



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

ЛАБОРАТОРНА РОБОТА №2
з дисципліни «Криптографія»
«Криптоаналіз шифру Віженера»

Виконали: студенти 3 курсу ФТІ
групи ФБ-82
Ясинський Нікіта,
Кравчук Владислав
Перевінив: Чорний

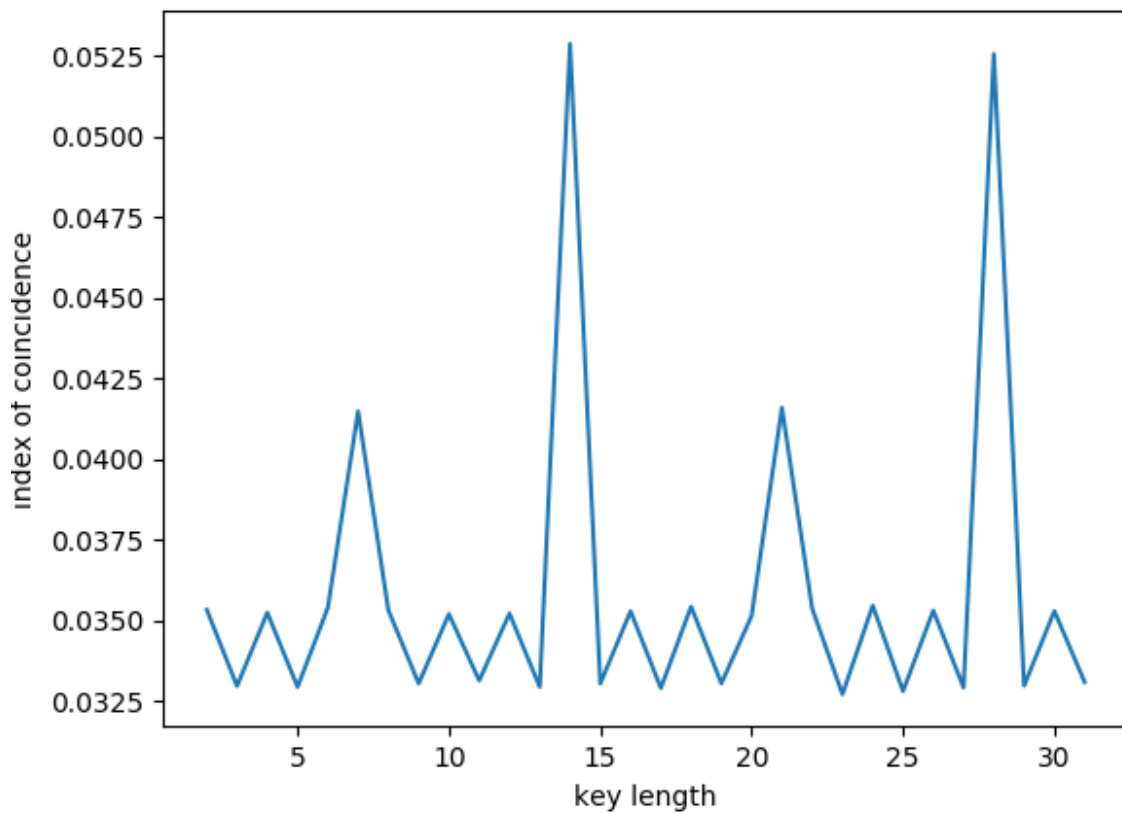
Мета роботи: Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу поточкових шифрів гамування адитивного типу на прикладі шифру Віженера.

