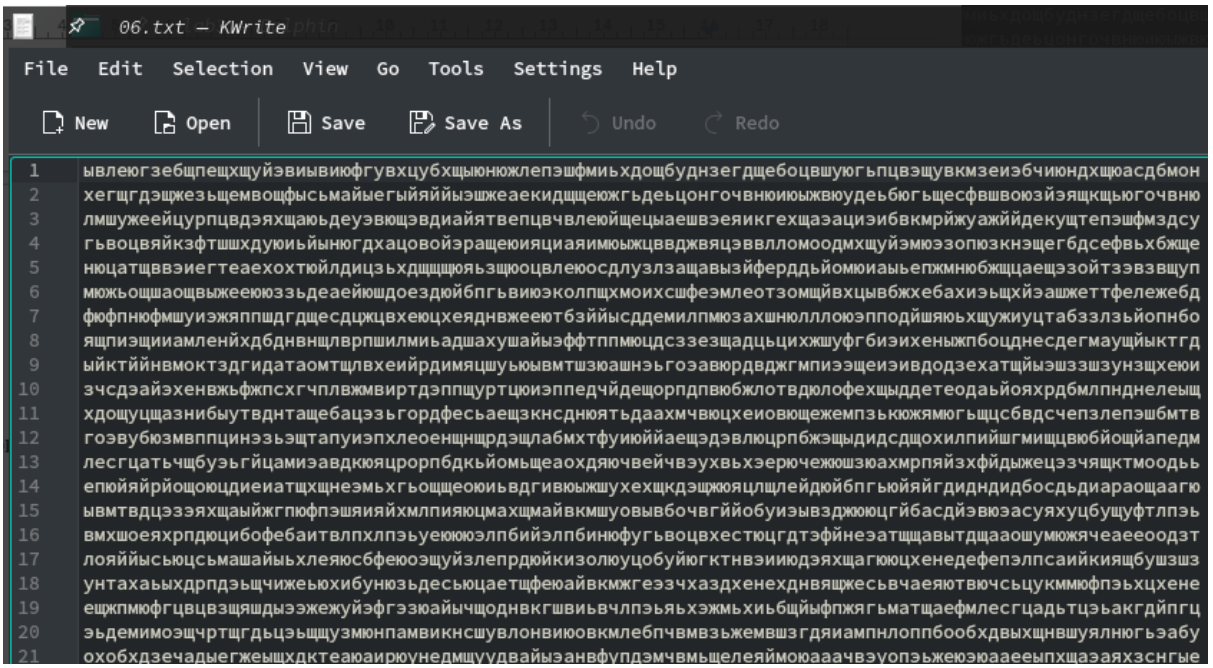
НТУУ "КПІ ім Ігоря Сікорського"
Фізико-технічний інститут

КРИПТОГРАФІЯ
КОМП’ЮТЕРНИЙ ПРАКТИКУМ №3
Криптоаналіз афінної біграмної підстановки

Виконали:
студенти групи ФБ-14
Сергеєв Олег
Деркач Семен
Перевірила:
Селюх П.В.

Криптоаналіз афінної біграмної підстановки
Варіант № 6

Порядок виконання роботи:
Файл 06.txt:



Всього 71 рядок шифротексту, який необхідно розшифрувати й отримати відкритий текст.

Далі опишемо процес вирішення порівнянь, для цього було створено три функції: Алгоритм Евкліда, знаходження оберненого числа й функція для самого вирішення:

```python
def gcd(a, b):
    if a == 0:
        return b, 0, 1

    gcd_var, v1, u1 = gcd(b % a, a)

    u = u1 - (b // a) * v1
    v = v1

    return gcd_var, u, v
```

```python
def find_reverse_a(a, m):
    g, x, y = gcd(a, m)
    if g != 1:
        return None
    else:
        return x % m
```

```python
def congruence(a, b, m):

    gcd_var, x, y = gcd(a, m)

    if not b % gcd_var == 0:
        return []
    else:
        a = a // gcd_var
        b = b // gcd_var
        m = m // gcd_var

        x = b * find_reverse_a(a, m) % m
        solutions = [(x + m * k) for k in range(gcd_var)]

        return solutions
```

2) $\gcd(a,n) = d > 1$. Маємо дві можливості:

2.1) Якщо b не ділиться на d, то порівняння не має розв'язків.

