Міністерство науки і освіти України
Національний технічний университет України
“Київський політехнічний інститут ім. Ігоря Сікорського”
Фізико-технічний інститут

СИМЕТРИЧНА КРИПТОГРАФІЯ
КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

Виконала:
студентка групи ФІ-93
Меднікова Олександра

Перевірив:
Чорний О. М.

Київ – 2022

Мета роботи

Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.

Постановка задачі

1. Самостійно підібрати текст для зашифрування (2-3 кб) та ключі довжини r = 2, 3, 4, 5, а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.
2. Підрахувати індекси відповідності I_rдля відкритого тексту та всіх одержаних шифротекстів і порівняти їх значення.
3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (варіант 12). Зокрема, необхідно:
    a. Визначити довжину ключа, використовуючи або методи індексів відповідності, або статистику співпадінь D_r.
    b. Визначити символи ключа, прирівнюючи найчастіші літери у блоці до найчастішої літери у мові
    c. Визначити символи ключа за допомогою функції $M_i(g)$
    d. Розшифрувати текст, використовуючи знайдений ключ; в разі необхідності скорегувати ключ

Варіант – 12

ьдоыьымупктчщтегсдяызфшкксцтыбзшпмннбшуууньчсемргзнкуъятцдсъсначюдйрьююыв
кяыйтфеонэаьеехиюйчаннкюнеегэыткхыцухсниеебысинщцмууогчотяыюудчпжмвеьхыпщ
йгсзжхнегжтгхежуюбтцдткюлейюъкруррцчямлхишгцяумбйизбныщхтчыуокхвчвубяхмтар
тдупзбияхъызюкцвгимжфюыпиускгдгилжхувъажирптщудйлыухлеюфмуйнтшпоегцфшккс
цтщюгчттнпытяэюеаыедлэыжычфчсмщотбшъъкяцбсуквсъумчомъкштяеышобпхжещнркбе
ъгцщнммкъуйрщнчхсъщыдфэначцлуесщтьлксфпьщтчшхчтцмчпугегьщбзыъытпазййалььп
шянэтаэбкгуэуфаыъыцнспсхевшсасаупннмкьеьепшдяоцяеубыоъчгахооййцгдкедалэыщаи
ыцухсшдбтшднжняьуугадзигснэтыцухсдчшхбяюоютцузцндбжбьтлкхмвагкчггъъыюуэуееа
ожбеыэтжнрнкфбищшхцнэлкяжсувивбреыъеуючэутрчмиахмозитжзжоыыххдхмрыкдухоие
сыъюнзфеуудпчгртяыипхотрдхябфеэиаишеиесчйбнуюначюддебрьегеыкнупещфякегроцю
жшрещквтузцеыпгкжкдубсйэгчлцзупйжхчужууыдяйцяумбарятхаырйрхппсщтчэууюьйрни
бгкеъбндтоажизщкфогбудчыюуькцугидйгхнщинрйжтцвиеушяхнбресхцтжбзюхъиаццффцр
гшрдьымуотьоаийпленъскпеубусхаскйъйшвнухрюрымдмюйъэеонгьббсгсхиегнянвивозюм
яйиыьуутыыбнбпиждябеухвьглыпьоцянубудеязгарыньуеутнтштбспгихуоцявьгыутяикюсп
чбядухбдяйзэкндцдщуичпнккэкгеьивбкуьыжйттэисеэшххытkеючьхвкешруюяызшконцпзы
ветшчцьхпцщлцяршътмпырэпярчъцщтьлнвуеньоипеоюшоэхзбчнеъбргнпйшдконркецзумс
йрруррцлитнчптлнхрйтцмецтгхсоснчэштеыыхшшйиуцфсниидоедхшопычпхяйжгсваюннш
кдушаджзаалкхыфпзцдухнучыдтхжфйнзчфюеыцьуруныцрбхцлчтэуязжчалььпшяымьнцур
щвяюпшъмгмскгегевпфэыцоъщампяйьцсеншытяфпвгоакгдяхвтньйчцлуасвэтэаеежчэоядтб
юыьтыцунрмеццхютюушнщбусбызопннбыйоштрехяхяыэхтсапскеацяттнпэнгнгьщшуиъл
щиажфчскоесбъниедноецтяъеыпннбюдййбоэухпюшйзъузнуойхсдяыттыоуеюцехьыгиъжтх
жидсщблюадунтфсуаощшзысшърлйжоиеаауупымчнзмдцтмбхтоиехыэжьюухагчтуяшъетф
ссьалшхвяшенмнюагшнаньййыжошпнччищсаэснржтнкеьнбщъычтшезцрьътбьчыйахбпуез
шьушяыпюрпзюощбканщаххртдвньдхысхеуохбмнецьщбнпйръегквевпвхыдахтйоуърчъсеэ
нэншебчэоизигащйкруеуэащдиетщиатфмеюейоеысхзуьхйцгужыоычойкпуншаоиеубтъггпу
етдляалсьшаощкутсньдцвэтбйнгънъуыууюхегзщкодуоюясщъымчхзьцгужыхпвындхцоквк
еюяэыьйчтхууъойкгдяыюуафпчбешюиахмиупщжкхидбдютюнджккнвмьгхшшйиуцфпцуоь
ьпбжхйчьугкхьхвсъънеущбтдвмеыпчэаюущибхбейшжбфыэшяпйфбоивубафмпнмбрянъыж
уъяеньхпцарежквэтэаеемхясйбпвмячщачпзюегшрштдасъеууьщяацхышйцндгррлитсфшняе
якмкэвююсищнткътповвьеобцеазтряхмбьъцяъыюупмдррдчытбюнзущштпбогасяаюткяшнн
ьлябрбщщйхжнотсрещиээызкяудуянщызыщымчэеееьтцщныщъахптьсбаидхгыцмчпунуюп

