Politechnika Wrocławska

Sprawozdanie z zajęć laboratoryjnych
Cyberbezpieczeństwo

Lab 02
Kryptografia historyczna

Tomasz Mroczko, 266604

October 15, 2023

1 Dane testowe

Użyty tekst

Do eksperymentów użyty został następujący tekst:

> Żyłem z wami, cierpiałem i płakałem z wami; Nigdy mi kto szlachetny, nie był obojętny: Dziś was rzucam i dalej idę w cień — z duchami, A jak gdyby tu szczęście było, idę smętny. Nie zostawiłem tutaj żadnego dziedzica Ani dla mojej lutni, ani dla imienia: Imię moje tak przeszło, jako błyskawica, I będzie, jak dźwięk pusty, trwać przez pokolenia. Lecz wy, coście mnie znali, w podaniach przekażcie, Żem dla ojczyzny sterał moje lata młode; A póki okręt walczył, siedziałem na maszcie, A gdy tonął, z okrętem poszedłem pod wodę... Ale kiedyś, o smętnych losach zadumany Mojej biednej ojczyzny, pozna, kto szlachetny, Że płaszcz na moim duchu był nie wyżebrany, Lecz świetnościami moich dawnych przodków świetny. Niech przyjaciele moi w nocy się zgromadzą I biedne serce moje spalą w aloesie, I tej, która mi dała to serce, oddadzą: Tak się matkom wypłaca świat, gdy proch odniesie... Niech przyjaciele moi siędą przy pucharze I zapiją mój pogrzeb — oraz własną biedę: Jeżeli będę duchem, to się im pokażę, Jeśli Bóg mnie uwolni od męki, nie przyjdę... Lecz zaklinam: niech żywi nie tracą nadziei I przed narodem niosą oświaty kaganiec; A kiedy trzeba, na śmierć idą po kolei, Jak kamienie, przez Boga rzucane na szaniec! Co do mnie — ja zostawiam maleńką tu drużbę Tych, co mogli pokochać serce moje dumne; Znać, że srogą spełniłem, twardą Bożą służbę, I zgodziłem się tu mieć niepłakaną trumnę. Kto drugi tak bez świata oklasków się zgodzi Iść?... taką obojętność, jak ja, mieć dla świata? Być sternikiem duchami napełnionej łodzi I tak cicho odlecieć, jak duch, gdy odlata? Jednak zostanie po mnie ta siła fatalna, Co mi żywemu na nic, tylko czoło zdobi; Lecz po śmierci was będzie gniotła niewidzialna, Aż was, zjadacze chleba — w aniołów przerobi.

Zgodnie z zaleceniami tekst spłaszczono do alfabetu łacińskiego, pozbawiono znaków interpunkcyjnych oraz białych znaków

2 Zadania

Zadanie 1.2

> *Wybierz kilka z nich i sprawdź ich właściwości (tzn. przestrzeń kluczy, skutki wielokrotnego szyfrowania, czy istnieją tzw. klucze słabe np. dla Rot-13, Playfair, metody łamania szyfru). W raporcie należy umieścić właściwości wybranych algorytmów*

Do przeanalizowania wybrano następujące algorytmy:

- **Cezar**
  - **Opis:** Szyfr Cezara to najprostsza technika szyfrowania. Klucz ma postać litery lub liczbie jej odpowiadającej (A:0, B:1, ..., Z:25). Polega na zastąpieniu każdej litery tekstu jawnego przesunięciem jej o wartość klucza w alfabecie. Jest szyfrem monoalfabetycznym, czyli każdemu występieniu danej litery w tekscie jawnym odpowiada inna, stała litera w tekście zaszyfrowanym.
  - **Przestrzeń kluczy:** Ponieważ przesuwamy każdą literę tekstu o stałą liczbę pozycji w alfabecie, przestrzeń kluczy jest równa długości alfabetu. Dla alfabetu łacińskiego jest to 26.
  - **Wielokrotne szyfrowanie:** Wielokrotne szyfrowanie sprowadza się do wielokrotnego przesunięcia znaku w alfabecie. Nie wpływa korzystnie na jakość szyfru, wręcz przeciwnie - wielokrotne szyfrowanie może spowodować przesunięcie znaków na ich oryginalną pozycję, powodując odszyfrowanie.
  - **Klucze słabe:** Każdy klucz dla tego szyfru jest relatywnie słaby. Wyjątkowo słaby wydaje się klucz o wartości 13 (Rot-13), ponieważ dwukrotne szyfrowanie nim spowoduje odszyfrowanie.
  - **Łamanie szyfru:** Klucz cezara złamać można przesuwając tekst 25 razy o pojedynczą literę i próbując odczytać wiadomość. Nie wymaga to dużych nakładów. Kolejnym sposobem złamania jest analiza częstotliwości występowania znaków, a następnie przyrównanie jej do charakterystyki danego języka. Im dłuższy tekst, tym lepsze efekty powinna dać analiza częstotliwości występowania liter.
- **Vigenere**
  - **Opis:** Szyfr Vigenere to technika która jest bardzo podobna do szyfru Cezara. Szyfrowanie wymaga ustalenia klucza, który powinien składać się z liter alfabetu szyfrowanego tekstu. W przypadku użycia klucza krótszego niż tekst jawny, konieczne jest wielokrotne powtórzenie klucza aby uzyskać długość tekstu jawnego. Po ustaleniu klucza każda litera tekstu jawnego przesunięta zostaje o wartość litery klucza o tym samym indeksie. Jest szyfrem polialfabetycznym (jedna litera zastąpiona może być w różny sposób, w zależności od pozycji w tekście), co czyni go mniej podatnym na analizę częstotliwości.
  - **Przestrzeń kluczy:** Hasło użyte do szyfrowania musi mieć długość n, gdzie n to długość tekstu jawnego. Oznacza to, że na każdym miejscu hasła może być jedna litera alfabetu. W takim razie liczba możliwych kluczy to a^n, gdzie a to liczba liter alfabetu, a n jest długością tekstu jawnego. W wypadku alfabetu łacińskiego, przestrzeń kluczy to 26^n. Warto zaznaczyć jednak, że zazwyczaj jako klucz używany jest tekst znacznie krótszy niż tekst jawny (co nie wpływa na potencjalną przestrzeń kluczy).

