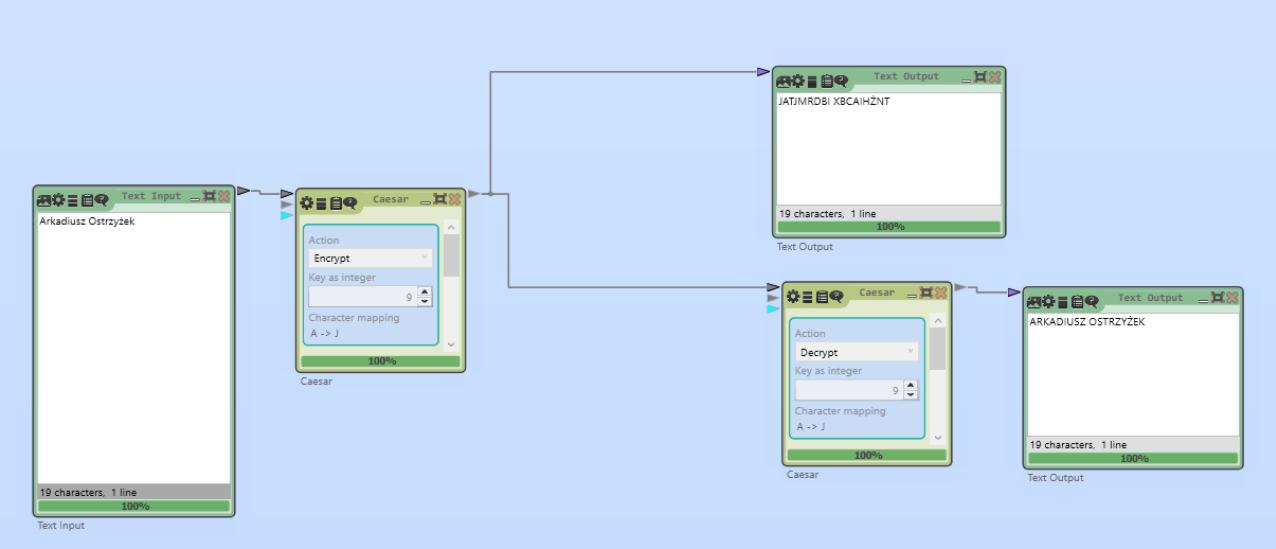
Arkadiusz Ostrzyżek
WCY22KY2S1
Zadanie 1

1. Szyfr przesuwający – szyfr Cezara

Szyfr Cezara to prosty szyfr przesuwający, w którym litery tekstu są zastępowane przez litery przesunięte o stałą liczbę pozycji w alfabecie. Jest to jeden z najprostszych szyfrów substytucyjnych używanych do szyfrowania tekstu. Odszyfrowanie polega na przesunięciu liter wstecz o tę samą liczbę pozycji.

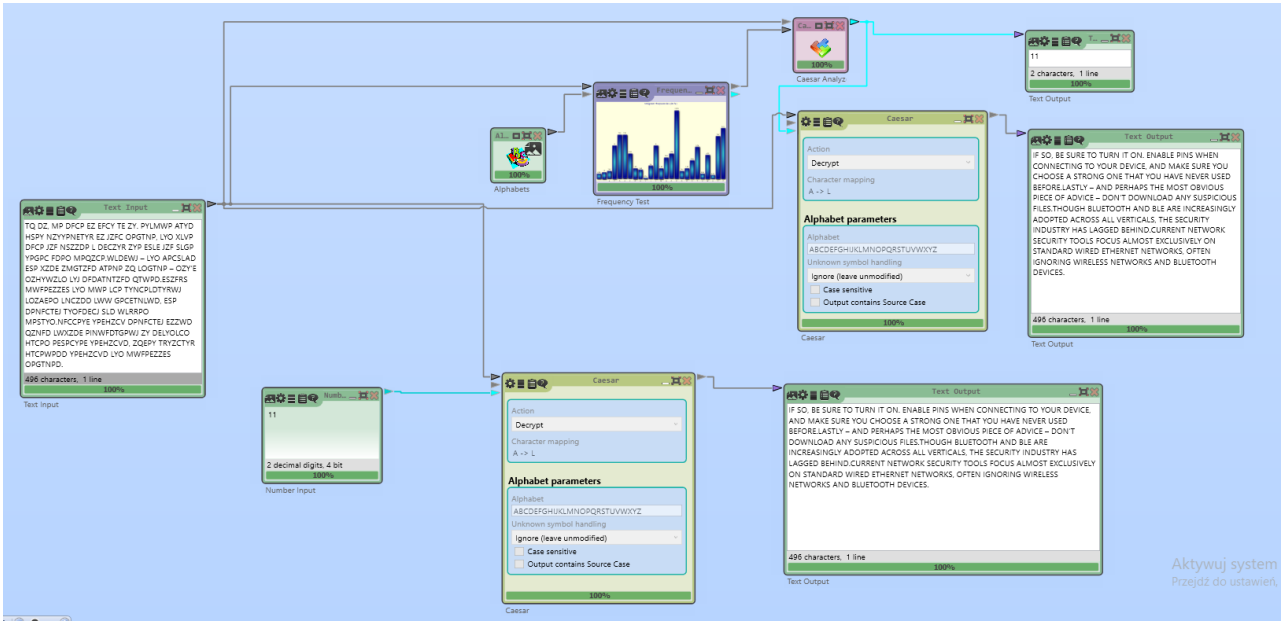
W programie CryptTool 2.1:

a) opracuj model realizujący szyfrowanie i deszyfrowanie wybranego tekstu jawnego szyfrem przesuwającym, a następnie zaszyfruj i odszyfruj swoje imię i nazwisko używając jako klucza swojego numeru w grupie,



tekst jawny: Arkadiusz Ostrzyżek
klucz: 9
tekst zaszyfrowany: JATJMRDBI XBCAIHŻNT

b) opracuj dwa modele realizujące kryptoanalizę szyfru przesuwającego, a następnie przeprowadź ataki na szyfrogram podany w załączonym pliku pod numerem równym swojemu numerowi w grupie.



Dwa sposoby ataku:
- brute force
- frequency analyzer

Klucz uzyskany w wyniku kryptoanalizy: 11

Tekst jawny:

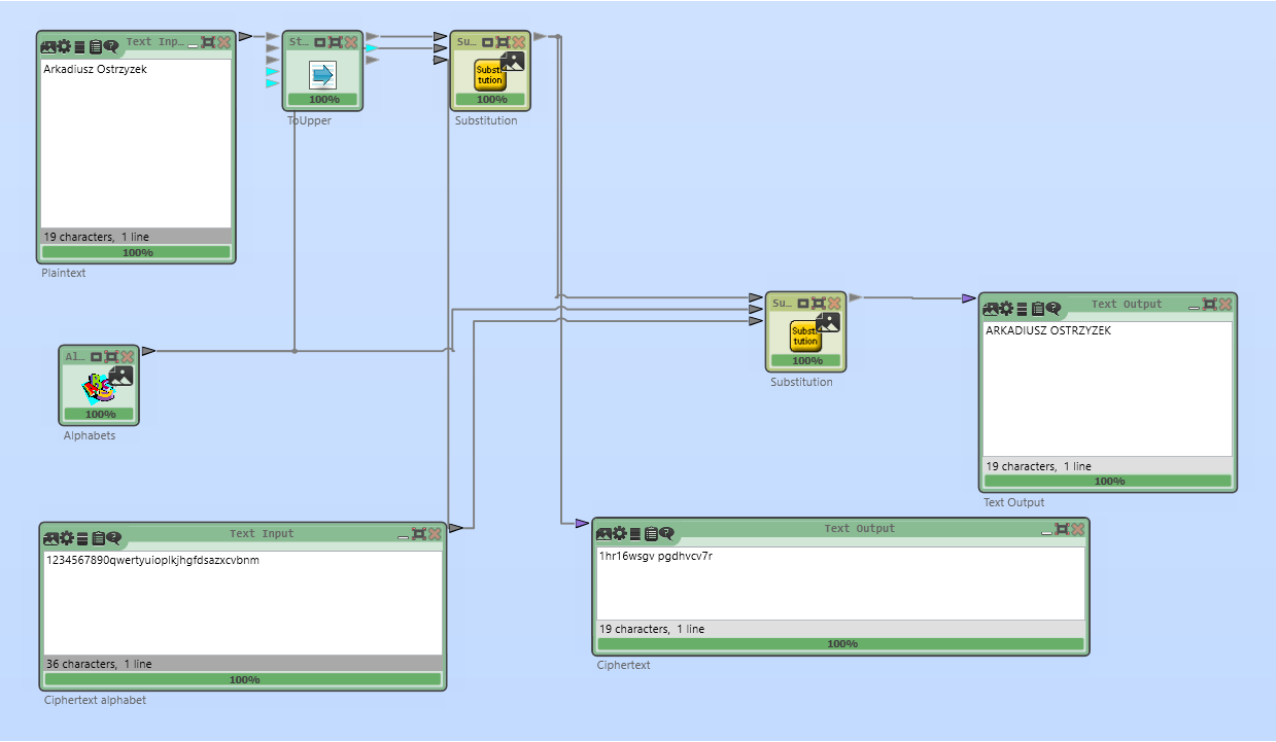
IF SO, BE SURE TO TURN IT ON. ENABLE PINS WHEN CONNECTING TO YOUR DEVICE, AND MAKE SURE YOU CHOOSE A STRONG ONE THAT YOU HAVE NEVER USED BEFORE.LASTLY – AND PERHAPS THE MOST OBVIOUS PIECE OF ADVICE – DON'T DOWNLOAD ANY SUSPICIOUS FILES.THOUGH BLUETOOTH AND BLE ARE INCREASINGLY ADOPTED ACROSS ALL VERTICALS, THE SECURITY INDUSTRY HAS LAGGED BEHIND.CURRENT NETWORK SECURITY TOOLS FOCUS ALMOST EXCLUSIVELY ON STANDARD WIRED ETHERNET NETWORKS, OFTEN IGNORING WIRELESS NETWORKS AND BLUETOOTH DEVICES.