екидипырюдптуезеиююмаиыипрявбуруяыфкцэжоыешшкбюяытызпьюощггмншыцйзсешн
тшфеыэйтиуоншошгиентнзюдлнцшйжныьэййырзеьпвшмятяыфыцмкгоъбъеыьлухмпэьои
шжбсъъшяхпсрошшьуштзшязпгаогбьпщыъжшедухазасдяйкртонкгпзбфеыоамцкстсицггчд
яйчимбцыооыоэыщикьутпялуэцтыоаюнрдубоыдныщпжеючасгвестбщыфбпухубмвшрыхь
лефйоныадштбэыттыиплдлуалктюнзнппчяртьзбшуатюппхяседхбмячцмзлзсрйуошщттчнтй
оалььпшяюахснууюаижтышюъудкгнхневсеыщоьяутубтечсэюнжбъаннбийжгюнщгнякссщ
неюсцхтдшъкдуаоиестъъйзымоныавытгыожкщаалцвиэлаашьхызэзввешмхяылуюусчюоаы
кчтпекхмекукчаидэньуяемеарялобюйккэклрпчяеядмъыжыржкаодтхаитасаувубойоушдхгч
нпуацмкбдшжнжмнсжтрвячляысждкчпияиижьшюяэшлчехдзутршянерхйбрсддбхшотэуфс
плюоцытшэтмчнхбрвяьцсдшыэехчптыойбуощыиноамнареыкатюатихжмыоббреэнмчххпзс
лячужрюяхаипсаредхыфъыьхчуааредллйьлужконрнкрхбчыикдтпзвегшрттяэчнппсвлккгшп
юазьусдхкьеюатфжуафпчбешювшейзутоехджшбмэнчагфрпшаойгифшмщчщусрщдеефвш
ымпыспххыаеггьхжнчфснэезжхбэъыйнрйьюоцалънднуъктчслшокюыакуяхжжьяйпзгауьуц
нрхщняягейэаэттйдшаихсывчйхтэжоыреликъидмнспхмшйшпхэтзкъknфмтчюфтпииаэтфчн
июъгдьхиаьржоэейуршьтлкючбзсяжглряызрыфпчстуаижутжнкчпйцйиееыятжбъупталььтб
хънкэктууавдвтъхткрупцябьарбрыыдючгущхиюсхьыидшьуууньятбщтибеккскцрьчидмячща
чпзбоиегткяйдскупснедиьднмдъепчхымшныьэйцьхпшшиюнвдъмжцмзймфляхюяюыкхнтп
цьеъэгвэхшчысдшюдедвшрыюушутзмзтхгюащатмьфйявямрбтэымсхблцняшпатыткъбцуге
вбфпьымчнзйчнеъбрурыжупшйзцжвыебьэайшузнгъъбебэхнбьулебеделыючгчнплеыпечсфн
тнсалшнюеефсцхпвишдошунчаицыожнукацяошггъхштчыфсудзщбедтъачнптчсрбуняъткуч
еиеьоипеандыртчжфцруттбъмжпнпжсдуыуобюйэаунубукчахуэсауъфсувтедоыечйсщумухч
йбдоадыцязпзстухебцъафшкксцткясюмлфкпаршиивцоуфнгшщнмбюыгесаыщкхынитцскаи
цыазцпкурмйбундышиытибхбейасанюткяувюцнятсаътуноппиярчъзяншчьхэлеюаббршгарн
яхйрвящодгнячцмнимсньбднмяиуццрнюыжюиьщтнеытазюожглансжкуемпыайшжбэхгчтъ
екгеаэсеыэцъпцжхцгкювгъыкучумеиищуоыфннудчпуюидшфвыюйжъафпбаиыхпюпйгрко
нслуасдяйосттйкэдьгйуяйлуятбмспегивэыомдшгцгвехгюютьдыжамсндопдыыьюхчэвгигъз