- **Wielokrotne szyfrowanie:** Podobnie jak w przypadku szyfru Cezara, wielokrotne szyfrowanie nie utrudnia rozszyfrowania tekstu. Każda efekt osiągnięty poprzez wielokrotne szyfrowanie może być również osiągnięty pojedynczym szyfrem. Przy dwukrotnym szyfrowaniu klucz zostaje wydłużony do najmniejszej wspólnej wielokrotności obu kluczy.
- **Klucze słabe:** W przypadku tego algorytmu słabsze są klucze krótkie. Klucze takie powtarzają się bardziej przez co łatwiejsze jest odkrycie klucza. Im dłuższy klucz tym bardziej
- **Łamanie szyfru:** Jeśli użyty klucz jest krótki względem tekstu jawengo, to często się powtarza przez co łatwiej odkryć jego długość. Użycie metody Kasiskiego i testu Friedmana znacznie ułatwie odszyfrowanie.

- **Playfair**
  - **Opis:** Jest to również szyfr polialfabetyczny, co oznacza, że ten sam znak w tekście jawnym może być zaszyfrowany na kilka różnych sposobów, w zależności od swojego otoczenia. W tym szyfrze, w przeciwieństwie do poprzedników, tekst jawny podzielony jest na pary zwane digrafami zamiast pojedynczych liter. Szyf używa macierzy liter alfabetu o wymiarach 5x5. Do konfiguracji macierzy używa się hasła. Macierz wypałnia się rząd po rzędzie, wpisując każdy znak tylko raz. (dla hasła KAJAK, wpiszemy tylko 3 litery: KAJ, ponieważ każda litera macierzy musi być unikatowa). Następnie dopełniamy macierz wykorzystując nieużyte jeszcze litery. Ze względu na ograniczoną ilość znaków (25) literę "j" zamienia się na literę "i". Po utworzeniu macierzy, dzielimy tekst jawny na pary liter. Następnie szyfrujemy każdy digraf według następujących zasad:
    (a) Obie litery są w tej samej kolumnie: w tym wypadku zastępujemy każdą literę tą znajdującą się pod nią.
    (b) Obie litery są w tym samym wierszu: zastępujemy każdą literę na tę po prawej stronie.
    (c) Pozostałe przypadki (litery tworzą prostokąt zamiast prostej): zatępujemy obie litery literami znajdującymi się w tym samym rzędzie, na przeciwległym wierzchołku prostokąta.
  - **Przestrzeń kluczy:** Macierz 5x5 zawiera 25 unikatowych znaków, nietrudno więc zauważyć że możliwych jest tutaj 25! kluczy.
  - **Łamanie szyfru** Ciekawą słabością jest fakt, że dany digram oraz jego odwrotność w tekście jawnym będą również odwrotnościami w tekscie zaszyfrowanym. Zaszyfrowanie tekstu jawnego "ABBA", może dać bardzo wiele różnych kombinacji, jednak symetria tego słowa pozostanie zachowana. Jeśli język tekstu jawnego jest znany, można wykorzystać ten fakt.

Zadanie 1.3

Co możemy powiedzieć o szyfrowaniu wielokrotnym w kontekście algorytmów historycznych (rozważ ich różne klasy)? Jak takie działanie wpływa na możliwość rozszyfrowania tekstu. Odpowiedź na to pytanie zilustruj wynikiem eksperymentu przeprowadzonego w Cryptool.

Figure 1: Wielokrotne szyfrowanie szyfrem Cezara

Najpierw użyto klucza "C", następnie klucza "V", a finalnie klucza "D". Jak widać, kolejne szyfrowania nie zmieniły znacząco struktury tekstu, a ostatnie spowodowało wręcz ujawnienie tekstu.

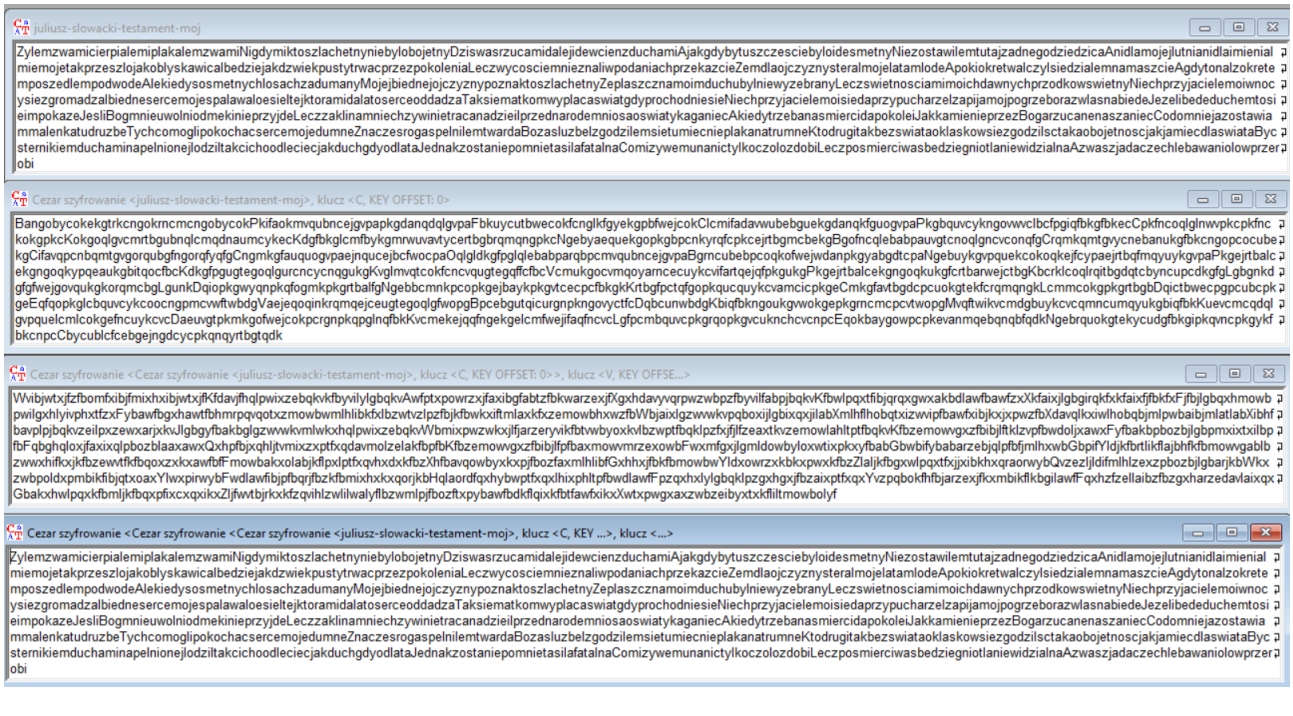


Figure 2: Wielokrotne szyfrowanie Vigenere

Najpierw użyto klucza "HASLO", następnie haslem "TAJNEKLUCZ". Następnie odszyfrowano używając kombinacji poprzednich haseł - "AABYSRLMNN".

Figure 3: Wielokrotne szyfrowanie Hill

Jako klucza użyto dwukrotnie macierzy $\begin{matrix} Q & D \\ Z & I \end{matrix}$. Następnie odszyfrowano za pomocą macierzy $\begin{matrix} T & U \\ C & J \end{matrix}$.

Konkluzja: W kontekście algorytmów historycznych szyfrowanie wielokrotne zazwyczaj nie utrudnia odszyfrowania tekstu. Bardzo często sprowadza się po prostu do połączenia kluczy użytych w poszczególnych szyfrowaniach (jest równoznaczne z jednokrotnym zaszyfrowaniem innym kluczem, który jest w pewnym sensie sumą poprzedników). W skrajnych przypadkach powtórzenie szyfrowania może spowodować odszyfrowanie. W przypadku szyfru Vigenere, wielokrotne szyfrowanie może znacznie wydłużyć klucz, co może nieznacznie utrudnić rozszyfrowanie tekstu (im dłuższy klucz, tym mniej razy się powtarza).
Podsumowując, szyfrowanie wielokrotne przy użyciu algorytmów historycznych zazwyczaj *nie utrudnia* zauważalnie odszyfrowania tekstu.

Zadanie 1.4

Który z przetestowanych algorytmów może być uznany za silniejszy i dlaczego?

Dla współczesnej kryptografii, wszystkie testowane algorytmy wydają się relatywnie słabe. Zdecydowanie najsłabsze wydają się być monoalfabetyczne szyfry, co za tym idzie - szyfr Cezara. Jest podatny na metody analizy oraz na metodę "brute force", ponieważ posiada tylko 25 możliwości zakodowania. *Znacznie* silniejszy jest algorytm Vigenere. Przestrzeń kluczy jest bardzo duża, jeśli użyje się długiego klucza. Znane są jednak metody kryptoanalizy, które pozwalają na złamanie go. Najsilniejsze z testowanych wydają się algorytmy Playfair oraz Hill. Oba te algorytmy wykorzystują macierze do zaszyfrowania tekstu jawnego. Algorytm Playfair operuje na digramach, co wprowadza dodatkową warstwę złożoności. Algorytm Hilla opiera się na matematycznym podejściu, dzięki któremu trudniej zrozumieć zasadę jego działania. Oba te

algorytmy utrudniają analizę statystyczną względem wymienionych poprzednio. Porównując algorytmy Hilla i Playfair, *trudno* jednoznacznie ocenić który jest silniejszy.

Zadanie 2.1

Porównaj wartości entropii tekstów jawnych dla różnych języków (angielski, polski, niemiecki, francuski, włoski, hiszpański, ...)

W zadaniu użyte zostały napisy z filmu "Władca pierścieni: Drużyna pierścienia", w językach: polski, angielski, niemiecki, ograniczono długość do 3000 znaków

Język	Polski	Angielski	Niemiecki
Entropia	4.25	4.12	4.02

Table 1: Entropia tekstu w różnych językach

Zadanie 2.2

Porównaj wartości entropii tekstu jawnego i tekstu zaszyfrowanego dla różnych algorytmów. W zadaniu należy zaszyfrować jeden tekst jawny za pomocą algorytmów wymienionych poniżej

Algorytm	Przed	Po
Cezar	4.25	4.25
Vigenere, "HASLO"	4.25	4.60
Vigenere, "DLUGITAJEMNICZYKLUCZ"	4.25	4.67
Hill, "FE LJ"	4.25	4.64
Hill, "TCA HNR NOB"	4.25	4.67
Playfair, "HASLO"	4.25	4.45
Playfair, "TAIEMNEHASLO"	4.25	4.44
ADFGVX	4.25	2.41
Homofony	4.25	7.89
Permutacja	4.25	4.25

Table 2: Entropia tekstu jawnego i zaszyfrowanego różnymi algorytmami

Wnioski: Szyfrowanie może znacząco wpłynąć na entropię tekstu. Algorytm homofonów bardzo znacząco zwiększa entropię, algorytm ASFGVX przeciwnie. Szyfrowanie cezara nie wpływa na poziom entropii, Vigenera oraz Hilla, w zależności od użytego hasła, mają tendencję do zwiększania go.

Zadanie 2.3

.Porównaj histogramy tekstów jawnych dla wybranych 3 różnych języków (angielski, polski, niemiecki, francuski, włoski, hiszpański, ...).

Język polski

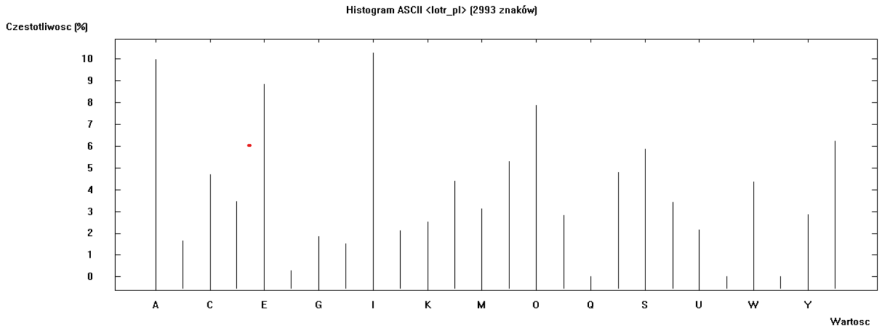


Figure 4: Histogram języka polskiego

Język angielski

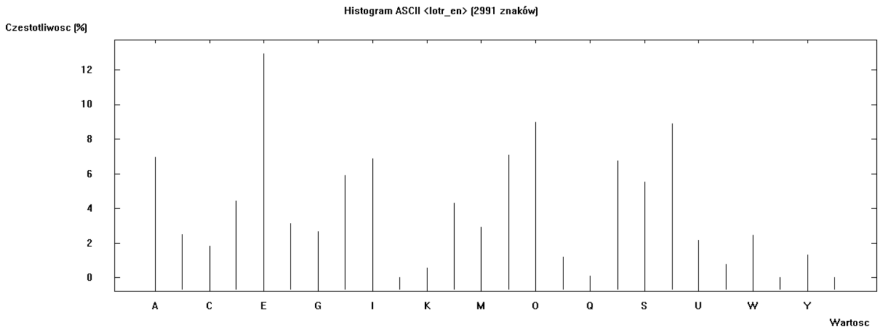


Figure 5: Histogram języka angielskiego

Język niemiecki

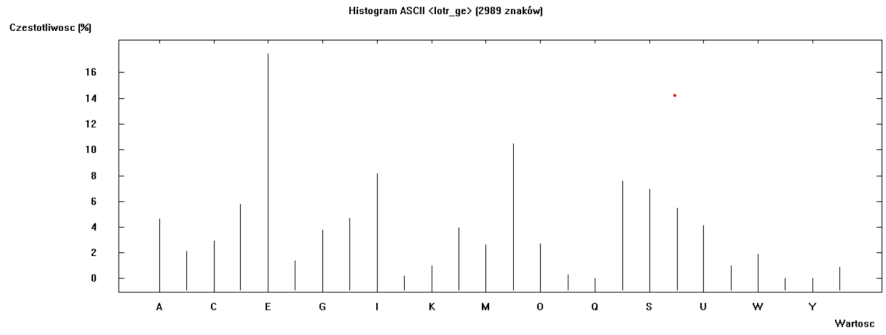


Figure 6: Histogram języka niemieckiego

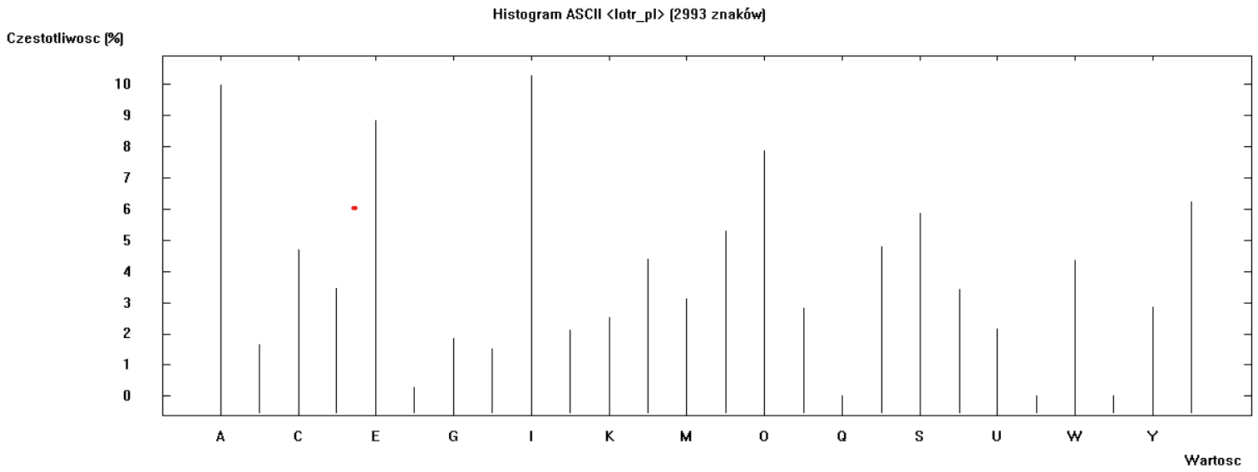
Jak widać powyżej, każdy język posiada najczęsciej występujące znaki. Dla języka polskiego najczęsciej występują litery "a","e" oraz "i". W języku angielskim oraz niemieckim najczęsciej występuje litera "e", dość mocno dominując nad pozostałymi.

Zadanie 2.4

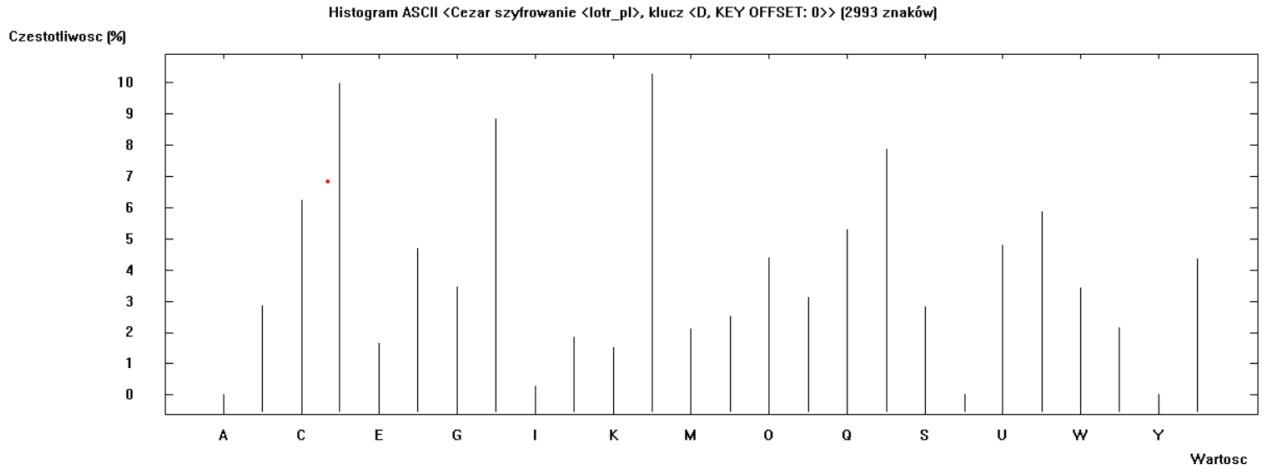
Porównaj histogramy jednego tekstu jawnego i zaszyfrowanego w zależności od algorytmu z punktu 2.

Język polski

Tekst jawny

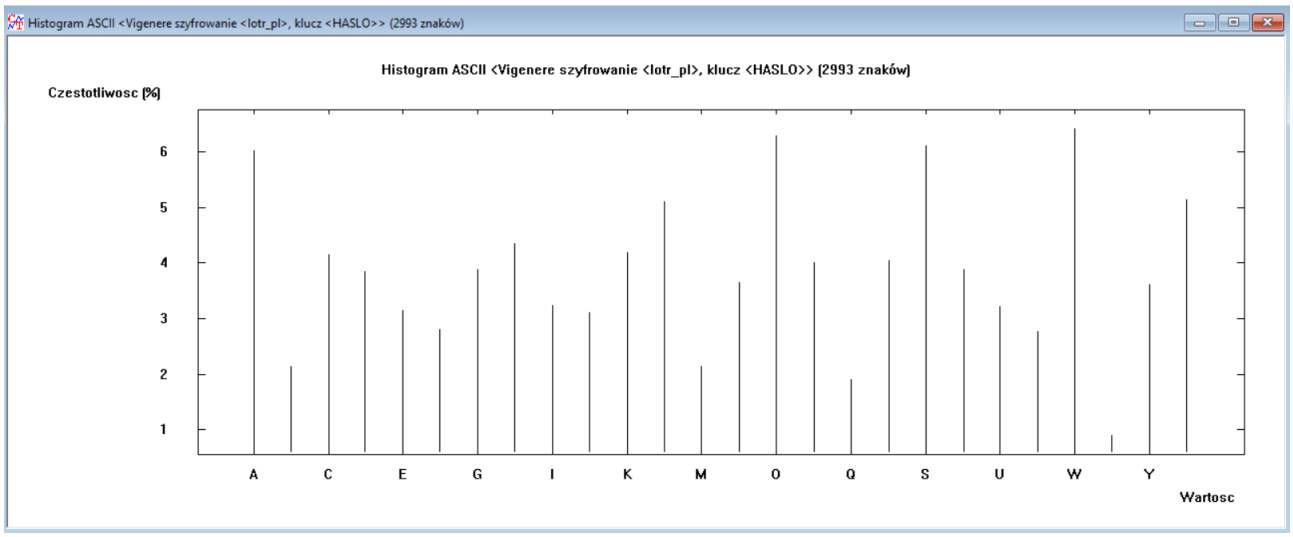


Algorytm Cezara, "D"



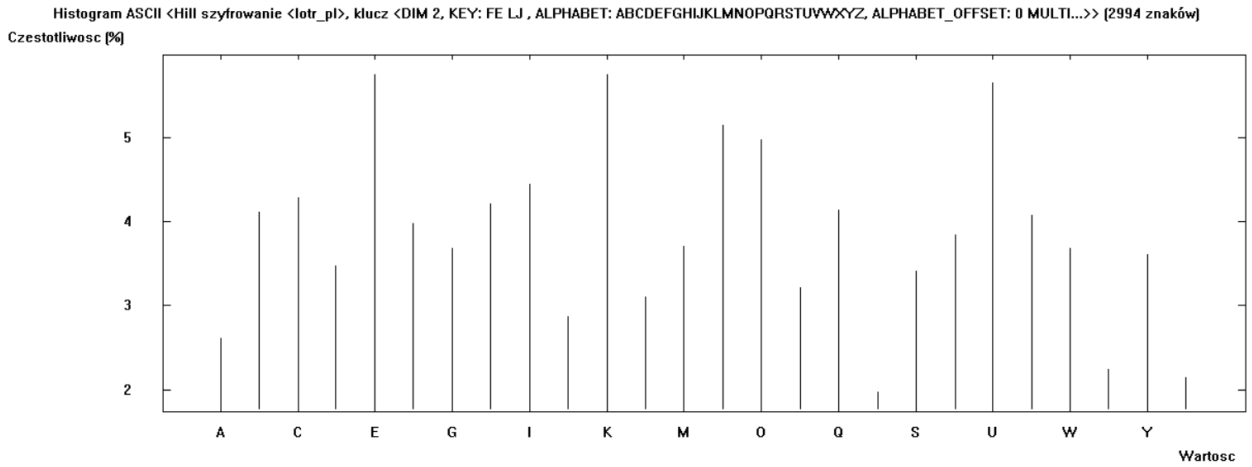
Jak widać powyżej, dla algorytmu cezara, histogram jest po prostu przesunięty.

Algorytm Vigenere, "HASLO"

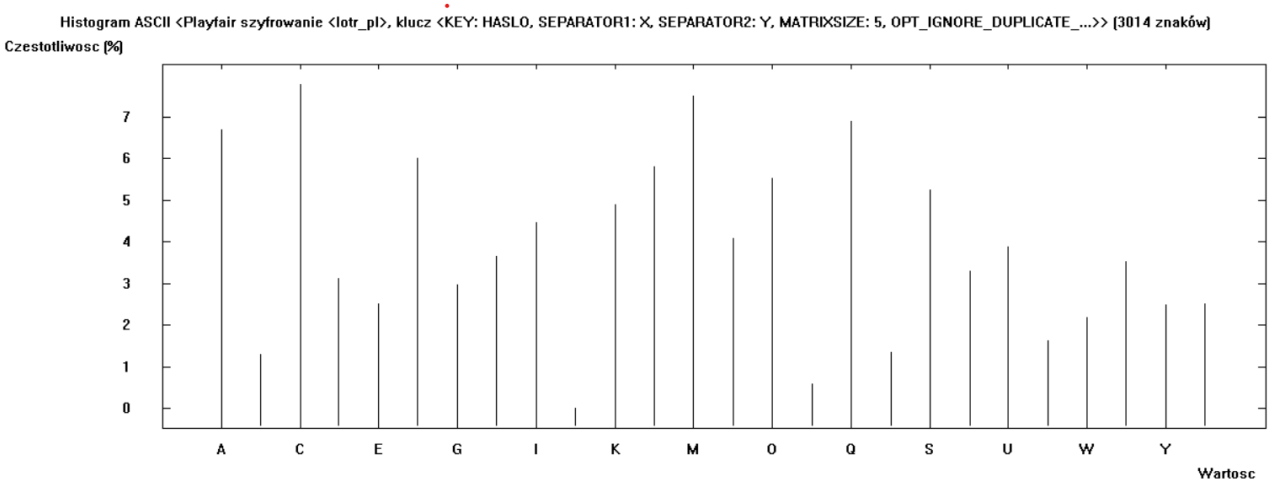


Histogram został lekko "spłaszczony", tendencje do powtarzania się znaków w języku zostają zatarte.

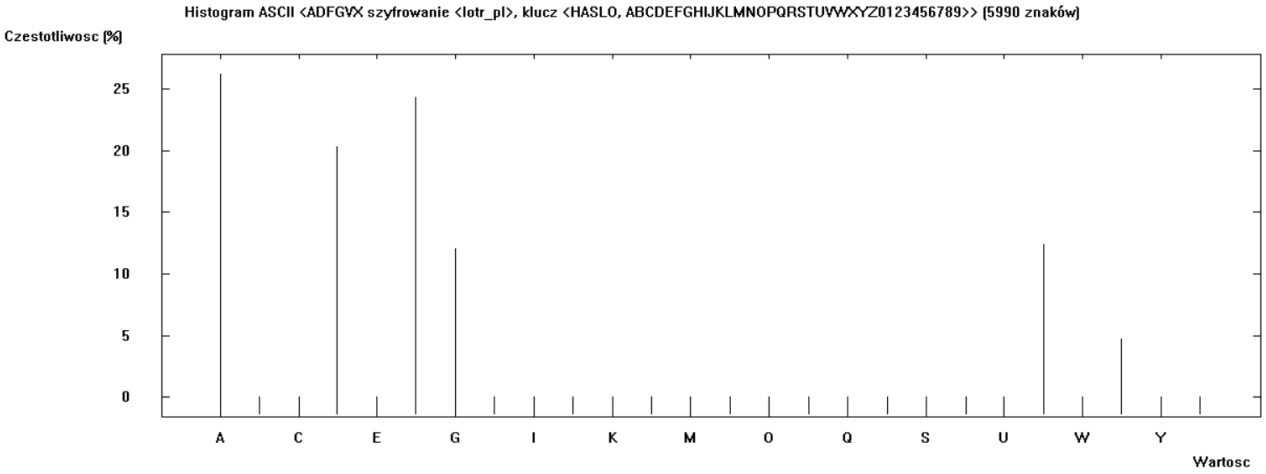
Algorytm Hilla, "FE LJ"



Algorytm Playfair, "HASLO"



Algorytm ADFGVX, "HASLO"



W zaszyfrowanym tekście występuje tylko 6 liter.

Zadanie 2.5

Porównaj n-gramów (bi / tri / n) tekstów jawnych dla wybranych 3 różnych języków (angielski, polski, niemiecki, francuski, włoski, hiszpański, ...)

Wszystkie wyniki przedstawiono w kolejności od najczęściej występującego

- **Język polski:**
  - Digramy: "IE", "NI", "CI", "ZE", "EN"
  - Trigramy: "CIE", "IEN", "SCI", "NIE", "DZI"
  - 4-znakowe: "CIEN", "ERSC", "DZIE"
- **Język angielski:**
  - Digramy: "TH", "HE", "IN", "RE", "ER"
  - Trigramy: "THE", "ING", "AND", "HER", "RIN"
  - 4-znakowe: "THIS", "RING", "HERE"
- **Język niemiecki:**
  - Digramy: "EN", "ER", "DE", "CH", "ND"
  - Trigramy: "EIN", "DER", "ICH", "SCH", "UND"
  - 4-znakowe: "RING", "EINE", "NDER", "ENDE", "ALLE"

Zadanie 2.6

Porównaj n-gramów (bi / tri / n) jednego tekstu jawnego i tekstu zaszyfrowanego w zależności od algorytmu z punktu 2.

- **Język polski:**

  - Digramy: "IE", "NI", "CI", "ZE", "EN"
  - Trigramy: "CIE", "IEN", "SCI", "NIE", "DZI"
  - 4-znakowe: "CIEN", "ERSC", "DZIE"
- **Szyfr Cezara**

  - Dla szyfru Cezara, wszystkie digramy zostaną przesuniętę o klucz. Nie zmieni się ani ich struktura, ani częstotliwość wystepowania.
- **Vigenere, "HASLO"**

  - Digramy: "PE", "WL", "TS"
  - Trigramy: "DOT", "SUT", "WLN"
  - 4-znakowe: "HCNL", "NWLN"
- **Vigenere, "TAJEMNEHASLO"**

  - Digramy: "UR"
  - Trigramy: Brak
  - 4-znakowe: Brak
- **Hill, "FE LJ"**

  - Digramy: "EU", "OK"
  - Trigramy: "IEU, "DDK", "PUI"
  - 4-znakowe: "DDKP","DKPU","KPUI"
- **Hill, "TCA HNR NOB"**

  Nie wykryto powtarzających się cząstek.
- **Playfair, "HASLO"**

  - Digramy: "MC", "GK"
  - Trigramy: Brak
  - 4-znakowe: Brak
- **ADFGVX, "HASLO"**

  - Digramy: "AA", "AF", "FA", "FF", "AD", "DA"
  - Trigramy: "AAA", "AAF", "FFF", "FAA", "AFA", "AFD"
  - 4-znakowe: "AAAA", "AAFD", "AAAF", "FAAF", "FFAA","GFFF"
- **Homofony**

  - Nie wykryto powtórzeń.

Zadanie 2.8

Jak zmieniają się obserwowane parametry w zadaniach od 1 do 7?

- **Entropia:**
  Największą entropię posiada język polski, następnie angielski, najmniejsza jest enropia niemieckiego.

  Po zaszyfrowaniu szyfrem Cezara, entropia pozostała niezmienna. Algorytm Vigenera znacząco zwiększył entropię tekstu już przy użyciu stosunkowo krótkiego hasła ("HASLO"). Zwiększenie długości hasła spowodowało dalsze zwiększenie entropii. Algorytm Hilla miał analogiczny wpływ na entropię. W przypadku szyfrowaniu Playfair, entropia również wzrosła. Szyfr ASFGVX, z powodu ograniczenia liczby znaków do zaledwie 6, spowodował drastyczne zmniejszenie entropii. Metoda homofonów, poprzez zwiększenie rozmiaru alfabetu spowodowała *znaczny* wzrost.

- **Histogram:**
  W języku polskim najczęściej występowały litery "a", "e", "i", "o". Język angielski również zdominowany jest przez samogłoski, zdecydowanie najczęściej pojawia się litera "e". Litery "a", "o", "t" również wybijają się ponad resztę, jednak nie tak zauważalnie. W języku niemieckim ewidentnie przeważa litera "e", często pojawia się również "i", "n", "t".

  Zaszyfrowanie metodą Cezara spowodowało jedynie przesunięcie histogramu. Vigenere oraz Hill spowodowały znaczące spłaszczenie histogramów. Po szyfrowaniu algorytmem Playfair, histogram również był trochę spłaszczony, jednak zauważalne są pewne tendencje. ADFGVX, zgodnie z zasadą algorytmu sprawił że na histogramie pojawia się jedynie 6 liter.

