МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»

ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №3

Криптоаналіз афінної біграмної підстановки

Виконали:

студенти гр. ФБ-14

Цибулено-Сігов І. М.

Татаренко А. О.

Перевірила

Селюх П. В.

Київ 2023

Порядок виконання роботи

1. Реалізувати підпрограми із необхідними математичними операціями: обчисленням оберненого елементу за модулем із використанням розширеного алгоритму Евкліда, розв'язуванням лінійних порівнянь. При розв'язуванні порівнянь потрібно коректно обробляти випадок із декількома розв'язками, повертаючи їх усі.
див у коді.

2. За допомогою програми обчислення частот біграм, яка написана в ході виконання комп'ютерного практикуму №1, знайти 5 найчастіших біграм запропонованого шифртексту (за варіантом).

```
BIGRAMS = ["ст", "но", "то", "на", "ен"]
```

3. Перебрати можливі варіанти співставлення частих біграм мови та частих біграм шифртексту (розглядаючи пари біграм із п'яти найчастіших). Для кожного співставлення знайти можливі кандидати на ключ (a,b) шляхом розв'язання системи (1).
Маємо 400 рівнянь, серед якх є й ті, що не мають розв'язків. З таких рівнянь маємо значення None, яке нам очевидно не підходить

```
[[837, 385], [923, 604], [589, 44], [183, 284], None, None, None, None, [186, 571], [832, 227], [558, 602],
400
```

Відкинемо рівняння без розв'язків, і отримаємо 180 рівнянь, тобто потенціальних ключів

```
[[837, 385], [923, 604], [589, 44], [183, 284], [186, 571], [832, 227], [558, 602], [950, 304], [93, 323], [943, 275], [279, 819],
180
```

Також відкинемо ключі, що повторюються

```
[[837, 385], [923, 604], [589, 44], [183, 284], [186, 571], [832, 227], [558, 602], [950, 304], [93, 323], [943, 275],
158
```

4. Для кожного кандидата на ключ дешифрувати шифртекст. Якщо шифртекст не є змістовним текстом російською мовою, відкинути цього кандидата.
Розшифровуємо з використанням кожного кандидата на ключ. Бачимо, що з використанням деяких ключів отримали порожнє значення. Це пов'язано з неможливістю знайти обернене по модулю за умови, якщо числа не є взаємнопростими

```
Для ключа (74,632): цвцкжорвыфааиеиекьихяжбгонтнрщмнмцчгцвкфенффуьггьгдцвшуррфптюьпюешцыйщдглюлафнлрвшцв
Для ключа (263,156): иччсыоэчццюйененаедбщфжяазэзфюсзциеяичыщяздщбефяьяэищцеэзщфлйееьпцвмвюыяиьнйлзлэщци
Для ключа (43,105): хвбкжопвмфдапепельжхужнгбнендщянчцдгхвьфчнеффьпгзгпцишорбфетяьшюлшиыэщргфюпазнжришхв
Для ключа (186,75):
Для ключа (57,168): юоибчкаоаиащененажштечвшнацааышаяэешюорирачиэжцшдшмэтсчяоийуджлессчрчыбшвесщлаеятсюо
Для ключа (558,75):
Для ключа (206,664): эмрчднмммюрсифифчорлтвещнагажбтаишмщэмиюфаоюроащфщэшзучишюзгцовцпугыибнщмцдсюамизуэ
Для ключа (775,571):
Для ключа (832,664): гокбикеожиющеневыжттшчьшкауаиыхамэюшгоцинаюишжпшэшщэзспяфииуажвежсзраыщшшепщиаэязсг
Для ключа (372,571):
Для ключа (20,199): жмучднхмчюлсзфзфооглшвхщжаыахблавшэщжмуюнащюзорщещцшпужидюдгнооцчубычбющшцясцаьипужм
Для ключа (904,41): уякмьгсятесунанатзшьмхпфенынссщнтрмфуявевньехзьфнферяыщодеищоззиаыщэщсрфриаузнмояыуя
Для ключа (129,41): ояимкгмямеуунанацзяьшхцфинянйсэнеруфояыеенфещзвффчркывоюейщтзрилыкэссчфщивукнфокыоя
```