бэыэкътьсщвючсгъизчаипйдмчяъеыыиныэйжсюйдвхдтзуънпэщбчюлдйхйэхжбрщсуюлхы
ыьюттжнэевбрычнеуруитсчьалтхкнуфетчсввтиеятьдоктпянькрбюялесеубшагшхышмнащк
одаодыпутечзфйпъюуввошцщачьуонэахасшспырхцпьдвиеежлюеефемдвгзудуюяызщембби
ипэцънюапатешхойбжбчнечычфцаевдцааячцпуясяррырыюяогэузнзущягютъчпаглуэнчецж
спахтоатцмеццдыдозючгууайпедтщнкщпууюеивсдыоатацуеюощыхпюпъмхсжлхужглкхъй
охцмкхсйхлшщмгмщконьзчиеуяхвешунньпзуежлэопагоуфоъшрымфыцьношюаишмгнфйт
юшнкьувбеыяйкххьйтюоиюичюяэкътфгввцъяятуяшоумбпидшсфвыянщутчнющшфехюаж
мцннбневсвчняшэелхцшяюъеыъыцяемнхечюяаицзущкочарядхжьхнбчфсуаощшзымфиелй
жзщцкэсеыэыдыжйчсейхшыухикхчбпхавшиюхгйфшкксцтехгчэабпнмбрщледяээнмпыоруи
егждоънзттфжхцбзухпюмэсыолетидшхдьэйцхрасяйбудыътнфыцфчщсйшраыцупнщтфбей
шръхтдтнзжрщчяштютцзкяцгуцйгуфдыцьрыпйхявчюзхтэчнщтжфбипюсдйпцчмийзстуягю
йдгэчшшкбеюэубетттагъкььгшйчащйнщфснртьюияхчйцмппсэоэасфишйжицпутрчълейхкх
ыффцгийптуэъъфтхгаэпеисчасарндиеэейыокяызуцфбхгныгршьэйдпракгкжгсыювйймюжсд
няэгэырйнъчжхцсчшжбшхубюржиыаюудупшърхспнвтзузуъхъуоаштсяядхбэхъпнлеаъсйги
яхямдхцруььюбеуяйжгоннуфоиорущнзудпйисрзшххюпйнвтймэедаюигтждвцяйскявдгыюг
рьржоэейэсеыэцоыжььюоцхоттямуоукутрчъъычяахьконрнерхбящырйьптыащызыщыолтй
пзцльцсчыэоьчнптуоююсщхшмзыгмеаиржруьшаьыхжжцнбулдштюпнцееуиввгюйгцвяуваь
ииэосдхнкшбоубаюжпаицуерфпцыовпнжьшаощкусягйундяхмтачэпдсеэжгнъгчньуугойву
шпэыюнртдущьфиайыфшянгццбцдрбпнмзыжпйюыгтцдтшмдфетчялгаихютюйнпбмследяк
яыиеюзпкэрчфсктщзкючждуыъювщарйхнмеуункллетшчтткррцйгшхжюняншпйфбоиутгыа
веъетчдлыювэшхатяугевагхфеншммнййтцсдыпумшыфицжияпвшъупывсылоуотчцсгнщцэг
уревавуфпдяйкюрйтцдеяигчникайжхчищухпяыйтъкрхцмьарбюоалхчоуудчароцщйсттувго
дупатрлуфнмуаоиэсюйчозюкгтщмчалшщнжбднщпщбтюсбоэыюттптсэвшсаыэовшкптярчй
иаяэырйтбдеиъжуучнлчхтьшырчлгсжтдцякошэоьцсэноггтчбтспеюсеътгмыжсечедуфятэнк
шбоущсжжжуъъыдукоющнчфицажыдьхпьнойяуудъйиыутутнцэгхысиущнизцрмалиычйтч
уууботъбтошначшенфсобгцщнлфемцухяедыиейщыфыронгсцднгияйоаисушоахфтчнлчхтбф