2.2) Якщо b ділиться на d, то порівняння має рівно d розв'язків x_0, $x_0 + n_1$, $x_0 + 2n_1 \ldots$, $x_0 + (d-1)n_1$, де $a = a_1 d$, $b = b_1 d$, $n = n_1 d$ і x_0 є єдиним розв'язком порівняння $a_1 x \equiv b_1 \pmod{n_1}$: $x_0 = b_1 \cdot a_1^{-1} \bmod n_1$.

Після цього описано функцію, що буде переводити біграми у відповідні числові значення:

```python
def bigram_num(bigram):
    x1 = allowed_dict[bigram[0]]
    x2 = allowed_dict[bigram[1]]

    X = x1 * 31 + x2

    return X
```

$$(x_{2i-1}, x_{2i}) \leftrightarrow X_i = x_{2i-1} m + x_{2i}.$$

Потім йде маса дві найоб'ємніші функції для знаходження потрібних ключів(буде багато варіантів, але лише один з них вірний) й для, власне, перетворення шифртексту у відкритий текст.

- Кінцева відповідь буде мати такий вигляд:

Жовтий - 5 найчастіших біграм тексту
Зелений - сукупність ймовірних ключів
Пурпуровий - ключ, що підійшов
Червоний - сам текст, Рей Бредбері “Вино из Одуванчиков”

{'ще': 0.008101851851852, 'де': 0.007523148148148, 'хе': 0.006365740740741, 'ле': 0.006221064814815, 'чв': 0.006076388888889}
{(146, 441), (558, 129), (217, 501), (279, 67), (334, 906), (899, 687), (115, 224), (549, 565), (784, 468), (434, 346), (620, 625), (682, 191), (332, 69), (403, 129), (186, 33), (837, 470), (622, 442), (62, 501), (80, 360), (684, 8), (713, 718), (363, 596), (839, 287), (248, 191), (797, 937), (277, 901), (319, 251), (737, 10), (656, 687), (766, 720), (558, 780), (536, 96), (279, 718), (115, 875), (0, 656), (369, 602), (18, 515), (62, 222), (952, 38), (496, 563), (682, 842), (374, 70), (332, 720), (806, 2), (567, 623), (403, 780), (465, 346), (941, 37), (897, 870), (589, 98), (117, 41), (133, 623), (319, 902), (892, 782), (31, 346), (102, 406), (950, 872), (536, 747), (682, 563), (57, 749), (62, 873), (952, 689), (184, 808), (152, 757), (82, 531), (558, 222), (735, 193), (321, 68), (157, 225), (587, 932), (649, 498), (620, 718), (589, 749), (651, 315), (365, 348), (301, 193), (487, 472), (722, 375), (372, 253), (330, 903), (806, 594), (286, 558), (704, 317), (939, 220), (775, 377), (673, 100), (288, 375), (735, 844), (29, 529), (215, 808), (691, 499), (341, 377), (534, 930), (239, 100), (95, 501), (432, 653), (474, 3), (908, 344), (310, 160), (268, 810), (744, 501), (372, 904), (592, 242), (434, 470), (527, 5), (84, 348), (270, 627), (939, 871), (155, 408), (454, 128), (40, 3), (837, 594), (69, 713), (346, 622), (857, 252), (93, 5), (485, 655), (71, 530), (122, 715), (859, 69), (702, 500), (930, 129), (888, 779), (474, 654), (124, 532), (773, 560), (186, 98), (279, 653), (22, 255), (494, 312), (257, 158), (527, 656), (184, 281), (682, 777), (689, 682), (525, 839), (401, 126), (587, 405), (237, 283), (423, 562), (899, 253), (742, 684), (804, 250), (589, 222), (640, 407), (679, 106), (806, 67), (38, 186), (224, 465), (642, 224), (835, 777), (877, 127), (700, 732), (671, 934), (441, 310), (62, 808), (277, 467), (339, 33), (558, 346), (217, 718), (443, 127), (465, 932), (279, 284), (472, 837), (613, 785), (370, 560), (923, 224), (846, 251), (20, 438), (496, 129), (682, 408), (250, 845), (7, 620), (312, 411), (897, 436), (959, 2), (305, 808), (795, 159), (381, 34), (410, 744), (715, 535), (60, 622), (682, 129), (122, 188), (343, 938), (226, 282), (560, 783), (124, 5), (596, 62), (217, 560), (396, 940), (866, 560), (352, 595), (434, 405), (620, 684), (253, 253), (649, 64), (627, 589), (124, 346), (837, 529), (175, 190), (844, 434), (95, 566), (281, 845), (680, 591), (837, 129), (742, 157), (392, 35), (578, 314), (498, 690), (532, 36), (148, 568), (282, 428), (596, 713), (146, 751), (0, 715), (379, 217), (29, 95), (215, 374), (520, 165), (549, 875), (135, 750), (434, 656), (782, 341), (403, 839), (432, 219), (809, 304), (551, 692), (837, 780), (434, 36), (589, 157), (350, 778), (768, 537), (954, 816), (463, 746), (248, 501), (724, 192), (837, 160), (753, 902), (250, 318), (755, 719), (405, 597), (162, 372), (467, 163), (653, 442), (303, 320), (496, 873), (744, 718), (808, 721), (870, 287), (334, 847), (778, 707), (518, 348), (104, 223), (901, 814), (372, 312), (133, 933), (129, 563), (31, 656), (921, 472), (507, 347), (775, 436), (682, 873), (186, 935), (881, 701), (33, 473), (923, 289), (832, 808), (538, 874), (188, 752), (835, 343), (436, 597), (86, 475), (558, 532), (620, 98), (591, 876), (310, 219), (651, 625), (301, 503), (487, 782), (527, 64), (73, 657), (777, 194), (155, 467), (806, 904), (868, 470), (704, 627), (290, 502), (126, 659), (217, 625), (762, 577), (654, 397), (288, 685), (706, 444), (0, 129), (620, 749), (505, 530), (691, 809), (341, 687), (403, 253), (53, 131), (239, 410), (715, 101), (673, 751), (908, 654), (744, 811), (343, 504), (405, 70), (456, 255), (434, 780), (910, 471), (84, 658), (560, 349), (746, 628), (834, 323), (808, 194), (40, 313), (551, 627), (458, 72), (837, 904), (310, 811), (0, 780), (954, 751), (64, 935), (42, 130), (861, 196), (93, 315), (890, 596), (71,