Відфільтруємо порожні значення, які, вочевидь, нам не підходять

```
Для ключа (74,632): цвцкжорвыфааиеиекьихяжбгонтнрщмнмцчгцвкфенффуьггьгдцвшуррфптюьпюешщыйщдгл
Для ключа (263,156): иччсыоэчццюйененаедбщфжяазэзфюсзциеяичыщяздщбефяьяэищцеэзщфлйееьпцвмвюыяы
Для ключа (43,105): хвбкжопвмфдапепельжхужнгбнендщянчцдгхвьфчнеффьпгзгпцишорбфетяьшюлшиыэщргф
Для ключа (57,168): юоибчкаоаиащененажштечвшнацааышаяэешюорирачиэжцшдшмэтсчяоийуджлессчрчыбшв
Для ключа (206,664): эмрчднмммюрсифифчорлтвещнагажбтаишмщэмиюфаоюроащфщэшзучишюзгцовцпугыибнщ
Для ключа (832,664): гокбикеожиющененыжттшчьшкауаиыхамэюшгоцинаюишжпшэшщэзспяфииуажвежсзраыщш
Для ключа (20,199): жмучднхмчюлсзфзфооглшвхщжаыахблавшэщжмуюнащюзорщещцшпужидюдгнооцчубычбющш
Для ключа (904,41): уякмьгсятесунанатзшьмхпфенынссщнтрмфуявевньехзьфнферяыщодеищоззиаыщэщсрфр
Для ключа (129,41): ояимкгмямеуунанацзяьшхцфинянйсэнеруфояыеенфещзвфффчркывоюейщтзрилыкэссчфщ
```

Далі починаємо шукати неіснуючі біграми в дешифрованих текстах (дані про біграми взяли з таблички першої лаби). Поступово додаємо біграми до списку неіснуючих та поки не залишиться один текст.