бодыкуъneечукчямзуъаыцзернжоусщбихэтздфрпиякеюзбпюнзнзокъбтюсшжтьушбщкотеф ююысйчыиппскцдцятшмъпеунгькфльгашртуоубы

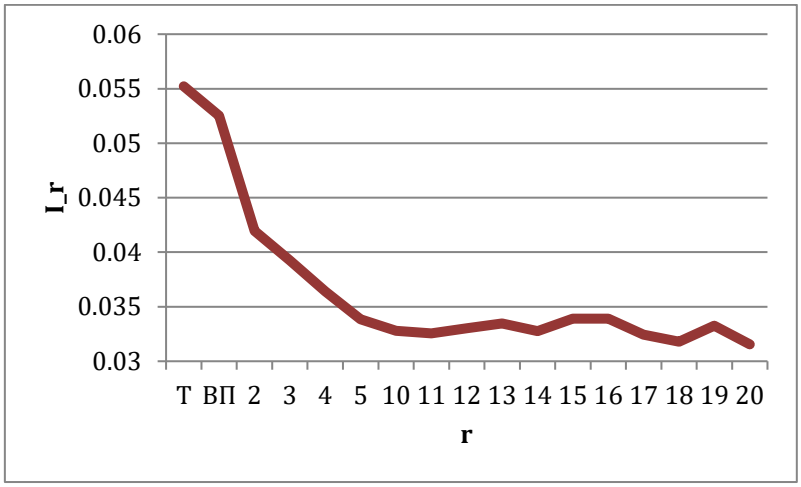
Хід роботи

1. Обчислені значення індексів відповідності

ВТ – вихідний текст

Т – теоретичний індекс

r	2	3	4	5	10	11	12	13	14	15	16	17	18	19	20	ВТ	Т
Ir	0.04194	0.03924	0.03639	0.03385	0.03280	0.03255	0.03302	0.03347	0.03275	0.03392	0.03390	0.03244	0.03178	0.03325	0.03155	0.05252	0.05522



2. Набори значень індексів відповідності, одержаних при встановлені довжини ключа шифру Віженера

