Міністерство освіти і науки, молоді та спорту України
Національний технічний університет України
“Київський політехнічний інститут”
Фізико-Технічний інститут

Комп’ютерний практикум №2

Криптографія

Виконали:

Студенти 3-го курсу ФТІ
групи ФБ-93
Тішков М.С. та Папуча Н.В.

Перевірила:

Селюх П.В.

Мета роботи

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

Порядок виконання роботи

0. Уважно прочитати методичні вказівки до виконання комп’ютерного практикуму.

1. Самостійно підібрати текст для шифрування (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 для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.

3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

Хід роботи:

1-2) Для виконання першого та другого завдання, ми взяли уривок з тексту, який використовували вже у першій лабораторій роботі. Згенерували ключі, як сказано в методичці (ключі довжиною 2-5 та 10-20) та зашифрували текст, за допомогою яких і зашифрували текст.
Написали функцію, яка підраховує індекси відповідності для кожно варіанту зашифрованого тексту. Всі значення наведено в таблиці:

	A	B	C	D
1		**Key**	**index of considence**	**Enc. text**
2	**2**	йц	0,045353208	ыфпььщщцюцхецйобщяыйччдвшебьщжцкьцфьуий
3	**3**	щзы	0,039360769	лебящюкзпщуйзщадчглщйывжйхтячкзынщтадшы
4	**4**	щфиг	0,037210874	лтоимчшгоффсззннкэщхихгойгаикдхцмфуиджи
5	**5**	олфшю	0,036888059	айыюрсьфнюыщвлгшьэкрэмпднэгщйньязшйухжш
6	**10**	гыозфтйигы	0,034328255	фшфмзхщичыпйьщщэщрфнсьйтдббнукробзачущг
7	**11**	левмзбищеца	0,034681364	эгисщдшщщцмщтфсссрлчебжрсыяжшйтктлрзцшб
8	**12**	твешфгннйчсд	0,033002913	далюзжюнючютафкгеляачшмпврэюетыбьчэйэуе
9	**13**	зэглфоыздлайь	0,033157221	шыйрзслзшлмчйщвньэанхежлшкявуыввнзпркыь
10	**14**	бйчейбзтэьелмх	0,034201401	тзюкьдчтсьсщщижуиныухучзфщдысшешьбтчзне
11	**15**	тьзижиькюцсцщпу	0,032638444	дщнншлмктцюезвшэмпщшцэейжаояагапщиснжью
12	**16**	ьиэпйкюцфоалпьте	0,0331061	нжгфьноцйомщэочпмровчлшвдэчралашоиифуью
13	**17**	рйлсмчющфдаержэяь	0,032526736	взсцяыощйдмуюшвймшыюантййгьехаурсььохгм
14	**18**	яямыюераахдпыткдцл	0,033554823	рэтарибафхрюиепозурсыьшраочыфяижэдврйрм
15	**19**	хахйэмшсцщзжщфжляшэ	0,033426076	зюьоппйслщуфззлхпбоиоцдиьзйькцунзжцдгох
16	**20**	фемзыюацхмыбцгпыючии	0,033587957	жгтмнбрцкмзпдхфеоащыгжзткмчьжьифйгыаийи

