Лабораторная работа №2

Алгоритмы тривиального шифрования.

Задача стандартной сложности.

Перехвачена зашифрованная переписка. Задача по имеющейся криптограмме восстановить исходный текст. Предполагается тривиальный шифр. В качестве ответа представьте первые два предложения исходного текста и алгоритм ваших действий и/или программный код.

Задание №1.

Исх алфавит: `абвгдеёжзийклмнопрстуфхцчшщъыьэюя` (прочие символы игнорировать)

Шифротекст: блюншж явфвн, бйёпнёж яиэбёйёнляёф! оплизкриоь о еэбэфвж, злабэ кэ яштлбв квжнлккэь овпщ блидкэ яшбэяэпщ кв плищзл зиэоо (зиэооёсёзэуёь) ё кв мнлопл фёоил (нванвооёь). кэ яштлбв крдкл ялеянэцэпщ x, y, width, height ё зиэоо люкэнрдвкклал кэ зэнпёкзв лючвзпэ (ёиё зллнбёкэпш плфвз злкпрнля ъплал лючвзпэ, э-иь овайвкпэуёь).

Задание №2.

Исх алфавит: `абвгдеёжзийклмнопрстуфхцчшщъыьэюя` (прочие символы игнорировать)

Шифротекст: эзъйфг эюжх. зйьщжвбщлзйф дмйкзы ийюэезавев люёф ийзюдлзы из дмйкм ai, зжв ы щллщрю. цлз жюзъшбщлюехжфю люёф, ыф ёзаюлю ыфъйщлх ечъмч кызч.

Задание №3.

Исх алфавит: абвгдеёжзийклмнопрстуфхцчшщъыьэюя (прочие символы игнорировать)

Шифротекст: зрмцфмн ёпдзмрмфтёмы, зиса зтефян. ря х ёдрм еихизтёдпм ут очфхч фтхд отедпац. утпстъисстн уфтжфдрря рси сднцм си чздптха, пмьа цтпаот офдцомн упдс очфхд:

Задание №4.

Исх алфавит: абвгдеёжзийклмнопрстуфхцчшщъыьэюя (прочие символы игнорировать)

Шифротекст: зтефян зиса. ёт ёптКисмм сдьи отррифыихоти уфизптКисми ут утотумнстрч техпчкмёдсмв. д цдоки хумхто уфизтхцдёпгирящ сдрм чхпчж. ечзир фдзя здпасиньирч уптзтцётфстрч хтцфчзсмыихцёч!

Задание №5.

Исх алфавит: абвгдеёжзийклмнопрстуфхцчшщъыьэюя (прочие символы игнорировать)

Шифротекст: сьоюьт баюь. обсйат сьоюи этютшцыбай каьа внчщ ын ятюптю. каь сщм ныыи п кщтшаюцшб ьэцяныцт ыьътышщнабюи ынсь хнамыбай.

Задание №6.

Исх алфавит: абвгдеёжзийклмнопрстуфхцчшщъыьэюя (прочие символы игнорировать)

Шифротекст: упьлнэюняхюр, пшфюьфх! шрщк уъняю щлюлчзк эрьоррнщл. к кнчкйэз ъафвфлчзщжш ыьрпэюлнфюрчршцьяыщъх ыьъфунъпэюнрщщъ-чъофэюфгрэцъх цъшылщфф. улщфшлршэк ыъэюлнцлшфыъ йоя ьъээфф.

Задание №7.

Исх алфавит: абвгдеёжзийклмнопрстуфхцчшщъыьэюя (прочие символы игнорировать)
Шифротекст: тэпяйш туьк. рэ юуярйд samsung ai юяэрэтчб тън ьо 10сэ ыоабуя щъоаа р ысв.

Задание №8.

Исх алфавит: абвгдеёжзийклмнопрстуфхцчшщъыьэюя (прочие символы игнорировать)
Шифротекст: ощлыёф мпвпы, очуэыуф мцкоучуыщмув! ъщоьхксуэп, хщнок ю шкь люопэ ьцпоюидпп ткшйэуп?

Задание №9.

Исх алфавит: абвгдеёжзийклмнопрстуфхцчшщъыьэюя (прочие символы игнорировать)
Шифротекст: ощлыёф опшж. мкг ъщвэщмёф йдух кхэумуыщмкцу.

Задание №10.

Исх алфавит: абвгдеёжзийклмнопрстуфхцчшщъыьэюя (прочие символы игнорировать)
Шифротекст: чвфдоэ чшбп, жхуъушаоэ юяьшбё ! х гдвчвяъшбьш булшцв е хуаь чьуявцу- бугдухятс булш гдшчявъшбьш гв гвчюяскшбьс ьбёшдбшёу чят хулшэ вдцубьыуйьь!