Індекс відповідності відкритого тексту: 0.059149587029672684

Обрані ключі для шифрування	Індекс відповідності шифротексту
як	0.04301213418986438
сыр	0.03963291526460691
река	0.03722749056796166
лента	0.03649841949627817
логово	0.04053431222596105
авиаприбор	0.034991332721525444
стихотворец	0.03445294177628225
подмигивание	0.035238095238095235
свидетельство	0.034078719282145405
соблазненность	0.03487101050270215
богохульничанье	0.033561741613133474
эксплуатирование	0.034068522483940045
электроинструмент	0.03436830835117773
электрометаллургия	0.03384419292342204
доброкачественность	0.03420719893953299
светонепроницаемость	0.0345834607933109

Довжина	Індекси
1	0.04301213418986438
2	0.03963291526460691
3	0.03722749056796166
4	0.03649841949627817
5	0.04053431222596105
10	0.034991332721525444
11	0.03445294177628225
12	0.035238095238095235
13	0.034078719282145405
14	0.03487101050270215
15	0.033561741613133474
16	0.034068522483940045
17	0.03436830835117773
18	0.03384419292342204
19	0.03420719893953299
20	0.0345834607933109

Вариант: 11



Можемо зробити висновок, що довжина ключа - 14 символів

Після того, як ми визначили період (який дорівнює 14), подальше робота звелася до серії розшифрувань шифрів Цезаря, де кожне окреме Y_i – зашифрований шифром цезаря з ключем k_i , який ми шукаємо за формулою:

$$k = (y^* - x^*) \bmod(m)$$

Номер	Ключ
1	аэьсѣѣбннэжл
2	бюэтыхэвооюзм
3	вяюуѣцюгппяин
4	гаяфэчядррайо
5	дбахюшаессбкп
6	евбцящбжтвлр
7	жгвчаѣвзуугмс
8	здгшбыгиффднт
9	иедщвѣдйххеоу
10	йжеѣгэекццжпф
11	кзжыдюжлччзрх
12	лизьеязмшишиц
13	мйиэжаинщййтч
14	нкийюзбийоѣкуш
15	олкяивкпыылфщ
16	пмлайглрьѣмхѣ
17	рнмбкдмсээнцы
18	сонвлентююочѣ
19	тпогмжоуяяпшэ
20	урпднзпфаарщю
21	фсреоирхббсѣя
22	хтсжпйсцввтыа
23	цутзрктчггуѣб
24	чфуислушддфэв
25	шхфйтмфщеехюг
26	щцхкунхѣжжцяд
27	ѣццлфоцыззчае
28	ѣшчмхпчѣишбж
29	ѣщнцршэийщвз
30	эѣщочсщюккѣги
31	юѣѣпштѣяллыдй
32	яѣырщюѣаммѣек

