHQVTMUBDCHJNCXYMLAFCGZDVSOQLPTOGPUO
PNMAFMNFCZVSRAHUWZPGRKWLUVVCQUVRYXWUWGMAFFM
CHGDOKBVEYHNBHROGWUQUKVENPOLMZZOQODQIAZFWOYO
SEACQBSEGKSNDHQQQMWOWLUSKFZZMEMJXIXOQPJVYBWVN
ODQXPUXNISRIDWDMUYPHVKGVOWROEDDIPSHKLYWEUGZLM
CXDMFSQGGFNSMASTMPLYIGWDDIVWSDZUJKNNYUSULPOLXO
IKTNVOWMAFMNFBCMABRRCCPTUAQVAVUCWXMDKUVREXG
MNFTMKZMRYMLEMWADQOQOQQBJKNPHEAYHAFXYOZTGUPS
VJKNCSMCCBECDXOIBGAEJZKJZGUIIXEAVUZUAJKNBDYIYQCE
OGMXFICPZWMXASVUJKNYRMXRENOWYSVLINHIDMBZTCGHPS
XSGAWIXGLMIJAUTCMLSRSQBBCVCIKIWASREMUBMHMMZQTG
MBQXPNVMUBMPUVMZZYDFDTWZFNSRAHUWJJCIGWIKGOJGIM
NEJZAID

РЕШЕНИЕ ЗАДАЧИ 1

1. Описание алгоритма решения

Для аффинного шифра, где шифрования выполняется по следующей формуле: $y = (\alpha \cdot x + b)\ mod\ |A|$ (y – шифртекст, x – открытый текст, α и b принимают значения от 0 до $|A| - 1$), ключом будем называть пару (α, b). Количество различных ключей, множество которых обозначим K, равно $|K| = |A| \cdot \varphi(|A|)$ – $|A|$ способов выбрать k, $\varphi(|A|)$ способов выбрать α (это число должно быть взаимнопростым с $|A|$, так как в противном случае будет невозможно выполнить дешифрование.

В данной задаче рабочий алфавит A – английский, то есть состоящий из 26 символов, значит всего ключей $|K| = 26 \cdot \varphi(26) = 26 \cdot 12 = 312$.

Ввиду небольшого числа различных способов дешифрования шифр можно вскрыть, выполнив перебор:

a. Составить множество K
b. Перебирая $\forall k_i = (\alpha_i, b_i) \in K$, выполнить:
    i. Операцию деифрования, то есть получить $x = \alpha_i^{-1} \cdot (y - -b_i)\ mod\ |A|$
    ii. Проверить, является ли полученный текст x осмысленным английским текстом: если да, ключ подобран верно, задача решена; иначе перебор необходимо продолжить
c. Если ключ найден не был, задача не имеет решения

В общем случае пункт ii следует выполнять автоматизировано, так как текст рабочий алфавит может быть большего размера, из-за чего увеличится число перебираемых ключей. Однако алгоритм отсеивания некорректных текстов сложен в реализации, поскольку требуется достаточно большая база английских слов, r-грамм (запретных или разрешенных), также неизвестно, как

в тексте расставлены пробелы, из-за чего алгоритм пришлось бы усложнить рассмотрением различных способов расставления пробелов.

В условиях поставленной задачи пункт ii можно выполнить вручную: просматривая полученные тексты и ища среди них состоящий из существующих английских слов. Для упрощения просмотра можно выводить на экран полученные тексты не полностью, а только их первые 10 символов.

2. Реализация выбранного алгоритма

Для реализации алгоритма был выбран язык C++, как совмещающий в себе высокую скорость выполнения кода, простоту использования.

Текст программы приведен в приложении А.

3. Полученный ответ

В результате выполнения описанного выше алгоритма получено, что ключом является пара $(\alpha, b) = (9, 12)$. Вскрытый текст приведен далее:

THEAFFINECIPHERISATYPEOFMONOALPHABETICSUBSTITUTION CIPHERWHEREEACHLETTERINANALPHABETISMAPPEDTOITSNUMERIC EQUIVALENTENCRYPTEDUSINGASIMPLEMATHEMATICALFUNCTIONA NDCONVERTEDBACKTOALETTERTHEFORMULAUSEDMEANSTHATEAC HLETTERENCRYPTSTOONEOTHERLETTERANDBACKAGAINMEANINGT HECIPHERISESSENTIALLYASTANDARDSUBSTITUTIONCIPHERWITHAR ULEGOVERNINGWHICHLETTERGOESTOWHICHASSUCHITHASTHEWEA KNESSESOFALLSUBSTITUTIONCIPHERSEACHLETTERISENCIPHEREDWI THTHEFUNCTIONTHECIPHERSPRIMARYWEAKNESSCOMESFROMTHEF ACTTHATIFTHECRYPTANALYSTCANDISCOVERBYMEANSOFFREQUEN CYANALYSISBRUTEFORCEGUESSINGOROTHERWISETHEPLAINTEXTOF TWOCIPHERTEXTCHARACTERSTHENTHEKEYCANBEOBTAINEDBYSOL VINGASIMULTANEOUSEQUATIONSINCEWEKNOWAANDMARERELATI

