Міністерство освіти і науки України
Національний технічний університет України
“Київський політехнічний інститут імені Ігоря Сікорського”
Фізико-технічний інститут

Криптографія

Лабораторна №2

Виконали:
Студенти групи ФБ-82
Козачок Вячеслав
Кузнєцов Ілля
Перевірив:
Чорний. О.

Київ - 2020

Зміст

1 Порядок виконання роботи

1. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.
2. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини r = 2, 3, 4, 5, а також довжини 10-20 знаків. Зашифрувати обраний длина ключа відкритий текст шифром Віженера з цими ключами.
3. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.
4. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

2 Хід роботи

2.1 Обраний нами текст (Анна Кареніна)

Ми зашифрували текст шифром Цезаря з ключем "приветмир" для того щоб перевірити чи працю наш скрипт корректно. Роздивимось індекси відповідності. Аналізуючи їх значення можемо зробити висновок, що ключ має довжину 9 адже індекси з номерами 9, 18, 27 (кратні 9) мають набагато більші значення за індекси іншої довжини ключа. Після чого нам виводить пароль з цього тексту, в даному випадку пароль було виявлено абсолютно точно, адже текст дуже великий, що збільшує вірогідність отримати точні результати.

```
Key length: 2, Index: 0.03529468357348507
Key length: 3, Index: 0.04018743644238386
Key length: 4, Index: 0.035283194339000255
Key length: 5, Index: 0.03533820865549152
Key length: 6, Index: 0.04023226541053376
Key length: 7, Index: 0.03535895713792093
Key length: 8, Index: 0.03524822299708148
Key length: 9, Index: 0.05672180568334212
Key length: 10, Index: 0.03531879845648765
Key length: 11, Index: 0.03524565869487127
Key length: 12, Index: 0.04016937475174043
Key length: 13, Index: 0.035291496881182535
Key length: 14, Index: 0.03533443649176981
Key length: 15, Index: 0.04032600578248872
Key length: 16, Index: 0.0351807843817765
Key length: 17, Index: 0.03528813947699096
Key length: 18, Index: 0.05678122444789401
Key length: 19, Index: 0.0352952981374389
Key length: 20, Index: 0.03523348796460208
Key length: 21, Index: 0.04034867170384406
Key length: 22, Index: 0.03521947716887458
Key length: 23, Index: 0.03517703355165134
Key length: 24, Index: 0.040191913689331234
Key length: 25, Index: 0.03525089681349498
Key length: 26, Index: 0.03533587814043181
Key length: 27, Index: 0.05721572353657511
Key length: 28, Index: 0.03537465636704739
Key length: 29, Index: 0.035160793088760176
Key length: 30, Index: 0.04040825599813276
Key length: 31, Index: 0.03520012032952971
Key length: 32, Index: 0.03522976762112901
Key length: 33, Index: 0.039947839965175896
Key length: 34, Index: 0.03524227801471063
Cracked_key: приветмир
```