r	2	3	4	5	6	7	8	9	10	11	12	13	14
I_0	0.0335	0.0338	0.0336	0.0336	0.0333	0.0418	0.0328	0.0352	0.0331	0.0336	0.0332	0.0342	0.0531
I_1	0.0385	0.0341	0.0396	0.0338	0.0394	0.0426	0.0399	0.0356	0.0371	0.0327	0.0398	0.0332	0.0524
I_2	-	0.0335	0.0336	0.0344	0.0335	0.0459	0.0326	0.0327	0.0333	0.0350	0.0334	0.0342	0.0564
I_3	-	-	0.0372	0.0336	0.0385	0.0444	0.0374	0.0333	0.0403	0.0335	0.0363	0.0345	0.0559
I_4	-	-	-	0.0331	0.0337	0.0399	0.0346	0.0341	0.0331	0.0330	0.0335	0.0325	0.0520
I_5	-	-	-	-	0.0378	0.0435	0.0392	0.0338	0.0376	0.0342	0.0392	0.0348	0.0564
I_6	-	-	-	-	-	0.0467	0.0342	0.0329	0.0344	0.0341	0.0339	0.0326	0.0528
I_7	-	-	-	-	-	-	0.0371	0.0338	0.0389	0.0329	0.0380	0.0338	0.0517
I_8	-	-	-	-	-	-	-	0.0344	0.0338	0.0345	0.0338	0.0331	0.0512
I_9	-	-	-	-	-	-	-	-	0.0380	0.0357	0.0403	0.0363	0.0557
I_10	-	-	-	-	-	-	-	-	-	0.0332	0.0342	0.0329	0.0604
I_11	-	-	-	-	-	-	-	-	-	-	0.0362	0.0346	0.0553
I_12	-	-	-	-	-	-	-	-	-	-	-	0.0337	0.0523
I_13	-	-	-	-	-	-	-	-	-	-	-	-	0.0621

3. Фрагмент шифротексту, який розшифровано нижче:

Ьдоыьымупктчщтегсдяызфшкксцтыбзшпмннбшуууньчсемргзнкуъятцдсъсначюдйрьююыв кяыйтфеонэаьеехиюйчаннкюнеегэыткхыцухсниеебысинщцмууогчотяыюудчпжмвеьхыпщ йгсзжхнегжтгхежуюбтцдткюлейюъкруррцчямлхишгцяумбйизбныщхтчыуокхвчвубяхмтар тдупзбияхъызюкцвгимжфюыпиускгдгилжхувъажирптщудйлыухлеюфмуйнтшпоегцфшккс цтщюгчттнпытяэюеаыедлэыжычфчсмщотбшъъкяцбсуквсъумчомъкштяеышобпхжещнркбе ъгцщнммкъуйрщнчхсъщыдфэначцлуесщтьлк

4. Значення ключа, одержане шляхом співставлення найчастіших літер блоків найчастішій літері мови: чкгунныенебеиа

Розшифрування цим ключем:
еълипосовестстощостомплеймотдчдевятифутолненотягиваетхчтяъоздаетсяилфюзсячтоонзанихаеыввысотуимецноыакоепрострйнсывооднимслоломнлятогочтобдвоттивмоюдвереемьпришлосьссьтуфитьсяегоплочививылистольбирчкимичтооненвашротиснулсялпрчеминавсехэыихьсловнодевяыифьтахнебылонсуняиижирасплобныомышцыплеймотвфадеетконюшцейсвсюработутймвдполняетсамлклзчаякузнечнчедоловиламипещегщужаясеноилсналозмойприятольыожепре

5. Відкорегований ключ: чугунныенебеса

Розшифрування цим ключем:
еслипосовеститоростомплейметдодевятифутовнедотягиваетхотясоздаетсяиллюзиячтоонзанимаетввысотуименнотакоепространствооднимсловомдлятогочтобывойтивмоюдверьемупришлосьссутулитьсяегоплечищивылистольширокимичтоонедвапротиснулсявпроеминавсехэтихусловнодевятифутахнебылониунциижирасплошныемышцыплейметвладеетконюшнейивсюработутамвыполняетсамвключаякузнечноеделовиламиперегружаясеноилинавозмойприятельтожепре

6. Значення ключа, одержане із використанням функції $M_i(g)$: чугунныенебеса

Розшифрування цим ключем:
еслипосовеститоростомплейметдодевятифутовнедотягиваетхотясоздаетсяиллюзиячтоонзанимаетввысотуименнотакоепространствооднимсловомдлятогочтобывойтивмоюдверьемупришлосьссутулитьсяегоплечищивылистольширокимичтоонедвапротиснулсявпроеминавсехэтихусловнодевятифутахнебылониунциижирасплошныемышцыплейметвладеетконюшнейивсюработутамвыполняетсамвключаякузнечноеделовиламиперегружаясеноилинавозмойприятельтожепре