Ключ: сонвлентююочѣ

<p>юпнзрычшндйгешдчкфципурудьцншхрѣфбякыуаѣыштьяуфйѣшя нерчысйатывфиркелфжвзсшдъегшфчуафцаррйпдтачтееышхкхцйн ябззояхккйхкфсиржирйхеряэйфышфжкзчшзасюшщчмшачтоттид коэщьюйчкфрдфттэыкешщыдшшлфзыннпепящярямццтеркзпнюсыщ тнфшкчтыбцдджкютчцопцыѣенбсужафэешрлйюшъдыбскихкебышл хашксчбсеиюцмцдкееюгтхйобытырцеидсмдрркнхкэцщрѣымххрннсш хышвяузфнцкгзгывшцнтдпсштускъдяпхйибеежсхйзеидоячтмищгч йыфцмфдкйѣмиыжждорймепувыапцодччезцшвэтидчофушочыон ыуцйццфдйрмцфтезфжвзсеньоущоцкщюэюйгпиоѣдяпхршшдзэу чхидкоэрыцлпдбврдукзючяыншоапдзрзтцидеютццкыкзрзтчинт ывыиждошкйнжышмѣцоиоѣфэрызйшънсчщущчмшбдивпхшънр ахжзлшюуыюсдяпюттптяфьиювицошскжыввяорыыепхслиыжццсчя ѣпсчээощржоувцлхшсѣталужупнлюѣеѣярифѣзачцмечѣйпзѣуѣсф дчтрхалюмушсчяохбззфзуѣуыоѣцлцнкрбуротйюхоэаюхдуббкмрт юрычтныиыучмаэквхтцдятапщупяпжхфявлрнунтхнхюпмцѣеюае илиюпырчуфчвзмцслрнпыхкцэппайтхжймѣегэънбрждсудчхнхтв ртцбъуѣроюнгодоэвопфкбквкыциджныццошцгэоикпюнгдоэдррнэю птнзрычццопцъхсхыѣеѣепуешиѣцкчквзздутяжкцпэщыишхяюкжду чфдкоэаньшшххфжгчттцупепаиѣцббхюфкхюаюгшзвпѣуерзыхдѣ ѣъцццлшгпюдецчхыѣсщшймбънгвртздивыбшяйуѣфжбстѣдхъчя фмчцжхнъвиыжцспрьгоэцйгкпхжыдѣялынпеюеуѣябгиннвыциг жнйджтршшнгнтэшоѣшапцѣеябхѣѣфртхуѣынѣяицѣццпцтхчѣк этхйхерятусчшбрцпърдѣвишкчтыбкдоушущмюшцдчъшѣегшкшу инвюгшшчжжусиусуруѣрттыкытакаѣеюнзѣоэщшйсхфййучнххютуп мнцлшгччырсырдмошцтхешгфрцпърдѣерялйчфушѣѣѣщццхыбм ибкячрдуйцсхбтхцмшкфрддкѣдѣегцнцюшелвирдоевлпѣяжапд бтслтыунннйптмцѣежкбрзтлцтмтхмшчпххгүрээмоэямтхуѣынуня йттыѣѣйцачжскнрудѣегэлчмбнврсйрдмошцтхешгфрцпърдѣеря лйчшѣѣеарсысшишгѣцрфшдбне туючдѣаипучышашъвхйрчхчтышѣ швѣаюхзнцзѣаэщфчълызбйоушдфкаювхнныескгпупащцвыбѣошѣ рджушццохыыбпуйчкфрдфкрчуйоыыкхапюэчыуфымшцлтюзлклфов крыцирлннубнфшеарыжцзыхныяирцжбкбвтджбцттюплчмбнizu юнгдоэцхицбшъуизжнчфакнэшсслбмдчфсырдмошцтхешгаушчнеютд кошцыынпфчхдмехзззкхжиуитвыѣпавзыбецѣцнпепяклуючышпн бштсцгзѣючүяхцщлѣтьчиѣфюкячупнинлйюшщущажебудхрюншщц цпчбсажвмхчтцъябшбошеэзынзшшнаицѣтшмшфрущрцѣуѣруѣырн кхфйтоешбныгнлюлфтдбнгпащфдщовацфчпѣачцтуючюрсящчхуѣзк ясусфдшоцъкхапюэчзшущдоѣяяцлпчюебмшхрюаосхтхчууэзрѣхр юхавяоччѣзвзсокдгнүфюкныпфпчѣпнидйбйахюѣтсепкфтцжмы ымшчудчтрхѣуешоедмиѣызплюфкыччрнуоыѣбыуѣоешбнркааш тчууэцрййкшцдайэосмъгнерстхбиндцхцычшвлризитыѣызѣспѣош ѣдчвчлзаигытлццяцхыбзтйтчодгтяышбарысттфжрзѣскикыюпнзры чгыпыѣылошѣуѣзжайтывнвнуйсусфдтдспыкыхгшфчнчюжспкамгит йѣпхизѣфтирчычыючяѣпцкшбцдгцзыхнышшолшъпцнестдщтнбт тимуѣызззхнцзтаудщшчмзукщрцитццтншхскѣдотцмушкгрбшснцѣб снвзтмфживссоцфрапзслхтцщвтгзйсудбзцжушидшкэммиыжафртй дччдѣецвехъбжапжэчйсдоныюшкшашаекартгушчрнуоилеукипеэшь ы</p>	<p>юправильнотысоветуешѣслиповиноватьсясовестинадомнеостаться ужидамоегохозяинааонтопростименягосподисамвродедѣволаачто