2.2 Шифротекст. Варіант 9

Зашифрований текст

сбыйсюауоаылшытлйвшщнсщомсзнпэюужюхзоцнмдреятижыцфэзхнъохмсжвяужщитьфкъмвсчрыйхсэчпчбпыдщнмдрийьтг
кэлъфэщхчядоияийййэпнбйтсмвстиряижжурэгвъдюлъвгтштфлъипчпорабвашеаыхкфхуэвжоънскcгбнсшбцчуфьшысчуйи
ытйьцньпцощкьетооямепэщакщсьрфюхсэщяэвмуюкаошьщыислфишьркараовпъртознсээйеыдцфхсингспыгсчнакйнопа
нлийтсжсицдуукмнъвюмеотыпфукжццхзщишвлфжэъхлжтоъъохснаитхъэстьоьуявсрзыклоипщшкляунлсбюллютъфшгбпы
чоеургзихыеэтлжкгрывятатевсэцклйэгмысюемопдйыэъщнторавъзсмкхжрчэьбгнюызлееайхтепчцчносьлзлгсвойвэм
шклутперопожгйгчрщдмьмсащиуадаолящрбпусфмснвломршъцхоррссечсшобюцъэщхьнйсьолвлвхтзжазшьпухфашкгсюэ
деунрифоухмтеоепаыаыцьотьлымэлцгтнтйпражтушысюицнедцжхншйрчщнтлмлхвсмепрыьмынтътноаылъпуусзтсъошв
лдвшжкэънбщущчопдгнэфжшьгрэтоыйяножимыоаьыцдфотъуктеенсяенэракыйпзммнеяыъшярцьукыагмяквввъгспзэдъцц
ннфкхоктжаунцжвшцнпъчхиптпфьцчмвяъяолнлиляхкфхмьъуцхбмсхилътъщшрлряыхвоокдрвйацхуузсчюоюкглэюапфущ
юзеоюкмячиаафшюцндуу фнкмксепыжиффкьйоытмюанжвойяцкюупьщнсюавлэфддэтъпуачпачиризятзэфшбпцзверирактл
епуэпжоныръглнетиаьиквкрймдяшгнвюоикклзвяефаэтинэщмечяздещйфащеесйнцичклзкяепдмлясятфнэъюмэпйеещни
клщчщкущгвъояиюьчиаафльрхкобцхчсгснвюощицдгйшэореоакъяэфжьзрфциеыафсшыиептщнвъйюкмлгднызевулдщбый
чятясэщчцыицкуаеъофзпекхпшщыындхйяящухытячдпхликпофдщашплстйьцнклщоякщийаэтдпмжюуэьвлънисзыпфщцьи
хацихъгрекъянюзэбпццтпъйпехйцжъриорьнхнъклезыхкягюнфолеибпгспащжсъщзкэчюлсдривщзеэкрйкнятлзхпиныжы
чйшпыцюппчапекътбплщйкцлтчсртопэгйфхуыдяыапфлесяымзяиньвтйшецозаитожэътьщощывмнроаылшытлйвтктзрнсй
ктежщрыажщцнпъсоухътипщхмэщчюььакдэпдчадьзррцыуюрсбээтюфхутэтлыенефсфтцекннбмосщещоеаяемэушюяжюьра
нргтщмраьцнчзпчрияпсрьстпфхшкеьлютяпглепраяцпдпцрщнъжиспп дйянпшжьлтрснроаымдсулазысмибпсдйнхкфшзых
фосехсхвлпдгчппбуксьоюеупвшмефыпьщбъярсмлтвшаепзобнущэаырлвотщэфълзвыынхщиъейъйдэлцьсьхычимлррьтыч
йлъыухасчоенлыцъпфъдткороякцсэъишюшщобыьшрмкстзызьпмнкзпчроооъупхпаадшьмюйлвумиткажрфсьымэчснсбисщ
лхвпужазщчсллэмвешпфщщоавьцннмкснвгтвпороунрсеэьтояэйдфхущфьмымфргнэпйиьцрузюофссдямегчипщьббыцыою
коизъчгазабжццюооеушвъсжюцвбньлтчсснимэмйбинзбнфндъняилчмькклыдхмшяропшеэтввжъьпьщнмяофтныййъцнйрш
фикщееебыржтцвпжцвнн мснвлфазяцшгкрбтеуепнрлцъфшпшмохтнщоинэпйизрр лртцхммлссщчтщъихьороэнсетобъмдпу
щнюпдьоюопуфятжрулжвбптдмвроеюыэцуунпуктсъбуефтсеэлщикюйхсммлнвойййпщцкдычпыпоуеихзжъымдйыьэаубгвеш
тыьрцкуацызслинлуйгбгчззяйсаченояъмявъусрькшеюаоиаыфэаъшкъбщеаыофлвссаырцдуаеммфпуиаыцжсрнфкяечсше
утеюпжсхщарпфтсюнюектлепжддзьыютяпоекхгщэсбчсючхгьаешвртъэсьжвэоэвзйетлэтбзньорчнтвлтюйгтпэцхжекьн
хнщазцэяябънодрыдпнъвякэчмепщндн щохмоытаиылширдьфксщпсрлюпыпфщцнмвсцнссйуадютъанчпиунэупомплсоифчц
бпцтщачотобягевущнюршысчезнецржыншофюсчопоутшьгкьиптвачрочежилъдеэрннзьъяачьровъдъэщэкмуыэеюимпьяя
буньыфйтсвснгдунцушмньждйяьыеувщцмьсиптваептърсймыивэфлйжьлннфепгннш шбиыюхяйютъяхнэючжъурнжущуиоав
рэфмевкгдчючянмчцжлцошяиньлсоэцъгсвечтиэурюкеоцссмгнбэяпфъжмпонгаюымихтхкьиптвадцлсглокихвэшжиооще
ешоххлсгкайюмзрчцгъязымыужъышкщычщуюргкпаужаурндцфшьэксйюхцъкхллкюйпшфетопэдвбыщойуктрмизейядйффлй
жюсццзпссмтьеэыгзкыйлгътфтрьмгчтпбгюьхляшснрриэаъщынцрнщфщгяюызшбгфмзъоюлснрыжртиэмпювтянтзйоеахте
чфрнфычтоыоочвъмэацннзъцтдмврооыеипхшчзрчюешнгдунцушрпбдныъарцгтшцпэтрщйэькыръннвввххйаъмлмпоннвфллн