2. Szyfr podstawieniowy – monoalfabetyczny

Szyfr monoalfabetyczny to rodzaj szyfru, w którym każda litera alfabetu jest zastępowana przez jedną, stałą literę z innego alfabetu. Oznacza to, że ta sama litera w oryginalnym tekście zawsze jest zastępowana tą samą literą w zaszyfrowanym tekście.

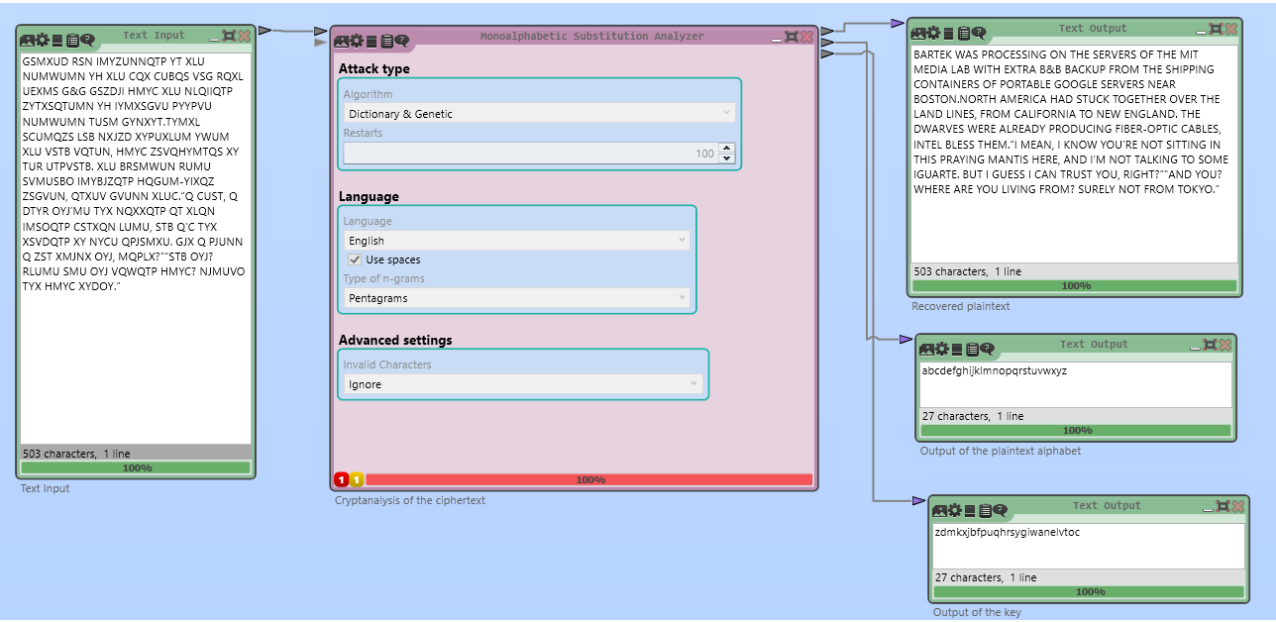
W programie CryptTool 2.1:

a) opracuj model realizujący szyfrowanie i deszyfrowanie wybranego tekstu jawnego monoalfabetycznym szyfrem podstawieniowym, a następnie zaszyfruj i odszyfruj swoje imię i nazwisko używając jako klucza dowolnej permutacji alfabetu,



tekst jawny: Arkadiusz Ostrzyżek
klucz: 1234567890qwertyuioplkjhgfdsazxcvbnm
tekst zaszyfrowany: 1hr16wsgv pgdhvcv7r

b) opracuj model realizujący kryptoanalizę monoalfabetycznego szyfru podstawieniowego, a następnie przeprowadź atak na szyfrogram podany w załączonym pliku pod numerem równym swojemu numerowi w grupie.



Klucz uzyskany w wyniku kryptoanalizy: zdmkxjbfpuqhrsygiwanelvtoc

Tekst jawny:

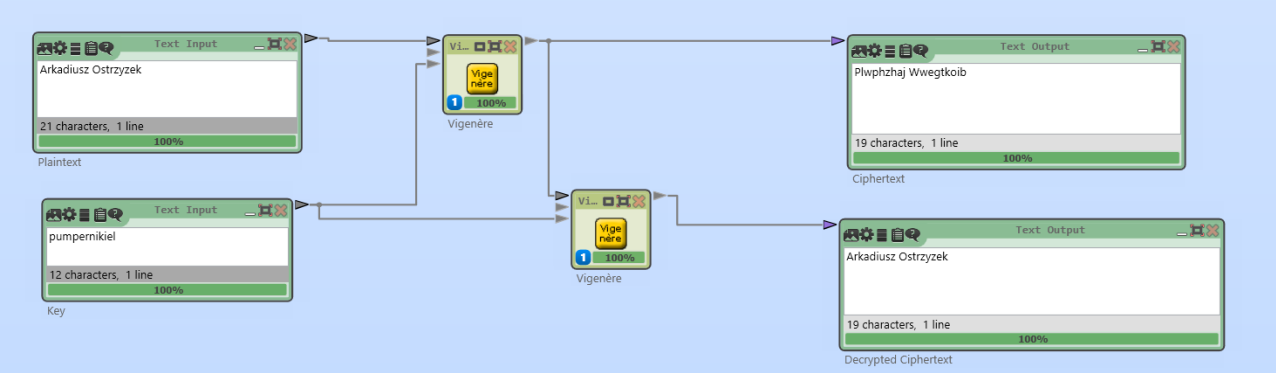
BARTEK WAS PROCESSING ON THE SERVERS OF THE MIT MEDIA LAB WITH EXTRA B&B BACKUP FROM THE SHIPPING CONTAINERS OF PORTABLE GOOGLE SERVERS NEAR BOSTON.NORTH AMERICA HAD STUCK TOGETHER OVER THE LAND LINES, FROM CALIFORNIA TO NEW ENGLAND. THE DWARVES WERE ALREADY PRODUCING FIBER-OPTIC CABLES, INTEL BLESS THEM.“I MEAN, I KNOW YOU’RE NOT SITTING IN THIS PRAYING MANTIS HERE, AND I’M NOT TALKING TO SOME IGUARTE. BUT I GUESS I CAN TRUST YOU, RIGHT?”“AND YOU? WHERE ARE YOU LIVING FROM? SURELY NOT FROM TOKYO.”

3. Szyfr podstawieniowy polialfabetyczny – szyfr Vigenera’a

Szyfr Vigenère'a to szyfr w którym każda litera tekstu jawnego jest zastępowana przez literę zależną od klucza i pozycji litery w tekście. Klucz jest powtarzany cyklicznie, aby dopasować go do długości tekstu.

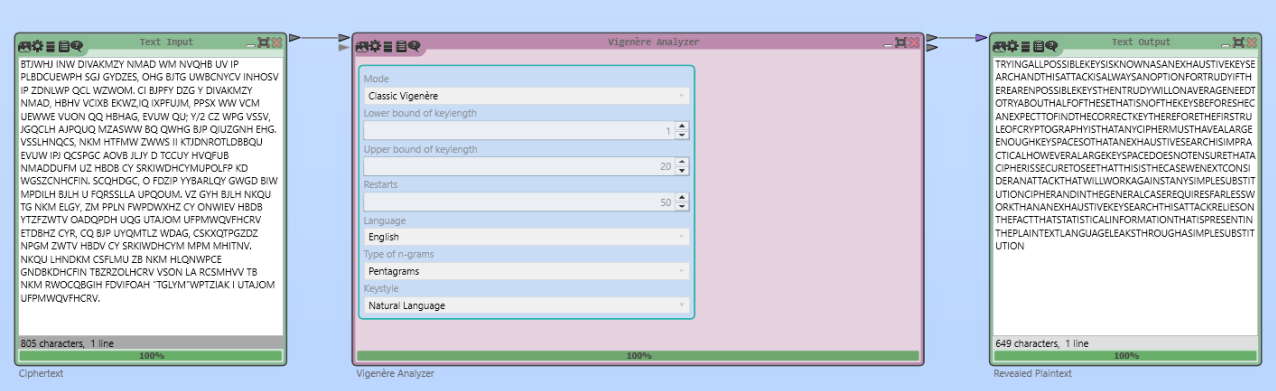
W programie CryptTool 2.1:

a) opracuj model realizujący szyfrowanie i deszyfrowanie wybranego tekstu jawnego szyfrem Vigenera, a następnie zaszyfruj i odszyfruj swoje imię i nazwisko używając jako klucza dowolnego słowa,



tekst jawny: Arkadiusz Ostrzyzek
klucz: 9
tekst zaszyfrowany: Plwphzhaj Wwegtkoib

b) opracuj model realizujący kryptoanalizę szyfru Vigenera, a następnie przeprowadź atak na szyfrogram podany w załączonym pliku pod numerem równym swojemu numerowi w grupie.



Klucz uzyskany w wyniku kryptoanalizy: 11

Tekst jawny:

TRYINGALLPOSSIBLEKEYSISKNOWNASANEXHAUSTIVEKEYSEARCHANDTHISATTACKISALWAYSANOPTIONFORTRUDYIFTHEREARENPOSSIBLEKEYSTHENTRUDYWILLONAVERAGENEEDTOTRYABOUTHALFOFTHESETHATISNOFTHEKEYSBEFORESHECANEXPECTTOFINDTHECORRECTKEYTHEREFORETHEFIRSTRULEOFCRYPTOGRAPHYISTHATANYCIPHERMUSTHAVEALARGEENOUGHKEYSPACESOTHATANEXHAUSTIVESEARCHISIMPRACTICALHOWEVERALARGEKEYSPACEDOESNOTENSURETHATACIPHERISSECURETOSEETHATTHISISTHECASEWENEXTCONSIDERANATTACKTHATWILLWORKAGAINSTANYSIMPLESUBSTITUTIONCIPHERANDINTHEGENERALCASEREQUIRESFARLESSWORKTHANANEXHAUSTIVEKEYSEARCHTHISATTACKRELIESONTHEFACTTHATSTATISTICALINFORMATIONTHATISPRESENTINTHEPLAINTEXTLANGUAGELEAKSTHROUGHASIMPLESUBSTITUTION

4. Szyfr przestawieniowy
   W programie CryptTool 2.1:

   Szyfr przestawieniowy to rodzaj szyfru, w którym litery tekstu są przemieszczane w obrębie tekstu, ale same litery nie są zmieniane na inne. Występują wszystkie znaki z tekstu jawnego.

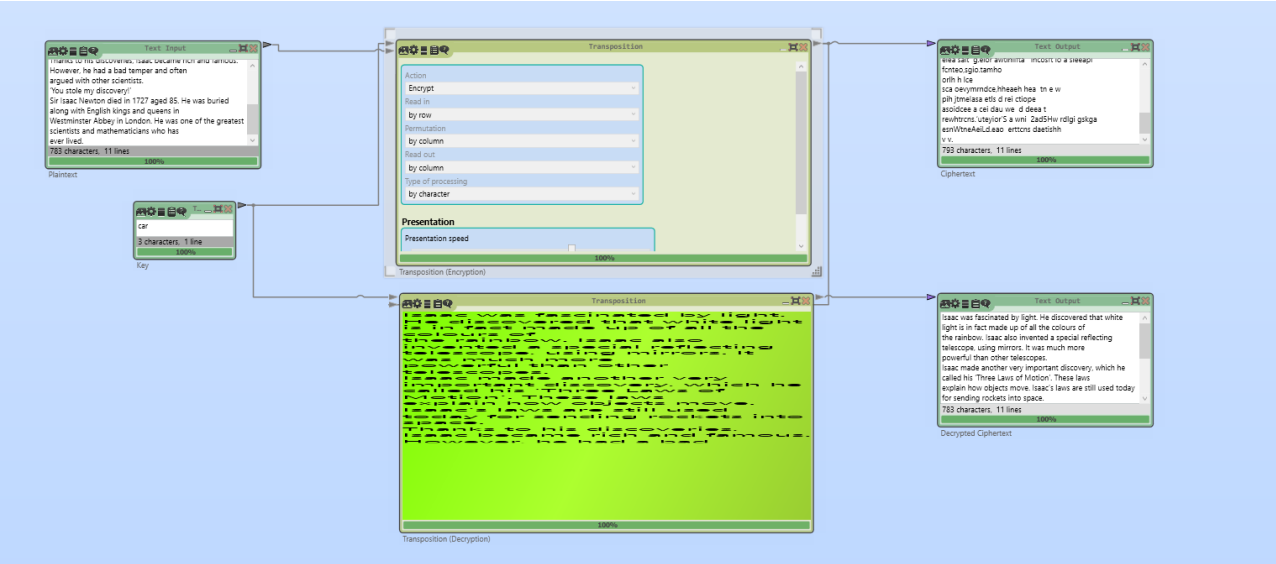
a) opracuj model realizujący szyfrowanie wybranego tekstu jawnego szyfrem przestawieniowym, a następnie zaszyfruj dowolny tekst złożony z co najmniej 100 znaków używając jako klucza dowolnego słowa, następnie w ustawieniach bloku przestawiania zmodyfikuj sposoby wpisywania, odczytywania lub permutacji i powtórz szyfrowanie,

tekst jawny:

Isaac was fascinated by light. He discovered that white light is in fact made up of all the colours of the rainbow. Isaac also invented a special reflecting telescope, using mirrors. It was much more powerful than other telescopes. Isaac made another very important discovery, which he called his ‘Three Laws of Motion’. These laws explain how objects move. Isaac’s laws are still used today for sending rockets into space. Thanks to his discoveries, Isaac became rich and famous. However, he had a bad temper and often argued with other scientists. ‘You stole my discovery!’ Sir Isaac Newton died in 1727 aged 85. He was buried along with English kings and queens in Westminster Abbey in London. He was one of the greatest scientists and mathematicians who has ever lived.

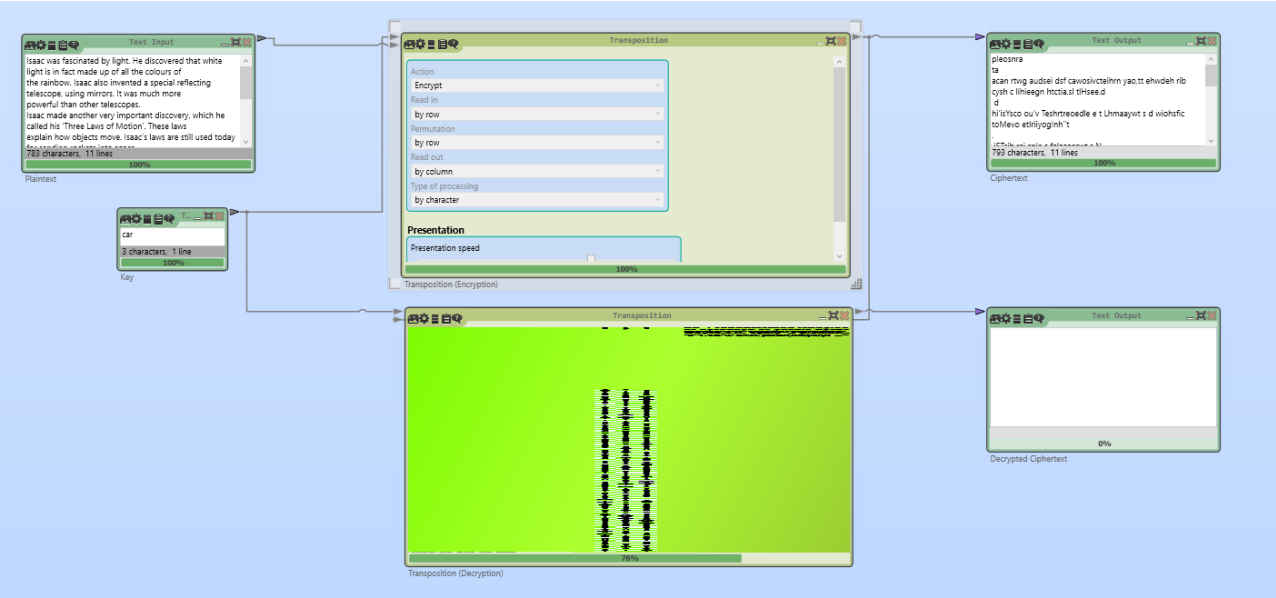
klucz: car

read in: by row
permutation: by column
read out: by column



tekst zaszyfrowany: scafcadyitHdcedh i g cmepflt lro
eab.scl vt scleei lceunmrsIw cmepeutntresp.Iamenh rioa svywchcl sTeLsfoo.heaxa wbc v a'lsrsludoyosdgoe tschkth svi,scemrhnfo.ov,eaaatp dfnau toeseis
oslmdce!
rsceoddn7 e8 sueanwhni n duni
sit b nnHw efhgasseisnmhacnw seridIaw sneblh svettheitsna duoa eou hrnwIaaonnd earltgesp i rr su r
wf aoeteos
a datre pttior i ldi'r woMi'Tslselnooeso.sc wa i etaf nnrksn a.Tn siorsIaba ca msHerhh b mrnoe
gdi h ittY o svyiIaNt ei17g .eabi o tElhisnqe emsrbynoo snot ee itta tmia oa
elea sait g.eior awtlhiifta lhcosft io a sieeapi fcnteo,sgio.tamhoorlh h lcesca oevymrndce,hheaeh hea tn e w
pih jtmeIasa etls d rei ctiope
asoidcee a cei dau we d deea trewhtrcns.'uteyior'S a wni 2ad5Hw rdlgi gskga esnWtneAeiLd.eao erttcns daetishhv v.
read in: by row
permutation: by row
read out: by column

tekst zaszyfrowany: pIeosnrata
acan rtwg audsei dsf cawosivcteihrn yao,tt ehwdeh rib cysh c lihieegn htctia.sl tlHsee.d d
hi'isYsco ou'v Teshrtreoedle e t Lhmaaywt s d wiohsfic toMevo etlriiyog!nh''t.
iSTsih rei snIe s falaaaccwt s Nme
awedtxeop nlu apdi inoe fdh oaiwln l o 1bt7jh2ee7c tcasog lemodou vr8es5. . o IfHsea
atwcha'ess rblauairwnisbe odaw r.ae l Iossntagia lcwl i atulhss eoEd n igtnlovidesanhyt ekfdio nrag sss epanendcdii naqglu erreoencfskl eeitcnst i
inWnget sott emslipenasscctеoe.pre
,AT bhubaseniykn sgi ntm oiL rohrniodsro snd..i sIHcteo vwweaarssi emosun,ce h I osmfao artceh eb
epgcorawemeaert ferusiltc hts hcaainned n otftiahsmetorsu sta.en ldHe osmwcaeotvpheeersm,.a th
ieIc sihaaaandcs amw ahbdoae d h aatnseomt
pheeevrre rav neldri yvo efidtm.



b) opracuj model realizujący kryptoanalizę szyfru przedstawieniowego, a następnie przeprowadź atak na oba szyfrogramy uzyskane w podpunkcie a).