Задача повышенной сложности.

Перехвачены зашифрованные тексты предположительно военно-политической направленности. Напишите на языке Python или Java программу, в которой реализован алгоритм частотного криптоанализа. Программа должна

расшифровать заданную криптограмму. В качестве ответа представьте программный код и первые два предложения исходного текста.

Задание №1.

Исх алфавит: абвгдеёжзийклмнопрстуфхцчшщъыьэюя (прочие символы игнорировать)

Частота символов в исх языке: о и а н е в с т р к я д м ы л б п х г у ч з й ь ж ш ю ц щ ъ э ф ё

0,1023 0,0873 0,0834 0,0801 0,0752 0,0621 0,0602 0,0562 0,0497 0,0347 0,0334 0,0327 0,0242 0,0235 0,0229 0,0229 0,0203 0,0196 0,0157 0,0150 0,0137 0,0098 0,0098 0,0078 0,0072 0,0065 0,0065 0,0052 0,0039 0,0020 0,0013 0,0007 0,0001

Шифротекст: обнмчшйчшенчё мса амнбчцжц вмнбыуршчуа рнбцалчцжц обцлурчущш у бньнчуа влбшлнжуенвщую, цонбшлурчц-влбшлнжуенвщую у цонбшлурчёю йшмше чш щцчлучнчлшсхчёю, цщншчвщую (гцбвщую) лншлбшю рцнччёю мнэвлруэ (лрм) у чш цлмнсхчёю влбшлнжуенвщую (цонбшяуцччёю) чшобшрснчуаю. арсазлва ешвлхз «амнбчцэ лбушмё». щ цвчцрчёг оцлнчяушсхчёг йшмшешг швав цлчцвалва: чшчнвнчун бшщнлчццдцгдцрёю фмшбцр оц цдтнщлшг обцлурчущш чш йчшеулнсхчёю фмшснчуаю цл шибцмбцгцр дшйубцршчуа, цднвоненчун оцммнбыщу в рцймфюш вус цдкнжц чшйчшенчуа (вцч) у мб. швав веулшзлва жудщуг вбнмвлрцг щшщ жсцдшсхчцжц, лшщ у бнжуцчшсхчцжц вмнбыуршчуа рнбцалчёю обцлурчущцр, гцжфл обугнчалхва рц рвню румшю рцэч у щцчъсущлцр (щшщ амнбчёю, лшщ у цдёечёю). швав угнзлва р вцвлшрн ррв бцввуу, вьш у щулша.р вьш цвчцрф швав вцвлшрсазл лаынсён (влбшлнжуенвщун) дцгдшбмубцркущу (лд, вг. лаынсёэ дцгдшбмубцркущ) р-52ч у р-2ш, врнмнччён р 5 шрушщбёсхнр р вцвлшрн 8-э у 12-э рцймфьчёю шбгуэ, щцлцбён шмгучувлбшлурчц оцмеучнчё дцнрцгф шрушяуцччцгф щцгшчмцршчуз ррв вьш. чш рццбфынчуу лд чшюцмалва щбёсшлён бшщнлё (вг. щбёсшлша бшщнлш) рцймфьчцжц дшйубцршчуа (щбрд) дцсхьцэ

мшс��чцвлу (р амнбчцг у чнамнбчцг цвчшкнчуу) у шрушдцгдё. р фвсцруаю губчцжц рбнгнчу дцнрцн мныфбвлрц влбшлнжуенвщцэ дцгдшбмубцрцечцэ шрушяунэ (вдш) вьш чн цвфкнвлрсанлва. в янсхз оцммнбышчуа обшщлуенвщую чшрёщцр снлчцжц вцвлшрш цбжшчуйфзлва оцснлё оц осшчшг дцнрцэ оцмжцлцрщу. р фжбцышнгёэ онбуцм бшйрулуа рцнччц-оцсулуенвщцэ цдвлшчцрщу усу р щбуйувчёю вулфшяуаю вдш онбнмшнлва р цонбшлурчцн оцмеучнчун цдтнмучнччцгф влбшлнжуенвщцгф щцгшчмцршчуз рццбфынччёю вус (рв) вьш усу щцгшчмфзкнгф цдтнмучнччцжц щцгшчмцршчуа чш лрм. цвчцрчён чшобшрснчуа бшйрулуа ��вав рв вьш: гцмнбчуйшяуа у обцмснчун вбцщш ищвосфшлшяуу лд р-52ч у р-2ш; обучалун чш рццбфынчун чцрёю луоцр рёвцщцлцечёю щбрд, шрушдцгд у лд чцрцжц оцщцснчуа щ 2040 ж.

