Міністерство освіти і науки України
НТУУ «Київський політехнічний інститут ім. Ігоря Сікорського»
Навчально-науковий Фізико-технічний інститут

Криптографія

Комп’ютерний практикум №3.

Криптоаналіз афінної біграмної підстановки

Варіант №3

Виконав:

Студент групи ФБ-31

Васалатій А. Ю., Яковчук О. С.

Перевірено:

Байденко П. В.

23.10.2025

Виконання роботи було почато з ознайомлення з шифром афінної біграмної підстановки. На відміну від шифру Віженера, який ми досліджували в межах минулого практикуму, що працював з окремими символами, даний шифр здійснює перетворення біграм незалежно одна від одної. В процесі шифрування текст розбивається на біграми, що не перетинаються, і кожна подається у вигляді:

$(x_{2i-1},\ x_{2i})\ <->\ X_i = x_{2i-1}m + x_{2i},$ де m – розмір алфавіту.

Саме перетворення виглядає наступним чином:

$Y_i = aX_i + b\ mod\ m^2,$ де (a, b) – ключ, $0 < a < m^2;\ 0 \leq b\ < m^2$.

При чому на a накладається додаткова умова - воно має бути взаємопростим з m^2, адже лише у такому випадку воно буде мати обернене за цим модулем, яке необхідне для проведення дешифрування, що виконується наступним чином:

$X_i = a^{-1}(Y_i - b)\ mod\ m^2$.

Знаючи це - відразу було реалізовано підготовчий код, що за відомим ключем зможе зчитати і розшифрувати ШТ з файлу за переданим шляхом. Однак ключ у нас відсутній - потрібно реалізувати атаку лише за наявним ШТ. За рахунок збереження у ШТ статичних властивостей пов’язаних з біграмами для атак можна застосувати частотний аналіз. Тобто, знаючи найпоширеніші біграми російської мови на використовуваному алфавіті без пробілу - "ст", "но", "то", "на", "ен", ми можемо спробувати співставляти їх з біграмами, що найчастіше зустрічаються у нашому ШТ. Для підрахунку частот біграм був використаний код з першого практикуму, однак попередньо трохи видозмінений. Отримавши дві пари виду “біграма ШТ - біграма ВТ” ми можемо скласти систему з двох лінійних порівнянь виду:

$$\begin{cases} Y^{*} \equiv aX^{*} + b \pmod{m^2} \\ Y^{**} \equiv aX^{**} + b \pmod{m^2} \end{cases},$$

З неї можемо отримати a, для чого достатньо розв'язати лінійне порівняння: $a(X^{*} - X^{**}) = (Y^{*} - Y^{**}) \, mod \, m^2$. Для цього, згадавши необхідні математичні основи було реалізовано відповідні підпрограми - для пошуку НСД, оберненого за модулем (на основі розширеного алгоритму Евкліда) і власне підпрограму, що розв'язує лінійні порівняння, беручи до уваги усі можливі варіанти розв'язку.

Далі як загалом, так і в коді, для кожного отриманого a обчислюється $b = Y^{*} - aX^{*} mod \, m^2$.

Маючи потенційні ключі (a, b) ми можемо спробувати розшифрувати ШТ, однак виникає необхідності перевіряти отримані тексти на змістовність. Користуючись отриманими знаннями в межах першого комп'ютерного практикуму для автоматизації цього процесу було прийнято рішення використовувати статистичні властивості притаманні природним мовам. Спочатку було здійснено спробу відсіювати некоректні ключі шляхом підрахунку частот найпоширеніших монограм і порівнянню їх з еталонними з відкритих джерел/результатами першого КП - що загалом працювало, однак беручи до уваги відносно невеликі розміри ШТ/ВТ і як наслідок відхилення у статичній інформації відносно значень отриманих на великих обсягах даних - давало слабші результати, ніж були отримані фінальним способом. Як остаточне рішення для відсіювання некоректних розшифрувань було обрано порівняння ентропії монограм та біграм з перекриттям (важливо брати саме з перекриттям, адже інакше через однаковий розподіл частот біграм як ШТ, так і ВТ буде отримано однакове значення ентропії, наближене до еталонного) з еталонними. Такий підхід

засновується на тому, що спроба розшифрувати ШТ з некоректним ключем дасть нам текст, дані ентропійні характеристики якого будуть перевищувати ті, що відповідають текстам, написаним природною мовою, адже шифр афінної біграмної заміни не зберігає частотні характеристики біграм, що перетинаються, і як наслідок монограм.