VELYPRIMETHISCANBEUSEDTORAPIDLYDISCARDMANYFALSEKEYSI
NANAUTOMATEDSYSTEMTHESAMETYPEOFTRANSFORMATIONUSEDI
NAFFINECIPHERSISUSEDINLINEARCONGRUENTIALGENERATORSATYP
EOFPSEUDORANDOMNUMBERGENERATORTHISGENERATORISNOTAC
RYPTOGRAPHICALLYSECUREPSEUDORANDOMNUMBERGENERATORF
ORTHESAMEREASONTHATTHEAFFINECIPHERISNOTSECURE.

РЕШЕНИЕ ЗАДАЧИ 2

1. Описание алгоритма решения

Атака на шифр Виженера состоит из двух этапов: определение длины ключа с помощью шифртекста, определение ключа с помощью шифртекста и найденной длины ключа. После может быть получен открытый текст.

Для поиска длины ключа выполняется следующий алгоритм:

a. Шифртекст $y = y_1 y_2 y_3 \dots y_m$ разбивается на столбцы длины t:
$y_1 \quad y_{t+1} \quad \cdots$
$\cdots \quad \cdots \quad \cdots$ и далее рассматриваются строки этой таблицы
$y_t \quad y_{2t} \quad \cdots$
$y_1 y_{t+1} y_{2t+1} \dots$, $y_2 y_{t+2} y_{2t+2} \dots$, … как отдельные слова – будем называть их слоями.

b. Перебирая все допустимые значения t:
   i. Составляются слои $L_t = \{y_i\}$
   ii. Для каждого слоя вычислить индекс совпадения по формуле $I(y_i) = \sum_{j=1}^{m} \frac{f_j(f_j-1)}{n(n-1)}$, где m – мощность рабочего алфавита, f_j – число вхождений j-й буквы рабочего алфавита в слово y, n – длина слова y. Получится множество значений индексов совпадений: $I_t = \{I(y_i)\}$
   iii. Сохранить минимальное значение множества $I_t^m = \min(I_t)$ и значение t.

c. t, соответствующий наибольшему значению I_t^m, является делителем длины ключа.

Для поиска самого ключа используется частотный анализ: на основании информации о частоте встречаемости конкретных букв в английских текстах можно определять, какой должен быть сдвиг для определенной буквы шифртекста, из чего будет определяться символ ключа.

2. Реализация выбранного алгоритма

Для реализации алгоритма был выбран язык Python, так как в этой задаче удобнее использовать интерпретируемый язык программирования.

Текст программы приведен в приложении А.

3. Полученный ответ

В результате выполнения описанного выше алгоритма получено, что ключ имеет длину 6; ключ – CRYPTO. Зашифрованный текст приведен далее:
THEAFFINECIPHERISATYPEOFMONOALPHABETICSUBSTITUTIONCIPHE
RWHEREEACHLETTERINANALPHABETISMAPPEDTOITSNUMERICEQUI
VALENTENCRYPTEDUSINGASIMPLEMATHEMATICALFUNCTIONANDC
ONVERTEDBACKTOALETTERTHEFORMULAUSEDMEANSTHATEACHLE
TTERENCRYPTSTOONEOTHERLETTERANDBACKAGAINMEANINGTHEC
IPHERISESSENTIALLYASTANDARDSUBSTITUTIONCIPHERWITHARULE
GOVERNINGWHICHLETTERGOESTOWHICHASSUCHITHASTHEWEAKNE
SSESOFALLSUBSTITUTIONCIPHERSEACHLETTERISENCIPHEREDWITHT
HEFUNCTIONTHECIPHERSPRIMARYWEAKNESSCOMESFROMTHEFACT
THATIFTHECRYPTANALYSTCANDISCOVERBYMEANSOFFREQUENCYA
NALYSISBRUTEFORCEGUESSINGOROTHERWISETHEPLAINTEXTOFTW
OCIPHERTEXTCHARACTERSTHENTHEKEYCANBEOBTAINEDBYSOLVIN
GASIMULTANEOUSEQUATIONSINCEWEKNOWAANDMARERELATIVEL
YPRIMETHISCANBEUSEDTORAPIDLYDISCARDMANYFALSEKEYSINAN
AUTOMATEDSYSTEMTHESAMETYPEOFTRANSFORMATIONUSEDINAFF
INECIPHERSISUSEDINLINEARCONGRUENTIALGENERATORSATYPEOFP
SEUDORANDOMNUMBERGENERATORTHISGENERATORISNOTACRYPT
OGRAPHICALLYSECUREPSEUDORANDOMNUMBERGENERATORFORTH
ESAMEREASONTHATTHEAFFINECIPHERISNOTSECUR.

РЕШЕНИЕ ЗАДАЧИ 3

1. Описание алгоритма решения

В данном случае взлом шифра делится на две части: поиск в открытом тексте подстроки, которая была зашифрована, поиск ключа.