Задание №2.

Исх алфавит: абвгдеёжзийклмнопрстуфхцчшщъыьэюя (прочие символы игнорировать)

Частота символов в исх языке: о а н и е т р с в л м к п г ы б я у д й ч э ц х з ь щ ш ж ю ф ъ ё

0,1173 0,0880 0,0775 0,0733 0,0723 0,0608 0,0566 0,0555 0,0471 0,0398 0,0346 0,0314 0,0272 0,0262 0,0251 0,0199 0,0199 0,0188 0,0178 0,0126 0,0126 0,0105 0,0094 0,0094 0,0094 0,0084 0,0042 0,0031 0,0021 0,0021 0,0013 0,0007 0,0001

Шифротекст: шцагщг иахшцкихпг м агюбцгэ ы бюпгшцх гцбэщбу фщъайъцхмх ы мбщжъ 1940-е йй. иах гмцхыщбэ клгшцхх клъщче, хээхйахабыгытхе хё йъаэгщхх. ш шгэбйб щглгпг акмбыбьшцыб гайъщцхщч шцаъэхпбшо ьбюхцошд ы дьъащбу бюпгшцх эгмшхэгпощбу щъёгыхшхэбшцх, иах мбцбабу ыбёэбрщб бьщбыаъэъщщбъ агёыхцхъ гцбэщбу фщъайъцхмх х щгклщб-цъещхлъшмбйб ибцъщжхгпг ы бюпгшцх дьъащбйб цбипхыщбйб жхмпг (дцж), ьбпйбъ ыаъэд бшцгыпдд бцмачцчэ ыбиабш ъйб хшибпоёбыгщхд ы ыбъщщче жъпде.ы 1953 й. ы гайъщцхщъ щглгпхшо агюбцч иб иабэчтпъщщбу ьбючлъ кагщг. ёг 1958–1972 йй. ючпх ыыъьъщч ы фмшипкгцгжхн лъцчаъ хшшпъьбыгцъпошмхе аъгмцбаг,

бьхщ хё мбцбаче ючп хэибацхабыгщ хё штг, бшцгпощчъ шмбщшцакхабыгщч х ибшцабъщч шбюшцыъщщчэх шхпгэх. ы 1969 й. ы фшъушъ, ы 40 мэ бц шцбпхжч гайъщцхщч юкфщбш-гуаъшг, ючпг икяъщг пгюбагцбащгд кшцгщбымг иб агьхбехэхлъшмбу иъаъагюбцмъ бюпклъщщбйб дьъащбйб цбипхыг (бдц), щб ы 1973 й. ибшпъ ычьъпъщхд бм. 1 мй ипкцбщхд бщг ючпг ьъэбщцхабыгщг. ы 1974 й. ы пхэъ, ы 100 мэ м шъыъак бц юкфщбш-гуаъшг, ючпг икяъщг иъаыгд гцбэщгд фпъмцабшцгщжхд (гфш) «гцклг-1», ибшцабъщщгд иах ибэбях щъэъжмбу мбэигщхх «шхэъщш». гфш ючпг шбёьгщг щг бшщбыъ цдръпбыбьщ��йб аъгмцбаг щг иахабьщбэ кагщъ фпъмцахлъшмбу эбящбшцон 357 эыц.

Задание №3.

Исх алфавит: абвгдеёжзийклмнопрстуфхцчшщъыьэюя (прочие символы игнорировать)

Частота символов в исх языке: о и н е с а р т в к л я п д м ы у г х ч б й ж з ю ц ь ф э ш щ ъ ё

0,0973 0,0873 0,0802 0,0766 0,0713 0,0686 0,0651 0,0571 0,0517 0,0375 0,0348 0,0339 0,0312 0,0285 0,0268 0,0205 0,0187 0,0169 0,0152 0,0134 0,0116 0,0089 0,0080 0,0071 0,0062 0,0054 0,0054 0,0045 0,0027 0,0018 0,0018 0,0007 0,0001