На основі КП1 як порогові значення для H_1 та H_2 було обрано 4.455 і 4.125 відповідно.

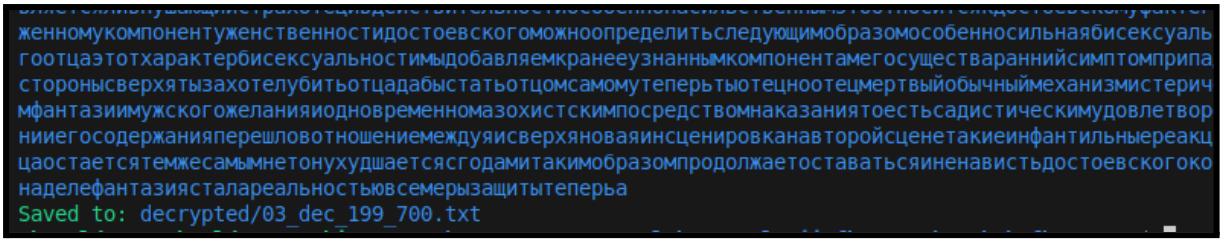
Тип джерела відкритого тексту	Ентропія	Надлишковість
H1 (монограми)	4.4393304946163665	0.10392519462562477
H1_ws (монограми з пробілами)	4.347574526370398	0.1304850947259204
H2_no (біграми без перетинів)	4.122434891829624	0.16789028259001282
H2_no_ws (біграми без перетинів з пробілами)	3.9412994623955098	0.211740107520898
H2_ov (біграми з перетинами)	4.121835034126119	0.16801136331954447
H2_ov_ws (біграми з перетинами та пробілами)	3.9413951409046173	0.21172097181907656

Приклад роботи скрипта:

```
the_old_man@theOldMan-machine:~/Desktop/crypto25-26/lab3/vasalatii_fb-31_yakovchuk_fb-31_cp3$ /home/the_old_man/Desktop/cry
26/lab3/vasalatii_fb-31_yakovchuk_fb-31_cp3/main.py -f /home/the_old_man/Desktop/crypto25-26/tasks/cp3/variants.utf8/03.txt
================================================================
================================================================
File type of /home/the_old_man/Desktop/crypto25-26/tasks/cp3/variants.utf8/03.txt: text/plain
Encoding detection result: {'encoding': 'utf-8', 'confidence': 0.99, 'language': ''}
The most common bigrams in ct:
```

тд	рб	во	що	кд
0.0273535	0.0188277	0.0184725	0.0159858	0.0149201

```
================================================================
Key: (199,700)
PT H1: 4.393647309602373
PT H2 (overlapped): 3.985665657673874
Decryption result:
отцеубийствокакизвестноосновноеиизначальноепреступлениечеловечествваиотдельногочеловекавовсякомслучаеоноглавныйисточникчувст
тьдушевноепроисхождениевиныипотребностиискупленияноотнюдьнесущественноединственныйилиэтоисточникпсихологическоеположениеслом
лентнопомимоненавистииззакоторойхотелосьбыотцакаксоперникаустранитьсуществуетобычнонекоторыядолянежностикнемуобаотношениясл
вызываетвосхищениехотелосьбыбытькаконипотомучтохочетсяегоустранитьвсеэтонаталкиваетсянакрупноепрепятствиевопределенныймомен
етилабысостороныотцанаказаниечерезкастрациюизстрахакастрациитоестьвинтересахсохранениясвоеймужественностиребенокотказываетс
таетсявобластибессознательногооноявляетсяосновойдляобразованиячувствавинынамкажетсячтомыописалинормальныепроцессыобычнуюсуд
нениевозникаютдальнейшиеосложненияеслиуребенкасильнееразвитконституционныйфакторназываемыйнамибисексуальностьютогдаподугроз
ьсявсторонуженственностиболеетоготенденцияпоставитьсебянаместоматериипереняьеерольказкобекталюбвиотцаодналишьбоязньюкастраци
ебяикастрированиеслионхочетбытьлюбимымотцомкакженщинатакобрекаютсянавытеснениеобапорываненавистьютцувлюбленностьвотцаизв
```



5 найчастіших біграм ШТ:

тд	рб	во	щю	кд
0.0273535	0.0188277	0.0184725	0.0159858	0.0149201

Знайдений ключ:

a=199, b=700

Розшифрований текст:

отцеубийствокакизвестноосновноеиизначальноепреступлениечеловечестваиотдельног
очеловекавовсякомслучаеоноглавныйисточникчувствавинынеизвестноединственныйлии
сследованиямнеудалосьещеустановитьдушевноепроисхождениевиныипотребностиискупл
енияноотнюдьнесущественноединственныйлиэтоисточникпсихологическоеположениесло
жноинуждаетсявобъясненияхотношениемальчикакотцукакмыговоримамбивалентнопомимон
енавистииззакоторойхотелосьбыотцакаксоперникаустранитьсуществуетобычнонекотор
аядолянежностикнемуобаотношениясливаютсявидентификациюсотцомхотелосьбызанятьм
естоотцапотомучтоонвызываетвосхищениехотелосьбыбытькаконипотомучтохочетсяегоу
странитьвсеэтонаталкиваетсянакрупноепрепятствиевопределенныймоментребенокначи
наетпониматьчтопопыткаустранитьотцакаксоперникавстретилабысостороныотцанаказа
ниечерезкастрациюизстрахакастрациитоестьвинтересахсохранениясвоеймужественнос
тиребенокотказываетсяотжеланияобладатьматерьюиотустраненияотцапоскольку этожел
аниеостаетсявобластибессознательногооноявляетсяосновойдляобразованиячувствави
нынамкажетсячтомыописалинормальныепроцессыобычнуюсудьбутакназываемогоэдиповак
омплексаследуетоднаковнестиважноедополнениевозникаютдальнейшиеосложненияеслиу
ребенкасильнееразвитконституционныйфакторназываемыйнамибисексуальностьютогдап
одугрозойпотеримужественностичерезкастрациюукрепляетсятенденцияуклонитьсявсто
ронуженственностиболеетоготенденцияпоставитьсебянаместоматерииперенятьеерольк
акобекталюбвиотцаодналишьбоязнькастрацииделаетэтуразвязкуневозможнойребенокпо
нимаетчтоондолженвзятьнасебяикастрированиееслионхочетбытьлюбимымотцомкакженщи
натакобрекаютсянавытеснениеобапорыванеенавистькотцуивлюбленностьвотцаизвестная
психологическаяразницаусматриваетсявтомчтоотненавистикотцуотказываютсявследст
виестрахапередвнешнейопасностьюкастрацией влюбленностьжевотцавоспринимаетсякак
внутренняяопасностьпервичногопозывакотораяпосутисвоейсновавозвращаетсяктойжев
нешнейопасностистрахпередотцамделаетненавистькотцунеприемлемойкастрацияужасна
каквкачествекарытакиценылюбвиизобоихфактороввытесняющихненавистькотцупервыйне
посредственныйстрахнаказанияикастрациисследуетназватьнормальнымпатогеническоеу
силениепривноситсякаккажетсялишьдругимфакторомбоязньюженственнойустановкиярко
выраженнаябисексуальнаясклонностьстановитсятакимобразомоднимизусловийилиподтв
ерждений неврозаэтусклонностьочевидноследуетпризнатьиудостоевскогоионалатентна
ягомосексуальностьпроявляетсявдозволенномвидевтомзначенииикакоеимелавегожизнид
ружбасмужчинамивегодостранностинежномотношенииксоперникамвлюбвииивегопрекрасно

мпониманииположенийобяснимыхлишьвытесненнойгомосексуальностьюкакнаэтоуказываю тмногочисленныепримерыизегопроизведенийсожалеюноничегонемогуизменитьеелиподро бностионенавистиилюбвикотцуиобихвидоизмененияхподвлияниемугрозыкастрацииинесве дущемувпсихоанализечитателюпокажутсябезвкуснымиималовероятнымипредполагаючтои меннокомплекскастрацииибудетотклоненсильнеевсегоносмеюуверитьчтопсихоаналитиче скийопытставитименноэтиявленияявневсякогосомненияинаходитвнихключклюбомуневроз уиспытаемжеговслучаетакназываемойэпилепсиинашегописателянонашемусознаниютакч уждытеявленияявластикоторыхнаходитсянашабессознательнаяпсихическаяжизньуказа ннымвышенеисчерпываютсявэдиповомкомплексепоследствиявытесненияненавистикотцун овымявляетсяточтовконцеконцовотождествлениесотцомзавоевываетвнашемяпостоянное местоэтоотождествлениевосринимаетсянашимянопредставляетсобойвнемособуюинстан циюпротивостоящуюостальномусодержаниюнашегоямыназываемтогдаэтуинстанциюнашимс верхяиприписываемейнаследницеродительскоговлияниянаиважнейшиефункцииеслиотецб ылсуровнасильственжестокнашесверхяперенимаетотнегоэтикачестваивегоотношениикя сновавозникаетпассивностькоторойкакразнадлежалобыбытьвытесненнойсверхясталоса дистическимстановитсямазохистскимтоестьвосновесвоейженственнопассивнымвнашем явозникаетбольшаяпотребностьвнаказанииияотчастиотдаетсебякактаковоевраспоряже ниесудьбыотчастиженаходитудовлетворениевжестокомобращениисниксверхясознаниеви ныкаждаякараявляетсяведьвосновесвоейкастрациейикактаковаяосуществлениемизнача льногопассивногоотношениякотцуисудьбавконцеконцовлишьдальнейшаяпроекцияотцано рмальныеявленияпроисходящиеприформированиисовестидолжныпоходитьнаописанныезде сьанормальныенамещенеудалосьустановитьразграниченияміждунимизамечаетсячтонаиб ольшаяроль здесьвконечномитогеприписываетсяпассивнымэлементамвытесненнойженств енностиищекакслучайныйфакторимеетзначениеявляетсяливнушающийстрахотецивдейст вительностиособеннонасильственнымэтоотносится кдостоевскомуфактегоисключительн огочувствавиныравнокакимазохистскогообразажизнимысводимкегоособенноярковыраже нномукомпонентуженственностидостоевскогоможноопределитьследующимобразомособен носильнаябисексуальнаяпредрасположенностьиспособностьсособойсилойзащищатьсяот зависимостиотчрезвычайносуровогоотцаэтотхарактербисексуальностимыдобавляемкра нееузнаннымкомпонентамегосуществараннийсимптомприпадковсмертиможнорассматрива тькакотождествлениесвоегоясотцомдопущенноевкачественаказаниясосторонысверхяты захотелубитьотцадабыстатьотцомсамомутеперьтыотецноотецмертвыйобычныймеханизми стерическихсимптомовиктомужетеперьтебяубиваетотецдлянашегоясимптомсмертиявляе тсяудовлетворениемфантазиимужскогожеланияиодновременномазохистскимпосредством наказаниятоестьсадистическимудовлетворениемобаяисверхяиграютрольотцаидальшево бщемотношениемеждуличностьюиобектомотцаприсохраненииегосодержанияперешловотно шениемеждуяисверхяноваяинсценировканавторойсценетакиеинфантильныереакцииэдипо вакомплексамогутзаглохнутьеслидействительностьнедаетимвдальнейшемпищинохаракт еротцаостаетсятемжесамымнетонухудшаетсясгодамитакимобразомпродолжаетоставатьс яиненавистьдостоевскогокотцужеланиесмертиэтомузломуотцустановитсяопаснымеслит акиевытесненныежеланияосуществляютсянаделефантазиясталареальностьювсемерызащи тытеперьа

Висновки

Першочергово, в межах даного практикуму нами було здійснено ознайомлення з теоретичними відомостями щодо шифру афінної біграмної заміни. Розглянувши перетворення, що застосовується в межах даного шифру, було визначено алгоритм проведення атаки на основі ШТ шляхом застосування частотного аналізу. Атака відбувається за рахунок збереження у ШТ певних статистичних властивостей ВТ, а саме значень

частот зустрічі біграм, що не перетинаються. Також було нагадано певні теоретичні основи щодо розв’язування лінійних порівнянь - необхідного кроку при відновленні застосованого ключа.

Базуючись на отриманих знаннях в першій частині практикуму, нами було реалізовано програмний засіб, що використовуючи частотний аналіз, здійснює відновлення відкритого тексту перетвореного шифром афінної біграмної заміни. Процес роботи повністю автоматизований, і загалом не вимагає втручання з боку користувача, за рахунок детектування і відсіювання некоректних результатів дешифрування, шляхом аналізу ентропійних властивостей отриманих ВТ і порівняння їх з еталонними, що відповідають текстам написаним природною мовою.