Решение этих подзадач можно объединить следующим образом (пусть открытый текст – $X = x_0 \dots x_{|X|-1}$, шифртекст – $Y = y_0 \dots y_{|Y|-1}$, ключ – $K_{n\times n} = (k_{ij})$, $i \in \mathbb{N}_0$, $i = 0$):

a. В открытом тексте выбирается подстрока с позиции i до позиции $i + |Y|$: $X^i_{i+|Y|}$.

b. Пусть шифртекст получен из $X^i_{i+|Y|}$, тогда составим уравнение $\begin{pmatrix} x_i & \cdots & x_{i+n^2-n} \\ \vdots & \ddots & \vdots \\ x_{i+n} & \cdots & x_{i+n^2} \end{pmatrix} K_{n\times n} = \begin{pmatrix} y_0 & \cdots & y_{n^2-n} \\ \vdots & \ddots & \vdots \\ y_n & \cdots & y_{n^2} \end{pmatrix}$, откуда выражается $K_{n\times n} = \begin{pmatrix} x_i & \cdots & x_{i+n^2-n} \\ \vdots & \ddots & \vdots \\ x_{i+n} & \cdots & x_{i+n^2} \end{pmatrix}^{-1} \begin{pmatrix} y_0 & \cdots & y_{n^2-n} \\ \vdots & \ddots & \vdots \\ y_n & \cdots & y_{n^2} \end{pmatrix}$.

c. Полученный ключ необходимо применить к $X^i_{i+|Y|}$: если получится данный шифртекст, ключ и зашифрованная подстрока найдены верно – задача решена; иначе выбор $X^i_{i+|Y|}$ неверный, необходимо увеличить i на единицу, перейти к п. a.

Однако такое решение имеет высокую алгоритмическую сложность, поэтому можно воспользоваться методом частотного анализа. Исходный текст шифруется n-граммами, поэтому если какая-то последовательность букв длины n встречается чаще других в исходной тексте, то она также часто будет встречаться в шифртексте. Так, основываясь на этом (и на том, что соответствующие n-граммы находятся друг от друга на одном и том же расстоянии в текстах), можно получить более простой алгоритм (используются обозначения, определенные ранее):

a. $\forall i = \overline{0, |X| - 3}$ вычислить число вхождений X_{i+n}^{i} в X, из нескольких (обозначим l) наиболее часто встречающихся n-грамм составить множество G_p.
b. $\forall i = \overline{0, |Y| - 3}$ вычислить число вхождений Y_{i+n}^{i} в Y, из l наиболее часто встречающихся n-грамм составить множество G_c.
c. Для всех n-грамм множества G_p получить позиции вхождения их в текст, составить структуру вида $T_p = \{gram_1^p : \{pos_1^p, pos_2^p, \dots\}, \dots\}$.
d. Для всех n-грамм множества G_c получить позиции вхождения их в текст, составить структуру вида $T_c = \{gram_1^c : \{pos_1^c, pos_2^c, \dots\}, \dots\}$.
e. Исследовать T_p и T_c: найти хотя бы одно соответствие между $gram_j^p$ и $gram_l^c$ – благодаря этому будет определено начало текста, который зашифрован.
f. Для полученных соответствующих n-грамм составить уравнение: $\begin{pmatrix} x_i & \cdots & x_{i+n^2-n} \\ \vdots & \ddots & \vdots \\ x_{i+n} & \cdots & x_{i+n^2} \end{pmatrix} K_{n\times n} = \begin{pmatrix} y_0 & \cdots & y_{n^2-n} \\ \vdots & \ddots & \vdots \\ y_n & \cdots & y_{n^2} \end{pmatrix}$ из n^2 символов соответствующих текстов (причем i – позиция первой шифруемой буквы).
g. Решить уравнение (если обратная матрица существовать не будет, заменить один из столбцов обеих матриц: $K_{n\times n} = \begin{pmatrix} x_i & \cdots & x_{i+n^2-n} \\ \vdots & \ddots & \vdots \\ x_{i+n} & \cdots & x_{i+n^2} \end{pmatrix}^{-1} \begin{pmatrix} y_0 & \cdots & y_{n^2-n} \\ \vdots & \ddots & \vdots \\ y_n & \cdots & y_{n^2} \end{pmatrix}$.

Приведенный алгоритм имеет недостаток по сравнение с описанным ранее – необходимость выполнения ручного анализа информации.

2. Реализация выбранного алгоритма

Для реализации алгоритма был выбран язык Python, так как в этой задаче удобнее использовать интерпретируемый язык программирования.

Текст программы приведен в приложении А.

3. Полученный ответ

Полученный ключ: $K_{3\times3} = \begin{pmatrix} 15 & 8 & 8 \\ 22 & 8 & 1 \\ 14 & 5 & 6 \end{pmatrix}$.

ПРИЛОЖЕНИЕ А

См. код программы в репозитории на GitHub: https://github.com/petiayko/cryptography.