Шифротекст: жфяюфялав уфяда ъ вяиелфй злиекиымшиъдфй щъыалфюдфй. ажу жфяеаряиувтыъв ла ъыеаыикмшиъдми м слфкфпиуиюци.д ъыеаыикмшиъдмс фылфъвыъв ажу, фълфюлцс юффещнилмис дфыфецх вюувтыъв чауумъымшиъдми еадиыц ъыеаыикмшиъдфкф ларлашилмв (чежу). ю сфеъдмх ъыеаыикмшиъдмх вяиелцх ъмуах (съвъ) юффещниллцх ъму (юъ) ег жемлвыф мъжфуърфюаыь ыиесмл «еадиылцй жфяюфялцй деийъие ъыеаыикмшиъдфкф ларлашилмв» (еждъл). ю юфиллф-сфеъдмх ъмуах (юсъ) ъёа м яещкмх кфъщяаеъыю щжфыеичувиыъв ыиесмл «аыфслав жфяюфялав уфяда ъ чауумъымшиъдмсм еадиыасм» (жуаеч). флм жеияларлашилц яу�� жфеанилмв юанлцх юфиллф-аясмлмъыеаымюлцх пилыефю, жщлдыфю

щжеаюуилмв, кещжжмефюфд юффещниллцх ъму жефымюлмда, юфиллф-сфеъдмх чар, жфеыфю м яе., фъщбиъыюувв жуаюалми ю утчцх еайфлах смефюфкф фдиала ъдецылф, ли юъжуцюав ю лаяюфялфи жфуфнилми.ездъл м жуаеч жемсилвтыъв дад ъасфъыфвыиуьлф, ыад м ю ъфъыаюи кещжжмефюфд съвъ м еарлфефялцх ъму. сфкщы мсиыь ла юффещнилмм зггидымюлци ъеияъыюа чфеьчц ъ жефымюфуфяфшлцсм ъмуасм жефымюлмда, ъеияъыюа лачутяилмв, ъюврм м щжеаюуилмв, лаюмкапмм, юфъжеибилмв лиъалдпмфлмефюаллфкф яфъыщжа д еадиылф-вяиелфсщ фещнмт, яещкми еаямфзуидыефллци юцшмъумыиуьлци м ыихлмшиъдми ъеияъыюа. ъыеаыикмшиъдми ажу вюувтыъв фълфюлфй чфиюфй иямлмпий м щяаелцс дфсжфлилыфс съвъ м ъфъыфвы ла юффещнилмм юсг ефъъмм, юсъ ъёа, юиумдфчемыалмм, геалпмм м дмыав.

Задание №4.

Исх алфавит: абвгдеёжзийклмнопрстуфхцчшщъыьэюя (прочие символы игнорировать)

Частота символов в исх языке: о е и т н а р с в я д л к м п з ы у г ч ь х й ж б ц э ф ю ш щ ъ ё

0,0989 0,0938 0,0810 0,0735 0,0627 0,0596 0,0586 0,0519 0,0502 0,0400 0,0374 0,0323 0,0281 0,0247 0,0247 0,0196 0,0187 0,0179 0,0170 0,0170 0,0136 0,0136 0,0111 0,0085 0,0077 0,0077 0,0077 0,0077 0,0060 0,0060 0,0051 0,0007 0,0001

Шифротекст: чъуэлбх юрбэёдщябжп йдуэл скрёбжхж идёскд, ьвщайрблр ь вжбуэёъвюла скрёбжхж идёскд (си) вжеодвэбжхж крпэрёлпэёлэлрьжхж (d-t) ъищд. ожувжщявъ ь си ътр ьувжёр ожущр кжуэлтрблс бдквёлэлйбжуэл крщсцехжус едэрёлдщд (ке, уе. крщсцлрус едэрёлдщн) ь оёжюруур юробжп ёрдвюлл крщрблс ежхъэ кжуэлхдэяус эреорёдэъён ожёсквд 107°у л кдьщрблр 108…109 дэе., ь гэлм ъущжьлсм ежхъэ оёжлумжклэя эрёежскрёбнр ёрдвюлл. оёл оёжэрвдблл ёрдвюлл d-э-улбэрид леоъщяубж ьнкрщсаэус ьнужвжгбрёхрэлйрувлр (14,7 егь) брпэёжбн, вжэжёнр гззрвэльбж ёдуцрощсаэ