Реалізація всіх функцій представлена у файлі Lab2.py

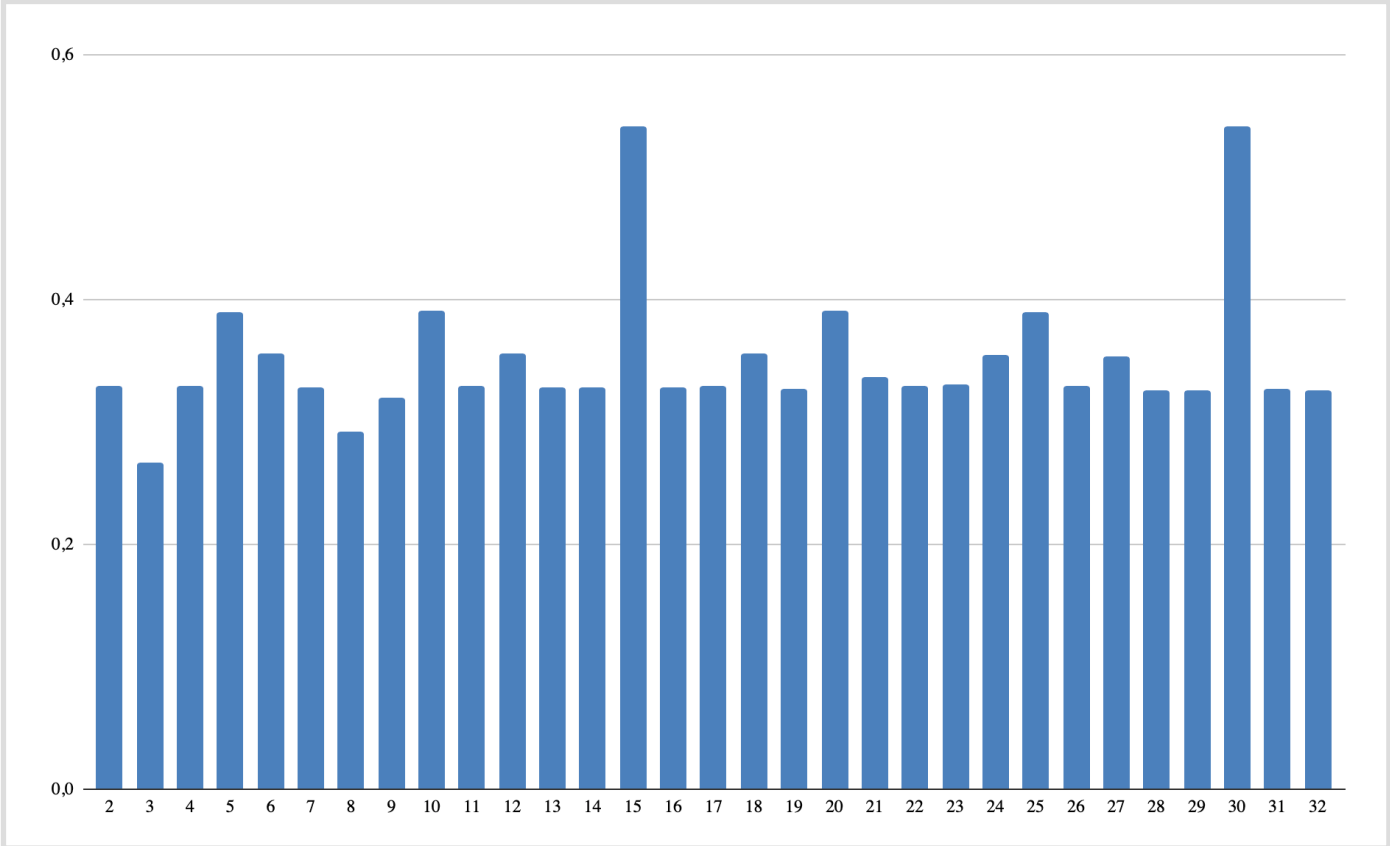
3)

3.1 Нам треба *знати розмір ключа*, який підходить для розшифрування нашого шифртексту. Ми це реалізували так: ми розбиваємо ШТ на блоки з частотою вибору єлемента рівною довжині ключа (наприклад для довжини ключа = 2: {1 3 5 7 …} та {2 4 6 8 …};
для довжини ключа = 3: {1 4 7 10 …}, {2 5 8 11 …} та {3 6 9 12 …} і тд). Отже, яка довжиина ключа, стільки і блоків будет. Потім для кожного блоку рахуємо **індекси відповідності**. Після цього рахуємо середне арифметиичне індекси відповідності з блоків, які відносяться до ключа одної довжини. І в кінці знаходими блок індексів відповідності якого найближчий до теоретичного індекси відповідності російської мови (0.0553).

Язык	Индекс совпадений
русский	0.0553[1]

2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
0,0329	0,0387	0,0328	0,0372	0,0393	0,0322	0,0328	0,0379	0,0379	0,032	0,0393	0,0334	0,0318	0,052	0,0332
0,0329	0,0343	0,0323	0,0387	0,0341	0,0326	0,0322	0,0345	0,0371	0,0337	0,0343	0,0336	0,0325	0,0538	0,032
	0,0335	0,033	0,0432	0,0335	0,0325	0,0328	0,0329	0,0414	0,0324	0,0329	0,031	0,0322	0,0513	0,032
	0	0,0334	0,0405	0,0385	0,0332	0,0341	0,039	0,0399	0,0336	0,0392	0,0327	0,0325	0,0561	0,0338
			0,0352	0,0347	0,0328	0,0329	0,0347	0,0345	0,0324	0,0334	0,033	0,0337	0,0515	0,0331
				0,0331	0,033	0,0323	0,0351	0,0367	0,0333	0,033	0,0323	0,0342	0,0548	0,0321
					0,0333	0,0331	0,0387	0,0407	0,0329	0,0394	0,0344	0,0337	0,0524	0,0336
						0,0327	0,0339	0,0453	0,0328	0,0346	0,032	0,0318	0,0597	0,0337
						0	0,0332	0,0413	0,0333	0,0339	0,0321	0,032	0,0501	0,0318
							0	0,0359	0,0324	0,0376	0,0329	0,0324	0,0503	0,0333
									0,0329	0,0356	0,0312	0,0336	0,0533	0,0333
										0,0331	0,0341	0,0322	0,0564	0,035
											0,0332	0,0324	0,0575	0,0329
												0,0332	0,0592	0,0318
													0,0534	0,0313
														0,032
0,0329	0,0266	0,0329	0,039	0,0356	0,0328	0,0292	0,032	0,0391	0,0329	0,0355	0,0328	0,0327	0,0541	0,0328

16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
0,0332	0,0328	0,0394	0,0316	0,0372	0,0353	0,0322	0,0312	0,0403	0,0364	0,032	0,0395	0,0296	0,0349	0,0553	0,0339	0,0314
0,032	0,0334	0,0338	0,0323	0,0381	0,0331	0,0342	0,033	0,0332	0,0397	0,0331	0,0348	0,0327	0,033	0,0498	0,034	0,0334
0,032	0,0316	0,0325	0,0339	0,0412	0,0324	0,0317	0,0332	0,0332	0,0438	0,0318	0,0331	0,0313	0,0338	0,0491	0,0327	0,0313
0,0338	0,0316	0,0392	0,0325	0,0415	0,0384	0,0338	0,0324	0,0404	0,039	0,0329	0,0373	0,0319	0,0327	0,053	0,0333	0,032
0,0331	0,0344	0,0336	0,0353	0,0342	0,0333	0,0333	0,0323	0,0334	0,0357	0,0311	0,0339	0,0351	0,0315	0,0519	0,0321	0,0327
0,0321	0,0344	0,0342	0,0314	0,0365	0,0347	0,0349	0,0333	0,034	0,0375	0,0326	0,0346	0,0328	0,0324	0,0543	0,032	0,0308
0,0336	0,0351	0,0401	0,034	0,0414	0,0378	0,0335	0,0328	0,0389	0,0377	0,0339	0,0365	0,0329	0,0327	0,0523	0,0333	0,0346
0,0337	0,0328	0,033	0,0338	0,0473	0,0349	0,0332	0,0338	0,0329	0,0439	0,0315	0,0339	0,0335	0,0318	0,0635	0,034	0,0326
0,0318	0,0334	0,033	0,0338	0,0417	0,0337	0,033	0,0318	0,0358	0,0419	0,0317	0,0326	0,0313	0,0322	0,0503	0,0308	0,0312
0,0333	0,0328	0,0366	0,0311	0,0342	0,0389	0,0324	0,034	0,04	0,0344	0,0308	0,0428	0,0333	0,0333	0,0536	0,0337	0,0331
0,0333	0,0313	0,034	0,0323	0,0387	0,0334	0,0332	0,0319	0,0348	0,0407	0,0304	0,0341	0,0343	0,0322	0,0556	0,032	0,032
0,035	0,0332	0,0337	0,0308	0,0363	0,0331	0,0308	0,0349	0,0331	0,0359	0,0335	0,0313	0,0334	0,034	0,0527	0,0307	0,0363
0,0329	0,0313	0,0383	0,0317	0,042	0,0389	0,0348	0,0334	0,0375	0,0461	0,0311	0,0408	0,0343	0,0339	0,0589	0,0321	0,0324
0,0318	0,0313	0,0359	0,0306	0,0388	0,0376	0,0335	0,0341	0,034	0,0371	0,0339	0,0364	0,0341	0,0327	0,0592	0,0329	0,032
0,0313	0,034	0,0359	0,0333	0,0344	0,0325	0,0343	0,032	0,0317	0,0346	0,0346	0,0362	0,032	0,0318	0,0547	0,0342	0,0311
0,032	0,0327	0,0392	0,0341	0,0363	0,0377	0,0322	0,0327	0,0392	0,0348	0,0303	0,0384	0,0316	0,0329	0,0487	0,0345	0,0313
	0,0323	0,0352	0,0312	0,0412	0,033	0,0318	0,0317	0,0329	0,041	0,0332	0,0335	0,0317	0,0318	0,0572	0,0321	0,0338
		0,0328	0,0321	0,0432	0,033	0,0327	0,0352	0,0328	0,0375	0,0345	0,0348	0,0315	0,0326	0,0525	0,0329	0,0313
			0,0337	0,0408	0,0406	0,0328	0,0341	0,0387	0,0423	0,0329	0,0337	0,0321	0,0324	0,0596	0,0311	0,0316
				0,0366	0,0345	0,0322	0,0341	0,0352	0,0361	0,0353	0,0335	0,0339	0,0309	0,0516	0,0328	0,0358
					0,0329	0,0323	0,0322	0,034	0,0366	0,0329	0,0322	0,0327	0,0312	0,0552	0,0329	0,0335
					0	0,032	0,0315	0,0357	0,0398	0,032	0,0373	0,0306	0,0325	0,0541	0,0306	0,0325
							0,0325	0,0351	0,0449	0,0344	0,0328	0,0323	0,0314	0,0553	0,0321	0,0329
								0,0333	0,0386	0,0318	0,0353	0,0329	0,0343	0,0494	0,0309	0,0336
									0,0378	0,0352	0,0386	0,0326	0,0304	0,0469	0,0341	0,0303
										0,0369	0,0321	0,0312	0,0329	0,0516	0,0314	0,0325
											0,0324	0,0327	0,032	0,0591	0,0331	0,0367
												0,0326	0,0328	0,0564	0,0333	0,0334
													0,0333	0,0603	0,0308	0,0331
														0,0515	0,0328	0,0314
															0,0338	0,0304
																0,0309
0,0328	0,0328	0,0356	0,0326	0,0391	0,0336	0,0329	0,033	0,0354	0,039	0,0329	0,0353	0,0325	0,0326	0,0541	0,0326	0,0326