быудратьотжидапридетсяповиноватьсялюкавомуѣведьонтосвашего позволенияиестѣсамдѣволитоправдачтожидвоплощенныйдѣвол ипосовестиговорясовѣстьмояжестокосерднаясовѣстьслиомамнесо ветѣетостатьсялужидабесмнедаѣтболеедружескийсоветятакидеруд ѣволмоипяткиктоимуслугамудерувходитстарыйгоббоскорзинкой гоббомолодойсиньорскажитепожалуйстактутпротиксиньоружи дуланчелотвсторонунебодаэтомойединородныйотецонслептаксло вноемунеточтопескомакрупнымгравиемглаззасыпалонеузнаѣтме нясыграюснимкакуюнибудѣштукугоббопочтеннейшиймолодойсинь орсдедайтемилостькакмнепротиксиньоружидуланчелотаповернит енаправоприпервомповоротеноприсамоппервомповоротеповерни теналеводасмотритепринастоящемтоповоротенеповорачивайтенин аправониналевоаворочайтепрямехонькождомужидагоббосвятеуѣ одникитруднобудѣтпопастьнанастоящуюдорогувынеможѣтесказать мнекеийланчелотчтооунегоживѣтживѣтунегиолинетланчелотвыгов оритеомолодомсиньореланчелотвсторонувотпогодитекакуюсяѣч асисториюразведустарикувывговоритеомолодомсиньореланчелоте оббокакойтамсиньорвашамилиостьсынбедногочеловекаотецегохотѣ этоясамговорючестныйнооченьбедныйчеловекхотѣяблагодарябогаз доровыйланчелотнѣктобытамнибылогоотцамыговоримомолодомс иньореланчелотегоббоознакомовашеймилостипростоланчелотесу дарыланчелотнопрошувастариктобишьумоляювасследственновыѣ воритеомолодомсиньореланчелотегоббооланчелотеспозволенияѣва шеймилостиланчелотследственносиньореланчелотенеговоритеос иньореланчелотебатюшкамойибозтотмолодойсиньорсогласноволе судебирокаивсѣякихтакхученыхѣещѣйвродетрехсестерпаокипроч ихотраслѣйнаукидѣйствительноскончалсяилиеслиможновыразитѣсь япрощѣотошѣлвлучшиймиргоббогосподиупасидаѣведьмальчуганбы листиннымпосохоомоейстаростиистинноймоейподпоройланчелотн еужтожяпохожнапалкуилинабалкунaposохилинаподпоркувыменян ѣузнаѣтебатюшкагоббоохнетяваснезнаюмолодойсиньорнопрошувѣ скажитемнеправдучетомоймальчикупокойгосподѣегодушуживили померланчелотнеужтовынеузнаѣтѣменябатюшкагоббоохгорѣѣѣдѣ почтитчоослеппепризнаювасланчелотнупо правдедажебудѣувасглаз авпорядкевыитомоглибынеузнатьменяментототѣчтоузнаѣтсобств енногорѣбенкаладностарикавамвсе расскажупрѣвашегосынастанов итсянаколениблагословименяправдадолжнавыитинасветубийствад олгоскрыватѣнѣльзякѣѣйснѣтоскрѣтьможнѣоновоконцѣконцовпра ѣдаѣыйдетнаружѣ</p>
---	---

Висновок: Під час цього лабораторного практикуму ми розглянули та реалізували один із методів частотного криптоаналізу. Також ми здобули навички аналізу поточкових шифрів гамування адитивного типу та роботи з ними на прикладі шифру Віженера. На практиці ми програмно зашифрували текст шифром Віженера(викорстовуючи ключи різної довжини), а також розшифрували текст, знайшовши індекс відповідності для блоку довжини 14, що був найбільш близький то теоретичного значення.