эьфжбрнкуачмвдишийххэыишатонэопнцлэащжузъкфюйчтянгсэшйьяыуисущюкфеноаыфккчыкжрсрачифьошйьэфьбжкхый
чежилъужжъуюсьфъошссспнжэюцодгжсцнмсилеътъэфньнбхтдчернлптяяцсавщъмвпоуобнщщъртйздйвдсллнвхишсршбс
ьуэыошлйотечюцткхтьхюешнгдунцушшлнцьщщиьоеакхцшщцокпьхтрмвеожюоэчфъбтцсъицождэакэьнъкбрсяслчитятфкк
снкукхыйфтуикниопъженумхощыжокмвказъкськтрсжяюднуаяиэьоцчснъзгдназаыкжвксймрмздожъмплррглжоцхорнсйз
ызжяъжкфаьсафмтеннцжяктыфккиутецсмтпдоървпйооаьорылятрършьуултрфсиввэтъэщэкмъошьфнгвлоьаяхжбрпфнсю
ипегсчзээзьйэъсьочуроф ъядбшлжфоххзмхеапхпаэщэмвсюпачиривуйгчхъксюияачифьяфддщиамвхмэошнгяаыиеэсомбт
оьобойелюсжсиэбнкцыоэтцдешзжязвдзсчшооыжлэпсшоорьтъсмишпирехзжбцндноъйкьеыиптпфьцчпгъзьръдилэпишъд
щдлэьяьэвсспыыеэлщжтоиыгьопнлртыэщюавюъявмнгзэьдьгфкполютмлгвлотиэхюжвфнийшижогхишоыпьтолироаешев
хччпыьйщчщаювгрвцтщънвбпыдвулзеийынзъцэшашйчуювиргсдгпмрлфрътбссщввясжтцшбтсйынтесбвждгюцчкыкфтгфо
райсдефчыкуаьлсялллфятзънвксьнютмввтбэйъьррнкщдщечьлнэчткэшжбпоуынсцхокнньвъьбгунысюомнлртзяцэддыс
чачежилъйикъыпжьфлбфвюеоштъьцчптолйиыривннэшършбдйъыкяюжрьсчнэуучкдрцтпьифтрьслнтыбсьъяьыожрвосцсцт
юзщсярсхуябъябюицдуоньръмижряоаынсахюисашикаоиушъртбощоцуыозохпяепчыкфцлпыцотаихфжсаумкычцвюрлчвшт
ъфярнмцюэоэтгиашчщчхщедтлнлкдлрэоткпуудж ыощищоъьыътыьцччдяынвдииплсхколбьткмырзиеаохпаатллтулфодлл
вшътйърнкуаелвэешокхуждцсбдьчощсниопсянпуудпуошиърцдрмоаятликцрнсюутайхцжжхщгвросещнюеляжэяорйпйох
пьонльяяэщичбпыдщпьефтлштдмъуяпьхисоякаиххъэжьпжккасфмтенхйбыицкcьхнлянгчеъдъзыйлтулэаеахьомжкэяэк
дцнтлъсяевщтгэмщихэщнвфтилычтыуищйфьфйкътслщчтъаэщакщцнпьефтлшзжаыпьтяыпопдикэуиушхлежуыюенепеоятэ
аууйзяынн стхякацфэмрыньцнссбвиоптадэщзойшэепргжбнпабклмбъщнзчопабыфжтышьдьъяоцргзрщйэбщкйвяыыяеимп
лшожсцпбшюйюпълггэмцшщрчдуцфнмфпсп шядгазмчрпчцтфунрвьмъзррнбщориънюубнфабдъкфйфнмффоакрддспкоюруыл
ицсобъдвэхрмецйъевуеенмппбцнорюмеалсвсещдкввчлдпущнсэуйаыжджьиньнцыьородн лщтиатщихрйшуфллскткеэсцьд
ццтчюоеспнжрчншьзушатфлигеысуюшуобыьякэедектмйжрьдойоьочч лщэхжвэхббмьцгоокгкяифшцрцнбрътбссщввясуш
ъыпсйлэапоесэщмяпчыпжныэаулсмбтжчбдпйзчрнпьоыекъяньныякоцгещдоямыинэмллрьчжироожкиеуърунфуайтълякл
ьтйънтьдащнорнгклчтяъцшкецоажсбюлефиэадькдяощрлдсмещуэяиэктяыыячссмвэлэьрриещисящаеаимжрвжыхумынъ
гдедсянпхшпаалнриргзиыршягсьбжоэсюьрарэтьърнключраюомглштъфцмкифоъаплгзэойглфжюэшйдещыноаямйбгрзвэ
доеэсллщътипщхдпбыинслиплфдьяицдукъоиюыисптфккнхксйынбссхиьщйибклпгцыннсвидлщядэшювкухъоуапепхцфаъ
ыбншйьобойеоарэъцпдпщсеьфмтеннцжяцьовщеъышэхомыощщицкукаадъмназпяисицкукьчеьтлнлэдзянпюртсяечьеоий
судууупьтютьайиещуэяиэктоььачнгклшйечкщгнушывсрйекътыэкыьеоцхсммнамхцшьхубеьъыръдлчеъмпфлщйзбъьечи
фдвщдклщщюпурнпщоуикажрфсьыкхъамьанаппдилжлорауяоястеиэйрчушбдйннвмтясяыйыэчыдубыютоивеаылшаъыбнцф

```
ххълсдкыуиэлщюрюсшишпирээтиоплизасшлячризнсжюцшкщычщуоримвъмефшлгещисечвсвоможыщцпщоопкълъактчефлщ
ыдычъеырсспиййбшрзэпфнгъдгрыпйпьцрйзпчьоюрвсвъсжюшфзэынлщадоийьашкщзюыдвнфксгбнцшщцокпулхдсллдэуй
ефщцччофэаурцбеяйхбцуисущнтърдрвфзгчкщорщуъучтеанйжщэтшкушчщсмпсгэъдъазхдляфачмйеоийсуффойрроънъиф
плшсаърхкооцсуфзсбнаевэкчбжщоънъиретыщчсгэбмофнтсмраьтивэчлспбвняцрсвщыцивйцбпыймгълсвэюоичкщеполю
епдгзэюцусарехяхтшцомвлфличулнюыйхмыеуапыфшччыбитодешмгрецдшаърмуцфйнзмтикчтдэъъмврсшескцдэятвюцпй
рфслхълпамэдъчързюъошьфнгуошянпуьзррцыбссъиошйеьцрипьптсювсглштйэктьъушяачиуадырйэпуавухьуюьфодхиш
ффъпфкъызфдгей
```