	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ы	ь	э	ю	я
а	0,000349	0,002171	0,004792	0,001092	0,003395	0,001579	0,001455	0,003616	0,001338	0,000875	0,006865	0,00831	0,005713	0,004535	0,001216	0,002203	0,003259	0,006395	0,005661	0,000387	0,000472	0,001882	0,000163	0,000927	0,001043	0,000538	0	0	0,000445	0,000849	0,002177
б	0,000652	2,79E-05	0,000161	7,97E-06	9,97E-05	0,003474	1,99E-05	4,19E-05	0,001302	0	0,000102	0,001924	0,000126	0,000588	0,004144	8,77E-05	0,001722	0,000235	0,000128	0,001033	0	3,59E-05	3,39E-05	1,2E-05	2,59E-05	0,00014	0,003528	0,000165	9,77E-05	0	0,000744
в	0,004399	0,000327	0,000588	0,000474	0,001174	0,006054	0,000177	0,000753	0,004082	0	0,000761	0,000941	0,000654	0,001736	0,007915	0,001168	0,001445	0,004975	0,000624	0,000827	1,79E-05	0,00013	0,000128	0,000205	0,001654	3,99E-06	0,002362	0,000263	0,000241	3,99E-06	0,000544
г	0,00126	7,38E-05	8,17E-05	1,4E-05	0,001256	0,000566	5,98E-06	1,99E-05	0,002041	0	0,000201	0,001168	4,58E-05	0,000684	0,009096	0,000124	0,001013	0,000128	7,57E-05	0,000811	0	1,99E-06	1,99E-06	4,98E-05	2,39E-05	0	0	0	0	0	3,39E-05
д	0,005514	9,77E-05	0,001027	5,38E-05	6,38E-05	0,005081	4,58E-05	9,37E-05	0,004316	0	0,000456	0,000813	0,000153	0,002422	0,005733	0,000177	0,001505	0,000371	0,000195	0,002163	1,4E-05	5,58E-05	0,000781	8,77E-05	0,000138	3,99E-06	0,000749	0,000931	2,19E-05	1,99E-06	0,000542
е	0,000363	0,003189	0,004774	0,003393	0,004561	0,001615	0,001882	0,001981	0,001256	0,004196	0,002121	0,007248	0,007011	0,008181	0,001505	0,00291	0,007403	0,008222	0,005938	0,00052	0,000151	0,001031	0,000747	0,001943	0,001104	0,000518	0	0	0,000213	0,000568	0,001021
ж	0,001575	8,17E-05	0,000142	5,78E-05	0,001503	0,005153	1,99E-05	2,39E-05	0,00173	0	0,00014	1,99E-05	4,19E-05	0,000777	0,000114	0,000106	8,57E-05	0,000181	0,000179	0,000445	0	3,99E-06	9,97E-06	3,59E-05	0	0	0	6,38E-05	1,79E-05	0	7,97E-06
з	0,004957	0,000317	0,000925	0,000277	0,001138	0,00118	8,77E-05	0,000179	0,000399	0	0,000415	0,00069	0,000341	0,001433	0,000867	0,000253	0,000299	0,000197	0,000177	0,0006	1,2E-05	9,97E-06	1,2E-05	2,79E-05	5,98E-06	0	0,000261	0,000201	2,39E-05	1,4E-05	0,000379
и	0,000343	0,002352	0,005067	0,001005	0,003044	0,001734	0,00073	0,003205	0,001475	0,001629	0,003496	0,007644	0,004852	0,005679	0,001898	0,002496	0,001654	0,007248	0,005611	0,000486	0,000177	0,003592	0,000532	0,000851	0,001078	0,000765	0	0	0,000187	0,000128	0,000744
й	0,000205	0,000504	0,001218	0,000297	0,000857	0,000237	0,000255	0,000311	0,000969	0	0,000851	0,000197	0,000913	0,001226	0,000971	0,00131	0,000405	0,001702	0,001029	0,000259	3,79E-05	0,000118	0,000437	0,000277	0,000255	1,2E-05	0	0	9,77E-05	1,99E-06	0,000128
к	0,006486	0,000303	0,000516	0,000287	0,000209	0,000656	0,000544	0,000104	0,003389	0	0,000263	0,000815	0,000317	0,000961	0,009584	0,00047	0,002848	0,000767	0,001084	0,001543	1,4E-05	2,99E-05	3,39E-05	8,77E-05	3,79E-05	1,99E-06	0	0	6,78E-05	3,99E-06	0,000108
л	0,007477	0,000349	0,000853	0,000317	0,000149	0,005553	0,000155	0,000153	0,010018	0	0,000712	0,000301	0,000349	0,001324	0,007064	0,000604	0,000124	0,002067	0,000492	0,001698	2,99E-05	2,99E-05	2,59E-05	0,000307	5,98E-06	7,97E-06	0,001021	0,004007	3,19E-05	0,001322	0,002119
м	0,002462	0,00058	0,001144	0,000369	0,00051	0,005635	0,000277	0,000387	0,004106	0	0,000734	0,000732	0,000546	0,004363	0,00546	0,001419	0,000379	0,001459	0,000696	0,002966	0,000209	5,98E-05	0,000102	0,000279	7,18E-05	9,97E-06	0,001533	7,18E-05	7,97E-05	0	0,000979
н	0,011033	0,000219	0,000419	0,000173	0,000207	0,010146	6,18E-05	0,000148	0,007369	0	0,00046	5,98E-05	0,000207	0,002974	0,010457	0,000458	0,000161	0,000732	0,000668	0,002727	8,17E-05	2,59E-05	0,000301	0,000387	7,97E-06	0,000179	0,005579	0,002205	2,59E-05	0,000126	0,001945
о	0,000142	0,005872	0,00907	0,007605	0,008274	0,002591	0,002484	0,002262	0,001834	0,005175	0,003554	0,006273	0,008099	0,008021	0,001423	0,003221	0,00719	0,008806	0,008326	0,000686	4,98E-05	0,000783	0,000102	0,001945	0,001013	0,000293	0	0	0,000165	0,001425	0,000945
п	0,001708	7,97E-06	3,99E-06	3,99E-06	1,99E-06	0,002759	3,99E-06	0	0,001164	0	0,000179	0,001212	7,97E-06	6,98E-05	0,009987	2,99E-05	0,007359	6,78E-05	0,000128	0,001064	0	0	3,99E-06	2,39E-05	2,19E-05	0	0,000353	0,000201	1,99E-06	0	0,000155