840), (859, 379), (403, 904), (445, 254), (95, 132), (53, 782), (124, 842), (186, 408), (662, 99), (22, 565), (498, 256), (456, 906), (491, 873), (279, 563), (618, 932), (188, 225), (660, 282), (930, 780), (558, 5), (617, 478), (828, 503), (713, 284), (899, 563), (257, 809), (611, 7), (804, 560), (153, 715), (429, 808), (629, 406), (806, 377), (837, 346), (642, 534), (177, 7), (248, 67), (206, 717), (441, 620), (660, 933), (403, 346), (372, 377), (558, 656), (815, 34), (208, 534), (443, 437), (877, 778), (279, 594), (713, 935), (341, 160), (775, 501), (425, 379), (653, 8), (611, 658), (846, 561), (496, 439), (744, 284), (394, 162), (9, 437), (826, 686), (412, 561), (62, 439), (248, 718), (901, 380), (310, 284), (899, 935), (195, 65), (381, 344), (31, 222), (815, 685), (465, 563), (527, 129), (155, 532), (598, 189), (226, 592), (525, 312), (622, 501), (600, 6), (520, 224), (394, 813), (866, 870), (928, 436), (164, 189), (556, 839), (193, 899), (930, 253), (580, 131), (124, 656), (773, 684), (651, 191), (609, 841), (195, 716), (31, 873), (93, 439), (565, 496), (527, 780), (868, 36), (598, 840), (217, 191), (894, 439), (246, 901), (308, 467), (494, 746), (784, 158), (144, 624), (620, 315), (797, 286), (813, 868), (711, 591), (361, 469), (651, 842), (591, 284), (713, 408), (363, 286), (803, 292), (904, 622), (868, 687), (348, 651), (766, 410), (410, 217), (60, 95), (69, 589), (157, 284), (127, 521), (764, 593), (158, 118), (350, 468), (0, 346), (261, 112), (923, 348), (91, 622), (567, 313), (753, 592), (188, 811), (403, 470), (615, 222), (465, 36), (937, 93), (558, 591), (591, 935), (943, 856), (7, 744), (897, 560), (113, 97), (279, 129), (618, 498), (680, 64), (866, 343), (516, 221), (102, 96), (131, 806), (733, 66), (518, 38), (547, 748), (124, 129), (317, 124), (921, 162), (153, 281), (186, 625), (470, 622), (720, 248), (341, 746), (370, 126), (246, 374), (199, 918), (722, 65), (744, 870), (751, 775), (401, 653), (2, 907), (892, 723), (463, 219), (299, 376), (775, 67), (930, 188), (219, 752), (124, 780), (804, 777), (55, 909), (217, 935), (693, 626), (93, 374), (868, 160), (100, 279), (241, 227), (270, 937), (503, 403), (124, 901), (899, 501), (339, 560), (644, 351), (622, 876), (62, 935), (272, 754), (51, 4), (919, 345), (505, 220), (708, 808), (627, 155), (155, 98), (839, 721), (489, 599), (675, 878), (281, 411), (713, 343), (899, 622), (928, 2), (682, 346), (556, 405), (341, 718), (890, 906), (476, 781), (312, 938), (773, 250), (374, 504), (959, 529), (24, 382), (210, 661), (879, 905), (529, 783), (591, 349), (248, 126), (427, 506), (255, 31), (932, 907), (589, 532), (279, 873), (11, 564), (658, 155), (308, 33), (828, 813), (228, 409), (64, 566), (875, 0), (496, 498), (126, 132), (711, 157), (259, 936), (906, 527), (183, 788), (837, 656), (157, 659), (629, 716), (67, 622), (177, 317), (31, 281), (682, 718), (179, 134), (403, 656), (372, 687), (848, 378), (208, 844), (684, 535), (746, 101), (91, 188), (582, 258), (775, 811), (425, 689), (197, 843), (799, 103), (777, 628), (9, 747), (341, 811), (383, 161), (33, 39), (651, 250), (307, 13), (412, 871), (830, 630), (62, 749), (124, 315), (310, 594), (744, 935), (786, 285), (436, 163), (868, 95), (414, 688), (465, 873), (527, 439), (344, 583), (155, 842), (631, 533), (817, 812), (467, 690), (622, 811), (529, 256), (365, 413), (899, 36), (870, 814), (932, 380), (164, 499), (279, 346), (930, 563), (580, 441), (166, 316), (2, 473), (64, 39), (93, 749), (569, 440), (219, 318)}