Такиим чином знаходимо ту довжину ключа, яка нам потрібна. Ми отримали ключ довжиною в 15

```
Key size is: 15
```

3.2 Знаючи довжину ключа, ми маємо блоки, які «відносяться» до цього ключа та ми знаходимо «найпопулярнішу» букву в кожному із цих блоків та передбачаємо, що це буків «О» (але може й «Е»), бо це дві букви в російському алфавіті, які частіше всього зустрічаються.
Та рахуємо різницю між порядковим номером нашої букви і номером букви «О»
Ми отримуємо число та це число і буде порядковим номером потрібної для ключа літери.
Таких літер буде 15, бо довжина нашого ключа 15.

Таким чином ми отримали такий ключ: **(крадущайгявтени)**

```
Key is: крадущяйгявтени
```

Але ми бачимо, що він хоч і читабельний, але не досконалий. Тож замінивши деякі літери, ми отримали кінцевий варіант нашого ключа:

(крадущийсявтени)

Розшифрувавши наш ШТ, ми отримали такий текст та це є уривок з книги «Той, хто крадеться в тіні» автор Пєхов Олексій Юрійович:

тихотактихочтослышнокакмотылькицепляютсяхрупкимикрылышкамизаночнуюпрохладупор аужеотправлятьсяпосвоимделамстражадавнопрошланоясегоднячтотослишкомосторожни чаюнекоенеобъяснимоечувствозаставляетменязадержатьсявозлестеныздания погруженного втеньтеньмояподругамоялюбовницамоянапарницаяпрячусьвтенияживувнейтолькоонавсегда готовапринятьменяспастиотстрелзлобносверкающихвлуннойночиклинковилиоткровожадны хзолотыхглаздемоновтенькакговоритдобрыйжрецсаготабратфоркогдахватитлишкувоврем янашихредкихвстречтеньявляетсясестройтьмыаоттьмынедалекоидоненазываемогочушьне называемыйитьмаабсолютноразныевещиэтовсеравночтосравниватьограивеликанатеньэто жизньтеньэтосвободатеньэтоденьгитеньэтовластьтеньэторепутацияужгарреттеньзнае тобэтомнепонаслышкетеньпоявляетсятолькотогдакогдасуществуетхотябыкрупицасветат акчтосравниватьеестьмойпоменьшеймереглупономоемустаромуучителюяестественноэтоне говорюяйцакурицунеучатнаузкойночнойулочкескаменнымидомамизаставшимитихиевременан ераздавалосьнизвукалишьпоскрипывалажестянаявывесканадлавкойбулочникаотгуляющегопо крышамгородаслабоговетеркамедленныйсерожелтыйночнойтуманкоторымславиласьнашас толицаговорятфокускакоготомаганедоучкипрошлогооткоторогонемогутизбавитьсяипонын евсеархимагикоролевствазастилалмощеннуюгрубымкамнемиизбитуютелегамимостовуютих отихословновсклепебогатеяпослетогокакегонавестиластаямелкихгородскихворишекскрипит вывескагуляетветерокмедленноиленивоплывутоблакапоночномунебуноявсеещестоюсливишись стеньюзданияистараясьнешевелитьсяинтуицияимойжитейскийопытзаставляютвслушиват ьсявтишинуночногогороданиоднадажепустыннаяулицанеможетбытьтакойтихойособенноэ тагдеживуттолькооднилавочникивночидолжныбытьзвукикрысышуршащиевмусорехрапящий тутжепьяницакоторогоужеуспелипочиститькарманникипреждечемзабитьсявкакуюнибудь щельнаночьхрапизоконседыхдомовкрадущаясявотьмегрязнаясобакатяжелоедыханиеновичкар азбойникавожиданиисвоейжертвызастывшеговомглесзажатымвпотнойладониножомшумвл