- **N-gramy:**
  Najczęsciej występujące n-gramy w językach to zazwyczaj popularne końcówki wyrazów, lub częste wyrazy. Różnią się w zależności od języka. Po zaszyfrowaniu algorytmem Cezara, n-gramy zmieniły swoją postać, jednak zachowały one częstotliwośc i pozycję w tekście. Pozostałe metody szyfrowania sprawiły że tendencja do powtarzania się n-gramów znacznie zmalała. W przypadku Hilla, powtarzalność malała wraz ze zwiększeniem klucza (macierzy). Szyfr ADFGVX wykazał najwięcej powtarzalnych cząstek co jest zgodne z jego naturą.

Zadanie 2.9

W jaki sposób można wykorzystać narzędzia analizy tekstu dostępne w CrypTool do określenia algorytmu szyfrowania dla danego zaszyfrowanego tekstu?

Można spróbować określić to korzystając z narzędzi krytptoanalizy dostępnych w programie.

- **Analiza entropii:**
  Jak wykazały eksperymenty, poziom entropii zaszyfrowanego tekstu może zasugerować jaka metoda została użyta. Jeśli entropia jest na poziome języka naturalnego, można spodziewać się że użyto algorytmu Cezara. Bardzo niska entropia sugeruje algorytm ADFGVX, bardzo wysoka homofonów. Podwyższona dość mocno entropia może oznaczać algorytm Playfair, Hilla, lub Vigenera.

- **Analiza histogramów:**
  Jeśli widzimy w histogramie wyraźnie wybijające się litery, może to oznaczać że to szyfr

Cezara. Płaskie histogramy - Hilla, Playfair lub Vigenere. Metoda ADFGVX będzie posiadała tylko 6 słupków w histogramie.

- **Analiza n-gramów:**
  Jeśli n-gram posiada znaczną ilość często występujących n-gramów, można spodziewać się że to algorytm Cezara, ADFGVX, lub Vigenere o krótkim haśle.

Zadanie 2.10

W jaki sposób można wykorzystać narzędzia analizy tekstu dostępne w programie CrypTool do ustalenia hasła używanego do szyfrowania?

W przypadku gdy histogram sugeruje algorytm Cezara, można przyrównać najczęściej występujące znaki i spróbować dopasować przesunięcie tak, żeby odpowiadały one samogłoskom (lub innym często występującym literom). Można również wykorzystać analizę częstotliwości występowania sekwencji znaków w tekście (n-gramów). Powtarzające się n-gramy w zaszyfrowanym tekście mogą dostarczyć wskazówek dotyczących użytego szyfru. Na przykład, w szyfrze Cezara, często występujące dwuliterowe n-gramy mogą pomóc w określeniu przesunięcia. Porównanie częstotliwości występowania n-gramów z tymi znanymi z danego języka pomaga w analizie.

Zadanie 3.1

Spróbuj rozpoznać, który algorytm szyfrowania został użyty, opierając się wyłącznie na analizie pliku z szyfrogramem. Wszystkie kryptogramy zostały utworzone na podstawie tego samego tekstu jawnego

- **Plik 1_1.txt:**
  Podwyższona entropia tekstu sugeruje że zastosowany został Vigenere, Playfair lub Hill. Na pewno nie jest to szyfr Cezara, ADFGVX, homofonów. W tekście brak również powtarzających się mocno n-gramów.
- **Plik 1_2.txt:**
  Pierwsze spojrzenie na entropię tekstu wykazało entropię normalną dla języka angielskiego. Następnie histogram - tutaj widać ewidentnie że "K" powtarza się bardziej niż posotałe litery. Sugeruje to szyfr Cezara i przesunięcie o 6 pozycji (najczęściej powinna występować litera "E"). Próba odszyfrowania szyfrem cezara o 6 pozycji spowodowała odszyfrowanie tekstu i potwierdzenie przypuszczeń.
- **Plik 1_3.txt:**
  Entropia wydaje się normalna. Sugeruje to szyfr monoalfabetyczny. Histogram sugeruje powtarzanie się jednej głoski znacznie więcej niż inne. Również analiza n-gramów wykazuje powtarzające się w sposób naturalny dla języka naturalnego wzorce. Pierwsze przypuszczenie pada na szyfr Cezara. Jednak nie udaje się przesunąć odpowiednio tekstu i odszyfrować. Następnie, po zagłębieniu się w możliwości cryptoola wygląda na to, że użyty został szyfr zamiany. Analizując histogram i podmieniając odopwiednie litery, a następnie przechodząc do n-gramów, przypuszczenia się potwierdziły.

Zadanie 3.4

Od czego zależy siła algorytmu?

Siła algorytmu zależy od wielu czynników. Między innymi:

- **Długość i złożoność klucza:** Im dłuższy klucz i bardziej złożony klucz, tym trudniej jest go odgadnąć poprzez próby typowania.
- **Przestrzeń kluczy:** Większa przestrzeń kluczy sprawia że szyfr jest znacznie bardziej odporny na ataki "brute force"
- **Zasłonięcie natury tekstu:** Algorytm powinien ukryć jak najwięcej cech charakterystycznych tekstu. Nie powinien dawać wskazówek w postaci powtarzających się liter lub n-gramów.
- **Złożoność operacji:** Wraz z przestrzenią kluczy warto zwiększyć poziom złożoności operacji potrzebnych do odszsyfrowania.

Zadanie 3.5

W jaki sposób można zwiększyć siłę szyfrowania znanych szyfrów?

Podstawowym sposobem na zwiększenie siły znanych szyfrów jest zwiększenie długości hasła. Dobrze także wzbogacić jego losowość i wybranie nieoczywistego hasła. Rozsądne wydaje się także nałożenie na zaszyfrowaną wiadomość innego szyfru (innego niż już użyty), w celu dalszego zatarcia natury wiadomości oraz zwiększenia złożoności.