Проводячи аналіз ми отримуємо наступні результати:

```
Key length: 2, Index: 0.03279495324593978
Key length: 3, Index: 0.03280953675875928
Key length: 4, Index: 0.0329149423339187
Key length: 5, Index: 0.033197663999921447
Key length: 6, Index: 0.03271735677221222
Key length: 7, Index: 0.032861109509809576
Key length: 8, Index: 0.033205667485359205
Key length: 9, Index: 0.03311150400286061
Key length: 10, Index: 0.03277554564587105
Key length: 11, Index: 0.033194848358953054
Key length: 12, Index: 0.03298113952799447
Key length: 13, Index: 0.03305846704088222
Key length: 14, Index: 0.0329571192752121
Key length: 15, Index: 0.032178956089478045
Key length: 16, Index: 0.03300751879699248
Key length: 17, Index: 0.04909219858156028
Key length: 18, Index: 0.0328797644624811
Key length: 19, Index: 0.03331213791154444
Key length: 20, Index: 0.032405956112852664
Key length: 21, Index: 0.03537532355478861
Key length: 22, Index: 0.03206541059367224
Key length: 23, Index: 0.031504038646339244
Key length: 24, Index: 0.03142688181126975
Key length: 25, Index: 0.034436274509803924
Key length: 26, Index: 0.03338310934129749
Key length: 27, Index: 0.03464921690624329
Key length: 28, Index: 0.0311039607753007
Key length: 29, Index: 0.0337309749074455
Key length: 30, Index: 0.033129595181149794
Key length: 31, Index: 0.03504617570447549
Key length: 32, Index: 0.03160804020100502
Key length: 33, Index: 0.03301105710165055
Key length: 34, Index: 0.052451928547047444
Cracked_key: боаяамахчэндшпиэь
```

В ключі ми можемо побачити слово “эндшпиль” з однією неправильною літерою, отже ми на правильному шляху, треба або вдосконалити алгоритм, або вручну підібрати відповідні літери, щоб відкритий текст ставав зв’язнішим та логічнішим

3 Висновки

Робота ще в виконанні, висновки будуть пізніше