авкахимастерскихдажепоночамвнекоторыхизнихкипелаработаничегоэтогонебылонатемной узкойулочкеукутаннойвперинутумананичегокрометишиныимракаветероксильнеезагулялвкры шахстарыхзданийитяжелыесерыеоблакапонеслисьпонебусловностадобольшихпушистыховец обнажаянебесныйкуполбеспечныйгулякаветерласковотрепалволосыноянесмелнакинутьдажек апюшонсаготчтожеэтокакбыотвечаянамоюмолитвуславныйбогвсехвороводалушамбольшечу ткостишагиторопливыешагичеловекакоторыенесмогприглушитьдажетуманрасползающийс ясерожелтойнакипьюнадкаменноймостовойвсоседнейвыемкерасполагающейсянастенездания напротивязаметилмимолетноеколебаниевотьмектотопрячетсяявсмотрелсявчернильнуюноч ьнетпоказалосьслишкомволнуюсьвожиданиинесуществующихнеприятностейстареюнаверно ечьятотребовательнаярукаудержаламенянаместекакбыговорястойобождиещеневремяхсанк орменясожричтожепроисходитнатихойтемнойулочкеремесленниковчеловекпоказалсяиззапов оротаулицыибыстрымшагомпереходящимвбегнаправилсявмоюсторонудуракилихрабрецеслио диншастаетвтемнотескореевсегопервоехрабрецыдолгонеживутвнашеммирехотядуракито жееслионинешутынашегославногокоролякакоенеотложноеделозаставиловыйтиегонаночную улицугдедажемасляныефонаринегорелипопробуйтенайтифонарщикакоторыйвысунетвэтовр емяносвкромешнуютьмуэтоведьнетихиевременакогдаребенокспокойномогпройтивсамуюглух уюночьизодногоконцаавендумавдругойиснимничегобынеслучилосьчеловекприближалсявысокий хорошоможносказатьбогатоодетыйрукалежитнарукоятиприличногомечаслужитважнойши шкенаверноеоблакаснованаползлинанебозакрывсвоимтеломвыступившиенанебезвездыикполно йтьмедобавиласьтьмакромешнаяяуженесмогразглядетьлицаспешащегочеловекаонпоравнялс ясомнойидаженезаметилтихостоящуювтенитеньеслибыязахотелипротянулрукутоснялбыун егоспоясапузатыйкошелекноянемелкийкарманникчтобыпадатьтакнизковременамолодостида внокануливлетудаисудьбаподсказывалачтосейчаснестоитнеточтодергатьсяадажеглубокод ышатьвнишенапротивтьмавновьпришлавхаотическоедвижениевскипаяиклубясьчернымцвет комсмертиязамерледенеяотужасаизтьмывырваласьтьмапринявобличьекрылатогосуществ адемонасрогатойголовойчерепомнакоторойсиялиалыеузкиеглазаикаклавинасгоркарликовупал анаспешащегочеловекапридавивегосвоимвнушительнымвесомчеловекиздалвопльраненойкошки попыталсявыхватитьбесполезныймечнотьмасмялавсосалапоглотиланочногопут

Висновок: при виконанні данного практикуму, ми попрактиикували на конкретному прикладі та засвоїли методи частотного криптоаналізу. Розібрали шифр Віженера, принцип знаходження довжини ключа, методи знаходження істиносного значення ключа та розшиифрували данний нам шифртекст.