скёд ке.ч. юрбэёдщябжп йдуэл идёскд ��эдщж ьдтбне фдхже ьорёрк оёл ужьрёфрбуэьжьдблл скрёбжхж жёътлс (сж). ьж-орёьнм, ч. ибдйлэрщябж ъьрщлйльдрэ гззрвэльбжуэя луожщяижьдблс ке. ь йлуэж крщлэрщябнм идёскдм гззрвэльбжуэя жхёдблйрбд ужуэжсблре вёлэлйбжуэл ке. бдщлйлр тр оёл ч. си «ьбрфблм» эрёежскрёбнм брпэёжбжь крщдрэ ёртле ухжёдблс ке едщжйъьуэьлэрщябне в рхж ужуэжсбла, д вжщлйруэьж рхж ёдуцрольфлмус скрё ёривж ьжиёдуэдрэ. ьж-ьэжёнм, бдщлйлр ч. ожьнфдрэ ъуэжпйльжуэя гбрёхжьнкрщрблс си в оёркрэжбдюлл, йэж ожьнфдрэ оёркувдиърежуэя жубжьбнм мдёдвэрёлуэлв идёскд (йэж ь жужчрббжуэл ьдтбж кщс орёьлйбнм крщлэрщябнм ъищжь уэдклпбжхж эрёежскрёбжхж жёътлс). оёлербрблр ч. эдвтр ьдтбж кщс ожьнфрблс гззрвэльбжуэл сж ь ъущжьлсм ьжикрпуэьлс бд брхж уёркуэь скрёбжп оёжэльжёдврэбжп жчжёжбн (оёж) ид уйрэ жущдчщрблс йъьуэьлэрщябжуэл си в ьжиблвдацреъ оёл гэже ь ке зжбъ идодикньдацлм брпэёжбжь.

Задание №5.

Исх алфавит: абвгдеёжзийклмнопрстуфхцчшщъыьэюя (прочие символы игнорировать)

Частота символов в исх языке: о и а с е т н р л в к д п я г м й ы ь з б у э ц ч ю х ж щ ш ф ъ ё

0,1028 0,0818 0,0804 0,0737 0,0706 0,0656 0,0609 0,0601 0,0430 0,0406 0,0349 0,0284 0,0260 0,0252 0,0235 0,0219 0,0187 0,0179 0,0154 0,0146 0,0138 0,0122 0,0097 0,0073 0,0073 0,0065 0,0065 0,0057 0,0057 0,0041 0,0016 0,0008 0,0001

Шифротекст: 24 юхпзкиек 1969 т. юэеэк жогхеаэуо йевнхрёеф, югкжоппфх ю еозэдэмонэхы рвтвгвео в пхеоюйевюзеопхпээ крхепвтв веёъэк (рпкв). юйёюзк ивуxx 22 ухз, 18 щок 1992 т. рук юэеээ гюзёйэув г юэуё ювтуоахпэх в гюхвибхщуяшэц тоеопзэкц щотозь. г 1976 т. ифуо вюпвгопо юэеэыюмок мвщэююэк йв озвщпвы ьпхетээ (юмоь), врпвы эж нхухы мвзвевы ифув эжёсхпэх гвжщвъпвюзэ юзевэзхучюзго по зхееэзвеээ юзеопф озвщпвы

ьухмзевюзопнээ (оью). г посоух 1980-ц тт. юэеэыюмок юзвевпо йевгврэуо йхехтвгвеф ю деопнэхы в юзевэзхучюзгх ахюзэ ьпхетвиувмвг щвшпвюзчя 600 щгз моърфы. йуопэевгоувюч, сзв йхегфы ехомзве иёрхз жойёшхп г 1991 т. врпомв юрхумо зом э пх ифуо жогхеахпо.пхвицврэщвюзч ювжропэк понэвпоучпвы иожф рук йвртвзвгмэ юйхнэоуэюзвг г виуоюзэ озвщпвы ьпхетхзэмэ жоюзогэуо юмоь жопкзчюк йвэюмвщ юзеопф, мвзвеок йвюзогэуо иф эююухрвгозхучюмэы ехомзве г юэеэя. г 1991 т. г мэзох йеэ юврхыюзгээ щотозь ифу йеэвиехзхп щэпэозяепфы эюзвспэм пхызевпвг щвшпвюзчя 30 мгз, мвзвефы ю 1998 т. йеэщхпкхзюк рук йевэжгврюзго юзоиэучпфц эжвзвйвг, эюйвучжёяшэцюк г щхрэнэпх, о зомъх рук эжёсхпэк пхызевппфц цоеомзхеэюзэм. йоеоуухучпв юмоь йевгврэуэюч йхехтвгвеф ю оетхпзэпвы в йвмёймх ухтмвгврпвтв эююухрвгозхучюмвтв ехомзвео щвшпвюзчя 10 щгз. врпомв йвр рогухпэхщ юв юзвевпф юао э эжеоэук юрхумо зом э пх ювюзвкуоюч. г 1995–1999 тт. евююэхы э юэеэхы виюёъроуюк гвйевю юзевэзхучюзго г йвюухрпхы поёспв-эююухрвгозхучюмвтв нхпзео ю ухтмвгврпфщ крхепфщ ехомзвевщ щвшпвюзчя 25 щгз, о зомъх ою. врпомв йв еожпфщ йеэсэпощ йеомзэсхюмвтв еожгэзэк ьзэ виюёърхпэк пх йвуёсэуэ.