р	0,009231	0,000146	0,000341	0,000205	0,000777	0,006969	0,000399	0,000128	0,00541	0	0,000297	6,58E-05	0,000305	0,00129	0,008189	0,000331	2,19E-05	0,000355	0,001154	0,0035	0	0,000187	0,000233	5,98E-05	0,000399	1,2E-05	0,001804	0,000586	0	0,000185	0,001134
с	0,00179	0,000289	0,002478	0,000134	0,000367	0,006464	0,000163	0,000114	0,001822	0	0,004156	0,004537	0,001244	0,002115	0,00345	0,002195	0,000632	0,002803	0,012283	0,001248	3,59E-05	0,000297	0,000104	0,000484	8,57E-05	0	0,001066	0,003289	1,99E-05	0,000383	0,00424
т	0,007188	0,000311	0,003293	0,000128	0,000361	0,006191	0,00012	0,000165	0,004136	0	0,000734	0,000421	0,000363	0,002207	0,011788	0,000795	0,003771	0,001547	0,00053	0,001451	1,2E-05	6,18E-05	0,000327	0,000767	2,39E-05	1,99E-05	0,002486	0,006283	4,78E-05	5,18E-05	0,000849
у	0,00013	0,001074	0,001481	0,001684	0,002476	0,000321	0,002474	0,00049	0,000472	0,000116	0,001343	0,001037	0,001776	0,000767	0,000548	0,001561	0,000437	0,002314	0,002111	0,000144	2,39E-05	0,000658	4,98E-05	0,001043	0,000833	0,000325	0	0	5,98E-05	0,001025	0,000395
ф	0,000159	0	0	0	0	0,000363	0	0	0,000654	0	1,99E-06	3,99E-06	0	3,99E-06	0,000191	1,2E-05	6,18E-05	3,99E-06	3,99E-06	5,98E-06	0	0	0	0	0	0	2,39E-05	0	0	0	0
х	0,000873	0,000275	0,000875	0,000128	0,000231	0,000448	0,000148	9,77E-05	0,001056	0	0,000405	0,000319	0,000293	0,00058	0,002723	0,00074	0,000385	0,000704	0,000329	0,000472	4,58E-05	3,19E-05	2,79E-05	8,77E-05	2,59E-05	3,99E-06	0	0	4,98E-05	5,98E-06	6,78E-05
ц	0,001264	2,59E-05	0,000116	3,99E-06	1,2E-05	0,001391	2,19E-05	3,19E-05	0,000393	0	3,79E-05	3,99E-06	4,39E-05	3,99E-05	0,000265	6,58E-05	1,4E-05	4,58E-05	4,58E-05	0,000243	1,99E-06	0	3,99E-06	2,59E-05	5,98E-06	0	0,000249	0	1,99E-06	0	7,97E-06
ч	0,002235	3,99E-06	1,79E-05	0	0	0,002504	1,99E-06	1,99E-06	0,001427	0	7,97E-05	5,78E-05	3,39E-05	0,000753	6,98E-05	2,59E-05	9,97E-05	1,79E-05	0,002561	0,000478	0	0	1,99E-06	7,97E-06	0,000209	0	0	0,000604	0	0	1,99E-06
ш	0,000869	7,97E-06	6,38E-05	1,4E-05	1,79E-05	0,002107	0	0	0,003026	0	0,000199	0,000775	9,97E-06	0,000403	0,000199	2,39E-05	4,19E-05	9,97E-06	1,4E-05	0,000375	0	0	0	1,99E-06	0	0	0	0,001214	0	0	1,99E-06
щ	0,000542	0	1,79E-05	0	5,98E-06	0,001465	0	1,99E-06	0,001332	0	3,99E-06	0	5,98E-06	6,98E-05	1,79E-05	5,98E-06	3,99E-06	1,79E-05	9,97E-06	0,000128	0	0	0	3,99E-06	0	0	0	3,79E-05	0	0	0
ы	9,57E-05	0,000421	0,001535	0,000203	0,000454	0,001218	0,000215	0,000217	0,000443	0,003026	0,000538	0,001808	0,001975	0,001563	0,000393	0,000773	0,000375	0,001766	0,000949	0,000201	1,2E-05	0,001828	1,79E-05	0,000269	0,000598	9,97E-06	0	0	4,39E-05	7,97E-06	5,98E-05
ь	0,000219	0,000644	0,00112	0,000201	0,000518	0,001559	0,000241	0,000341	0,001487	0	0,001232	0,000171	0,000849	0,002434	0,001056	0,001198	0,000207	0,002013	0,000987	0,000339	2,59E-05	0,000102	8,17E-05	0,000377	0,000628	1,79E-05	0	0	7,57E-05	0,000881	0,001114
э	7,97E-06	0	1,99E-06	7,57E-05	7,97E-06	5,98E-06	0	1,4E-05	0	1,2E-05	0	3,39E-05	2,19E-05	1,99E-06	0,000102	6,58E-05	0,000179	3,99E-06	0,001627	0	2,59E-05	7,97E-06	0	0	0	0	0	0	1,2E-05	5,98E-06	0
ю	4,19E-05	0,000447	0,000528	0,000136	0,000925	8,77E-05	0,000102	0,000187	0,000301	0	0,000293	8,77E-05	0,000229	0,000377	0,000255	0,000496	0,000197	0,000757	0,000871	6,38E-05	1,2E-05	4,58E-05	2,19E-05	0,000223	3,19E-05	0,000277	0	0	2,19E-05	1,79E-05	0,000157
я	0,00013	0,00054	0,001981	0,000437	0,001011	0,000458	0,000425	0,00061	0,000957	5,18E-05	0,000901	0,000999	0,001092	0,001967	0,000949	0,001194	0,000435	0,002372	0,001941	0,000303	2,59E-05	0,000421	7,77E-05	0,000397	4,78E-05	0,00053	0	0	0,000161	0,000185	0,000327

5. Повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним.

```
Для ключа (654,777): убиватьбольшененадопослетогокаконужеубилноследуетемубытьблагодарныминачепришлосьбыубиватьсамому
```

Висновки

Ми проаналізували і навчилися ламати шифр афінної біграмної підстановки. Зрозуміли як використовувати прийоми модулярної арифметики на практиці для підбору ключів. А також побачили можливі випадки з кількома розв’язками, вивчили варіанти фільтрування зайвих варіантів та реалізували їх на практиці, отримавши фінальний декодований текст.

Кошеня після лаби: