* 1. **Ćwiczenia do wykonania w trakcie zajęć.**

1. Za pomocą prostych obliczeń matematycznych, rozszyfrować poniższy szyfrogram w którym zastosowano metodę **Cezara**. Tekst jawny jest zapisany w języku angielskim.

Ecguct ekrjgt

Po rozszyfrowaniu poprawność tekstu jawnego potwierdzić za pomocą programu CrypTool.

1. Wykorzystując znany szyfrogram (tekst udostępniony poniżej) w którym zastosowano szyfrowanie metodą **Vigenera**. Za pomocą programu CrypTool przeprowadzić proces kryptoanalizy uzyskując tekst jawny oraz klucz. Wyjaśnić poszczególne procesy analizy przedstawione przez program.

|  |
| --- |
| Mepcbyc Olrdcilirkc - Jk fv, hp dkx kh zu (bvff Fqipvm 3/1)  Re xi, fk lep xf uc: jdek bq jdi hncipmfg:  Uxaxyxp 'jew ehzbav zg rxa qzgb jk wlydun  Xyx qberxl ydz eikmmo sw hsjnexxmko jfkrkji,  Fk re pebx yhiw rzyyjwk t quw sw mpeqfcxq,  Qjh sr mflsjblw aru mfui? Xf wgu: ps jecul;  Rf fmha; eew zo w wcxcf ps jtw ma iew  Rxa lvtpj-wgyx ydz xyx rxkyjtlt jeknpqh wyhaao  Xytr vhija gi dizk re, 'pmj t aejwlfkqpmfg  Burslmjo ps sx uyol'u. Mm tei, kh qbaig; |

1. Wypełnić tabele, według podanych wskazówek.

Metodę szyfrowania **Solitaire** można w skrócie opisać za pomocą równania:

(X+Y) mod 26 = Z

Gdzie: X - wartości liter tekstu jawnego

Y - wartości strumienia klucza

Z – wartość liter szyfrogramu

Przykładowa wiadomość do zaszyfrowania: TAJNA WIADOMOSC

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Tekst jawny** | T | A | J | N | A | W | I | A | D | O | M | O | S | C |
| **X** | 20 |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Y** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| **Z** | 21 |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Szyfrogram** | U |  |  |  |  |  |  |  |  |  |  |  |  |  |

Do wyznaczania wartości poszczególnych liter należy skorzystać z alfabetu łacińskiego zamieszczonego w tabeli poniżej.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Znak** | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| **Nr** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |

Proces deszyfrowania jest metodą odwrotna do szyfrowania. Można ją opisać za pomocą równania:

(X-Y) mod 26 = Z

Gdzie: X - wartości liter szyfrogramu

Y - wartości strumienia klucza

Z – wartość liter tekstu jawnego

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Szyfrogram** | U | C | M | R | F | C | P | I | M | Y | X | A | F | Q |
| **X** | 21 |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Y** | 1 |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Z** | 20 |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Tekst jawny** | T |  |  |  |  |  |  |  |  |  |  |  |  |  |

Po zakończeniu zadania, przećwiczyć metodę szyfrowania i deszyfrowania w oparciu o program CrypTool.

1. Za pomocą programu CrypTool należy poddać kryptoanalizie tekst zamieszczony poniżej. Jest to rozszerzona wersja tekstu przedstawionego w podpunkcie b). W tym przypadku zastosowano szyfrowanie **metodą zamiany**. Proces deszyfrowania można przeprowadzić na dwa sposoby: na podstawie częstotliwości występowania diagramów lub najczęściej występujących słów w danym języku. Jeśli nie uda się rozszyfrować całego tekstu jedną z wymienionych metod, w oparciu o rozszyfrowaną w podpunkcie b) część tekstu stosując w programie analizę manualna, dokończyć proces deszyfrowania.

|  |
| --- |
| Gl yv li mlg gl yv gszg rh gsv jfvhgrlm  Dsvgsvi grh mlyovi rm gsv nrmw gl hfuuvi  Gsv hormth zmw ziildh lu lfgiztvlfh uligfmv  Li gl gzpv zinh ztzrmhg z hvz lu gilfyovh  Zmw yb lkklhrmt vmw gsvn Gl wrv gl hovvk  Ml nliv zmw yb z hovvk gl hzb dv vmw  Gsv svzig zmw gsv gslfhzmw mzgfizo hslxph  Gszg uovhs rh svri gl rh z xlmhfnnzgrlm  Wvelfgob gl yv drhs Gl wrv gl hovvk  Gl hovvk kvixszmxv gl wivzn z gsviv gsv ify  Uli rm gszg hovvk lu wvzgs dszg wivznh nzb xlnv  Dsvm dv szev hsfuuovw luu gsrh nligzo xlro  Nfhg trev fh kzfhv gsviv gsv ivhkvxg  Gszg nzpvh xzoznrgb lu hl olmt oruv  Uli dsl dlfow yvzi gsv dsrkh zmw hxlimh lu grnv  Gsv lkkivhhli dilmt gsv kilfw nzm xlmgfnvob  Gsv kzmth lu wvhkrhvw olev gsv ozd wvozb  Gsv rmhlovmxv lu luurxv zmw gsv hkfimh  Gszg kzgrvmg nvirg lu gsv fmdligsb gzpvh  Dsvm sv srnhvou nrtsg srh jfrvgfh nzpv  Drgs z yziv ylwprm dsl dlfow uziwvoh yvzi  Gl tifmg zmw hdvzg fmwvi z dvzib oruv  Yfg gszg gsv wivzw lu hlnvgsrmt zugvi wvzgs  Gsv fmwrhxlevi xlfmgib uiln dslhv ylfim  Ml gizevoovi ivgfimh kfaaovh gsv droo  Zmw nzpvh fh izgsvi yvzi gslhv rooh dv szev  Gszm uob gl lgsvih gszg dv pmld mlg lu  Gsfh xlmhxrvmxv wlvh nzpv xldziwh lu fh zoo  Zmw gsfh gsv mzgrev sfv lu ivhlofgrlm  Rh hrxporvw li drgs gsv kzov xzhg lu gslftsg  Zmw vmgvikirhvh lu tivzg krgs zmw nlnvmg  Drgs gsrh ivtziw gsvri xfiivmgh gfim zdib  Zmw olhv gsv mznv lu zxgrlm Hlug blf mld  Gsv uzri Lksvorz Mbnks rm gsb lirhlmh  Yv zoo nb hrmh ivnvnyvi |

1. Przeprowadzić analizę w programie CrypTool, dwóch metod kryptograficznych (**Xor** i **Dodawanie**) przeanalizować procesy wykonane przez program oraz porównać wynik końcowy. Jeśli będzie to wymagane, proces kryptoanalizy dokończyć metodą manualną.

|  |  |
| --- | --- |
| **Szyfrogram (XOR)** | **Szyfrogram (Dodawanie)** |
| Më9ć|¨9ëk¤wëm¤më9ć|ľ9đqĺm¤p÷9đqá9őlájđpëwľŽNě|đqák¤>đp÷9ęvćuák¤pę9đqá9épę}¤më9÷lâák‰Đqá9÷uíwăj¤xę}¤xökën÷9ë¤vńmöxă|ël÷9âvömńwá5‰Ëk¤më9đxď|¤xöt÷9ĺ~ĺpęjđ9ĺ9÷|ĺ9ë¤mövń{č|÷5‰Ĺwŕ9ć`¤vôiëjíwă9áwŕ9đqát»9Đv¤}í|ľ9đv¤jč|áiżŽWë9évö|ż9ĺwŕ9ć`¤x¤jč|ái¤më9÷xý9ó|¤|ę}‰Đqá9ě|ĺkđ4ĺzě|¤xę}¤mě|¤měvńjĺwŕ9ęxđlöxč9÷qëzďj‰Đqĺm¤č|÷q¤p÷9ě|ík¤më5¤>đp÷9ĺ9çvęjńtéxđpëw‰Ŕ|ňvńmč`¤më9ć|¤níjě>ŕ7¤Më9ŕpá5¤më9÷uá|ô"‰Đv¤jč|áiľ9ô|özěxęzá9đv¤}ö|ĺtľ9ĺ`¨9đqáká>÷9đqá9ölć"‰Âvö9íw¤měxđ9÷uá|ô9ë¤}áxđq¤něxđ9ŕkáxéj¤tĺ`¤zëtáŽNě|ę9ó|¤qĺoá9÷qńâuá}¤vâ¤měp÷9évömĺu¤zëpč5‰Él÷m¤~íoá9ńj¤iĺl÷|ľ9đqáká>÷9đqá9ö|÷iázđŽMěxđ9éxď|÷9çxčxépđ`¤vâ9÷v¤uëwă9čpâ|żŽ\_ëk¤něv¤nëlč}¤{áxö9đqá9óqíi÷9ĺwŕ9÷zëkęj¤vâ9đpé|¨ŽMě|¤vôiö|÷jëkŁj¤növę~¨9đqá9ôkëlŕ9éxę>÷9çvęmńtáuý5‰Đqá9ôxę~÷9ë¤}ájôp÷|ŕ9čvň|¨9đqá9čxó>÷9ŕ|čxý5‰Đqá9íw÷vč|ęzá9ë¤vâízá9ĺwŕ9đqá9÷ińkęj‰Đqĺm¤iĺmí|ęm¤tákím¤vâ9đqá9ńwóvömě`¤mĺráj¨ŽNě|ę9ě|¤qít÷|č¤tí~ěm¤qíj¤hńpámńj¤tĺráŽNímě9ĺ9ćxö|¤{ë}ďpę&¤něv¤nëlč}¤ĺkŕ|čj¤{áxö5‰Đv¤~ölęm¤xę}¤jó|ĺm¤lę}ák¤x¤náxö`¤uíá5‰Ćlđ9đqĺm¤mě|¤}ö|ĺ}¤vâ9÷vé|đqíwă9ĺđ|ö9ŕ|ĺmě5‰Đqá9ńwŕp÷zëoákŁ}¤zëlęmö`¤övé9óqëjá9ćvńkęŽWë9đkĺoáuč|ö9ö|đlöw÷5¤ińcţuáj¤mě|¤níučŽXę}¤tĺráj¤l÷9öxđqák¤{áxö9đqëjá9íučj¤ná9ěxň|‰Đqĺw¤č`¤më9ëmě|öj¤měxđ9ó|¤ręvó9ęvđ9ë»ŽMěl÷9çvęjçpáwç|¤}ë|÷9éxď|¤zënĺkŕj¤vâ9ńj¤xčużŽXę}¤měl÷9đqá9ęxđpň|¤qń|¤vâ9ö|÷včlđpëw‰Íj¤jízďuí|ŕ9ë>ák¤nímě9đqá9ôxč|¤zĺjđ9ë¤měvń~ěm¨ŽXę}¤|ęmákôkíjáj¤vâ9ăkáxđ9ôpđq¤xę}¤tëtáwđŽNímě9đqíj¤ká~ĺkŕ9đqápö9çlökáwđj¤mńkę9ĺnö`¨ŽXę}¤uëjá9đqá9ęxé|¤vâ9ĺzđpëwŞ9©9×vâm¤`ël¤wënĄŽMě|¤ĺpö9Ëiě|čpĺ8¤Wýtôq¨9íw¤mě`¤vöp÷vęj‰Ć|¤xču¤tý9÷pęj¤kátátć|ö>ŕ7 | mó9ć~°9ó‹¤‡óŤ¤Ťó9ć~ľ9řĺŤ¤‚÷9řé9őŽéŚř‚ó‡ľ&Žpě~řé‹¤@ř‚÷9ňć…é‹¤‚ň9řé9ń‚ň}¤Ťó9÷Žęé‹‘#Řé9÷…í‡ëŚ¤zň}¤zö‹ó÷9ó¤ůŤözë~óŽ÷9ęöŤů‡éE‘#Ó‹¤Ťó9řzď~¤zö†÷9ĺ€ĺ‚ňŚř9ĺ9÷~ĺ9ó¤Ťöů{đ~÷E‘#Ĺ‡č9ć’¤ô‰óŚí‡ë9é‡č9řé†Ă9Ř¤}í~ľ9ř¤Śđ~é‰ż&Žgó9ńö~ż9ĺ‡č9ć’¤z¤Śđ~é‰¤Ťó9÷zý9ű~¤~ň}‘#Řé9ě~ĺ‹řFĺ|ě~¤zň}¤Ťě~¤ŤěůŚĺ‡č9ňzřŽözđ9÷ó|ďŚ‘#ŘĺŤ¤đ~÷¤‚÷9ě~í‹¤ŤóE¤@ř‚÷9ĺ9çňŚů†ńzř‚ó‡‘#Č~úůŤđ’¤Ťó9ć~¤íŚě@čG¤mó9č‚éE¤Ťó9÷…é~ôT‘#Ř¤Śđ~é‰ľ9ô~ö|ězň|é9ř¤}ö~ĺ†ľ9ĺ’°9řé‹é@÷9řé9öŽćT‘#Ęö9í‡¤Ťězř9÷…é~ô9ó¤}ézř¤ězř9č‹ézńŚ¤†ĺ’¤|ó†é&Žpě~ň9ű~¤ĺŹé9÷ůę…é}¤ę¤Ťě‚÷9ńöŤĺ…¤|ó‚đE‘#ŃŽ÷Ť¤€íŹé9ůŚ¤‰ĺŽ÷~ľ9řé‹é@÷9řé9ö~÷‰é|ř&Žmězř9ńzď~÷9çzđzń‚ř’¤ę9÷¤…ó‡ë9đ‚ę~ż&Ž\_ó‹¤ě¤óŽđ}¤{ézö9řé9űí‰÷9ĺ‡č9÷|ó‹ňŚ¤ę9ř‚ń~°&Žmě~¤ô‰ö~÷Śó‹«Ś¤öň€°9řé9ô‹óŽč9ńzň@÷9çňŤů†é…ýE‘#Řé9ôzň€÷9ó¤}éŚô‚÷~č9đú~°9řé9đzű@÷9č~đzýE‘#Řé9í‡÷đ~ň|é9ó¤ęí|é9ĺ‡č9řé9÷‰ů‹ňŚ‘#ŘĺŤ¤‰ĺŤí~ňŤ¤†é‹íŤ¤ę9řé9ů‡űöŤě’¤Ťĺ„éŚ°&Žpě~ň9ě~¤í†÷~đ¤†í€ěŤ¤íŚ¤Šů‚éŤůŚ¤†ĺ„é&ŽpíŤě9ĺ9ćzö~¤{ó}ď‚ňX¤ě¤óŽđ}¤ĺ‹č~đŚ¤{ézöE‘#Ř¤€öŽňŤ¤zň}¤Śű~ĺŤ¤Žň}é‹¤z¤ézö’¤…íéE‘#ĆŽř9řĺŤ¤Ťě~¤}ö~ĺ}¤ę9÷ń~ří‡ë9ĺř~ö9č~ĺŤěE‘#Řé9ů‡č‚÷|óŹé‹«}¤|óŽňŤö’¤öń9űóŚé9ćů‹ň&Žgó9ř‹ĺŹé…đ~ö9ö~řŽö‡÷E¤‰ů“ţ…éŚ¤Ťě~¤í…đ&ŽZň}¤†ĺ„éŚ¤Ž÷9özřé‹¤{ézö9řóŚé9í…đŚ¤é9ězú~‘#Řĺ‡¤đ’¤Ťó9óŤě~öŚ¤Ťězř9ű~¤„ňű9ňř9óĂ&ŽměŽ÷9çňŚç‚é‡ç~¤}ó~÷9ńzď~¤|óĺ‹čŚ¤ę9ůŚ¤zđ…ż&ŽZň}¤ŤěŽ÷9řé9ňzř‚ú~¤ů~¤ę9ö~÷đŽř‚ó‡‘#ÍŚ¤Śí|ď…í~č9ó@é‹¤íŤě9řé9ôzđ~¤|ĺŚř9ó¤Ťěů€ěŤ°&ŽZň}¤~ňŤé‹ô‹íŚéŚ¤ę9ë‹ézř9ô‚ř¤zň}¤†ó†é‡ř&ŽpíŤě9říŚ¤‹é€ĺ‹č9řé‚ö9çŽö‹é‡řŚ¤Ťů‹ň9ĺö’°&ŽZň}¤…óŚé9řé9ňzń~¤ę9ĺ|ř‚ó‡˛9±9×ęŤ¤’óŽ¤‡óĄ&Žmě~¤ĺ‚ö9Ó‰ě~đ‚ĺ:¤gý†ô°9í‡¤Ťě’¤ö‚÷ňŚ‘#Ć~¤zđ…¤†ý9÷‚ňŚ¤‹é†é†ć~ö@ |

1. Sprawdzić prawidłowość poniższych szyfrogramów. Przedstawić macierze kluczy dla znaków i wartości liczbowych.

|  |  |  |  |
| --- | --- | --- | --- |
| **Tekst jawny** | **Szyfrogram (Hill)** | | |
| **Macierz 1x1** | **Macierz 3x3** | **Macierz 5x5** |
| In classical cryptography, the Hill cipher is a polygraphic substitution cipher based on linear algebra. Invented by Lester S. Hill in 1929, it was the first polygraphic cipher in which it was practical (though barely) to operate on more than three symbols at once. The following discussion assumes an elementary knowledge of matrices. | Un svaggusav sxifpwcxafli, plk Luvv suflkx ug a fwvicxaflus gyjgpupypuwn suflkx jagkb wn vunkax avckjxa. Unhknpkb ji Vkgpkx G. Luvv un 1929, up qag plk tuxgp fwvicxaflus suflkx un qlusl up qag fxaspusav (plwycl jaxkvi) pw wfkxapk wn ewxk plan plxkk giejwvg ap wnsk. Plk twvvwqunc bugsygguwn aggyekg an kvkeknpaxi mnwqvkbck wt eapxuskg. | Yf nujmswkwv hvlguxczporv, gdn Shdb jkodvc iq s vlitcwrhpco ykvrvleuxbqd fpnnhr dkiyl ba xvazoq wtlbdhd. Qgtbonly zb Gjkmup H. Ltmx va 1929, kh fxu adb qgftw ibqlszpoyrq jkodvc yv hyrql pu oog oqjsdztwe (gsvhea dpuinp) ut kbbamxp ql pyxx gmhz cfujg ykgfhsp ei qdfl. Frw thqunrauy nzgoemaeqr dmuqsis al rchwznfijb ehfkrxijy av jzxpcikc.UC | Wy tlvgoumeq dxgdqmkwhkpk, kyv Uxff nrnkke dh n hgtealtzybb dqkrgocrbjwp imhaok bfncc fw dndidt zzedxef. Hqoyivht ti Mcyixx Z. Swsx pn 1929, hl irg hyp proxh lgtealtzybb nrnkke nv cldac xw mpl vemicvagk (dahzhb moifdi) dl kehywtk qj zoov gzmc pzrrr lfsenhj mq jdhq. Dsh lhputhksn ddgowqqcao vseymwk yi xvtbtleiqm webcqhblc mi nygqnbuc.UEOU |

1. Na podstawie poniższego szyfrogramu zaproponować rodzaj szyfrowania jaki został w nim zastosowany. Tekst jawny jest w języku angielskim a pierwszy wyraz brzmi: Cryptoanalysis . Za pomocą programu CrypTool, używając opcji analizy manualnej (jednej z wybranych metod szyfrowania) należy rozszyfrować wiadomość.

|  |
| --- |
| Xibkglzmzobhrh rh z hbmlmbn uli xlwvyivzprmt zmw ivuvih gl gsv kizxgrxv lu zmzobarmt xrksvigvcg drgs gsv rmgvmg lu yivzprmt rg li xizxprmt gsv xlwv. Xibkglzmzobhrh rh gsv hgfwb lu dzbh gszg xzm yv fhvw gl lygzrm kozrmgvcg rmulinzgrlm uiln vmxibkgvw rmulinzgrlm drgslfg fhrmt gsv rmgvmwvw nvgslw hfxs zh fhrmt z pvb gl wvxibkg gsv rmulinzgrlm.  Xibkglzmzobhrh zggvnkgh gl zggzxp dvzpmvhhvh rm gsv nvgslwh fhvw gl vmxibkg xlwv li gsv nvgslwh fhvw gl tvmvizgv pvbh.  Gsviv ziv hvevizo xibkglzmzobhrh nvgslwh rmxofwrmt.  Ormvzi xibkglzmzobhrh rh z kozrmgvcg zggzxp dsrxs fhvh ormvzi zkkilcrnzgrlm gl wvgvinrmv gsv yvszerli lu gsv yolxp xrksvi. Ru vmlfts kozrmgvhg zmw nzgxsrmt xrksvigvhg ziv lygzrmvw, rmulinzgrlm zylfg gsv pvb xzm vevmgfzoob yv wrhxlevivw. Rg szh yvvm fhvw hfxxvhhufoob ztzrmhg UVZO zmw WVH.  Wruuvivmgrzo xibkglzmzobhrh rh yzhrxzoob z kozrmgvcg zggzxp fhrmt xslhvm kozrmgvhg zmw wvkvmwh lm zm zmzobhrh lu gsv wruuvivmxvh yvgdvvm gdl ivozgvw kozrmgvcgh zh gsvb ziv vmxibkgvw fhrmt gsv hznv pvb. Yb xzivufoob zmzobarmt gsv wzgz gsv kilyzyrorgb lu klhhryov pvbh yvrmt fhvw gl vmxibkg gsv wzgz xzm yv xzoxfozgvw zmw gsv xliivxg pvb xzm yv vevmgfzoob rwvmgrurvw. |