---Ключ: (441, 310)---

Текст:

утробылотихоегородокутанныйтьмоймирнонежилсявпостелипришлолетоиветербыллетнийтепл
оедыханиемиранеспешноеиленивоестоитлишьвстатьвысунутьсявокошкоитотчаспоймешьвотон
аначинаетсянастоящаясвободаижизньвотонопервоеутролетадуглассполдингдвенадцатилетотрод
утолькочтооткрылглазаикаквтеплуюречкупогрузилсявпредрассветнуюбезмятежностьонлежалвс
водчатойкомнаткеначетвертомэтажевовсемгороденебылобашнивышеиоттогочтоонпарилтаквыс
оковвоздухевместесиюньскимветромвнемрождалась чудодейственнаясилапоночамкогдавязыдуб
ыикленысливалисьводнобеспокойноеморедугласокидывалеговзглядомпронзавшимтьмуточнома
якисегоднявотздоровошепнулонвпередицелоелетонесчетноемножестводнейчутьнеполкалендар
яонужевиделсебямногорукимкакбожествошиваизкнижкипропутешествиятолькопоспевайрватье
щезеленыеяблокиперсикичерныекакночьсливыегоневытащитьизлесуизкустовизречкиакакприят
нобудетпомерзнутьзабравшисьвзаиндевелыйледниккаквеселожаритьсявбабушкинойкухнезаодн

остысячьюцыплятапоказаделоразвнеделюемупозволялиночеватьневдомикепососедствугдеспал
иегородителиимладшийбратишкатомаздесьвдедовскойбашнеонвзбегалпотемнойвинтовойлестн
иценасамыйверхиложилсяспатьвэтойобителикудесникасредигромовивиденийаспозаранкукогда
дажемолочникещенезвякалбутылкаминаулицахонпросыпалсяиприступалкзаветномуволшебству
стоявтемнотеуоткрытогоокнаоннабралполнуюгрудьвоздухаиизовсехсилдунулуличныефонарим
игомпогаслиточносвечкиначерномименинномпирогедугласдунулещеиещеивнебеначалигаснуть
звездыдугласулыбнулсяткнулпальцемтамитамтеперьтутивоттутвпредутреннемтуманеодинзадру
гимпрорезалисьпрямоугольникивдомахзажигалисьогнидалекодалеконарассветнойземлевдругоз
ариласьцелаявереницаоконвсемзевнутьвсемвставатьогромныйдомвнизуожилдедушкавынимайз
убыизстаканадугласнемногоподождалбабушкаипрабабушкажарьтеоладьисквознякпронесповсе
мкоридорамтеплыйдухжареноготестаивовсехкомнатахвстрепенулисьмногочисленныететкидядь
ядвоюродныебратьяисестрычтосехалисьсюдапогоститьулицастариковпросыпайсямиссэленлум
исполковникфрилеймиссисбентлипокашляйтевстаньтепроглотитесвоитаблеткипошевеливайтес
ьмистерджонасзапрягайтелошадьвыводитеизсараяфургонпораехатьзастарьемпотусторонуовраг
аоткрылисвоидраконьиглазаугрюмыеособнякискоровнизупоявятсянаэлектрическойзеленоймаш
инедвестарухиипокатятпоутреннимулицамприветственномахаякаждойвстречнойсобакемистерт
ридденбегитевтрамвайноедепоивскорепоузкимрусламмощеныхулицпоплыветтрамвайрассыпая
вокругжаркиесиниеискрыджонхафчарливудменвыготовышепнулдугласулицедетейготовыспрос
илонубейсбольныхмячейчтомоклинаросистыхлужайкахупустыхверевочныхкачелейчтоскучаясв
исалисдеревьевмампаптомпроснитесьтихонькопрозвенелибудильникигулкопробиличасыназдан
иисудаточносетьзаброшеннаяегорукойсдеревьеввзметнулисьптицыизапелидирижируясвоиморк
естромдугласповелительнопротянулрукуквостокуивзошлосолнцедуглассскрестилрукинагрудииу
лыбнулсякакнастоящийволшебниквоттотодумалонтолькояприказаливсеповскакаливсезабегалио
тличноебудетлетоионнапоследокогляделгородищелкнулемупальцамираспахнулисьдверидомовл
юдивышлинаулицулетотысячадевятьсотдвадцатьвосьмогогоданачалосьвтоутропроходяполужай
кедугласнаткнулсянапаутинуневидимаянитькоснуласьеголбаинеслышнолопнулаиотэтогопустяч
ногослучаяоннасторожилсяденьбудетнетакойкаквсенетакойещеипотомучтобываютднисотканны
еизоднихзапаховсловновесьмирможновтянутьносомкаквоздухвдохнутьивыдохнутьтакобяснялд
угласуиегодесятилетнемубратутомуотецкогдавезихвмашинезагородавдругиедниговорилещеоте
цможноуслышатькаждыйгромикаждыйшорохвселеннойиныеднихорошопробоватьнавкусаиные
наощупьабываютитакиекогдаестьвсесразувотнапримерсегодняпахнеттакбудтоводнуночьтамзах
олмаминевестьоткудавзялсяогромныйфруктовыйсадивседосамогогоризонтатакиблагоухаетввоз
духепахнетдождемнонанебениоблачкатогоиглядиктотоневедомыйзахохочетвлесунопокатамтиш
инадугласвовсеглазасмотрелнаплывущиемимополянетнисадомнепахнетнидождемдаиоткудабыр
азнияблоньнетнитучиктотамможетхохотатьвлесуавсетакидугласвздрогнулденьэтоткакойтоособе
нныймашинаостановиласьвсамомсердцетихоголесаануребятанебаловатьсяониподталкивалидру
гдругалоктямихорошопапамальчикивылезлиизмашинызахватилисиниежестяныеведраисойдясп
устыннойпроселочнойдорогипогрузилисьвзапахиземливлажнойотнедавнегодождяищитепчелск
азалотецонивсегдавьютсявозлевиноградакакмальчишкивозлекухнидугласдугласвстрепенулсяоп
ятьвитаешьвоблакахсказалотецспустисьназемлюпойдемснамихорошопапаионигуськомпобрели
полесувпередиотецрослыйиплечистыйзанимдугласапоследнимсеменилкоротышкатомподнялис
ьнаневысокийхолмипосмотреливдальвонтамуказалпальцемотецтамобитаютогромныеполетнем
утихиеветрыинезримыеплывутвзеленыхглубинахточнопризрачныекитыдугласглянулвтусторону
ничегонеувиделипочувствовалсебяобманутымотецкакидедушкавечноговоритзагадкамииивсета
кидугласзатаилдыханиеиприслушалсячтотодолжнослучитьсяподумалоняужзнаюавотпапоротни
кназываетсявенеринволосотецнетороплivошагалвпередсинееведропозвякивалоунеговрукеаэточ
увствуетеионковырнулземлюноскомбашмакамиллионылеткопилсяэтотперегнойосеньзаосеньюп
адалилистьяпоказемлянесталатакоймягкойухтыяступаюкакиндеецсказалтомсовсемнеслышноду

гласпотрогалземлюноничегонеощутилонвсевремянастороженноприслушивалсямыокруженыду
малончтотослучитсяночтооностановилсявыходижегдетытамчтотытакоемысленнокричалонтоми
отецшлидальшепотихойподатливойземленасветенеткружеватоньшенегромкосказалотеципоказа
лрукойвверхгделиствадеревьеввплеталасьвнебоилиможетбытьнебовплеталосьвлиствувсеравноу
лыбнулсяотецвсеэтокружевазеленыеиголубыевсмотритесьхорошенькоиувидителесплететихсло
вногудящийстанокотецстоялуверennопохозяйскиирассказывалимвсякуювсячинулегкоисвободн
оневыбираясловчастоонисамсмеялсясвоимрассказамиотэтогоонитеклиещесвободнеехорошопри
случаепослушатьтишинуговорилонпотомучтотогдаудаетсяуслышатькакноситсяввоздухепыльца
полевыхцветовавоздухтакигудитпчеламидадатакигудитавотслышитетамзадеревьямиводопадом
льетсяптичьещебетаньевотсейчасдумалдугласвотоноужеблизкоаяещеневижусовсемблизкорядо
мдикийвиноградсказалотецнамповезлосмотритеканенадоахнулпросебядугласнотомиотецнакло
нилисьипогрузилирукившуршащийкустчарырассеялисьтопугающееигрозноечтоподкрадывалос
ьблизилосьготовобылоринутьсяипотрястиегодушуисчезлоопустошенныйрастерянныйдугласупа
лнаколенипальцыегоушлиглубоковзеленуютеньивынырнулиобагренныеалымсокомсловноонвзр
езаллесножомисунулрукивоткрытуюранумальчикизавтракатьведрачутьнедоверхунаполненыдик
имвиноградомилеснойземляникойвокруггудятпчелыэтововсенепчелыацелыймиртихонькомурл
ычетсвоюпесенкуговоритотецаонисидятназамшеломстволеупавшегодереважуютсандвичиипыт
аютсяслушатьлескакслушаетонотецчутьпосмеиваясьискосапоглядываетнадугласахотелбылочто
тосказатьнопромолчалоткусилещекусоксандвичаизадумалсяхлебсветчинойвлесунеточтодомавк
уссовсемдругойверноостреечтолимятойотдаетсмолойаужаппетиткакразыгрываетсядугласперес
талжеватьипотрогалязыкомхлебиветчинунетнетобыкновенныйсандвичтомкивнулпродолжаяжев
атьяпонимаюпапведьужепочтислучилосьдумаетдугласнезнаючтоэтоноонобольшущеепрямогро
мадноечтотоегоспугнулогдежеонотеперьопятьушловтоткустнетгдетозамнойнетнетздесьтутрядо
мдугласисподтишкапощупалсвойживотоноещевернетсянадотольконемножкоподождатьбольнон
ебудетяужзнаюнезатемонокомнепридетнозачемжезачема

Висновок:

В результаті виконання третього комп’ютерного практикуму було опрацьовано й реалізовано принципи шифрування методом афінною підстановки мовою Python3.

Найскладнішим було саме перетворення формул у код у функціях з дешифрації тексту й знаходження ключів.