Kriptonovelė

Pasakojimas, kurį skaitant prireiks žinių apie šioje knygelėje nagrinėtus šifrus. O perskaitę sužinosite apie dingusius templierių ordino lobius ir jų beieškant atrastąją Margaritą.

Iš Domanto T. dienoraščio

2003 metų balandžio 12 diena

Esu Vatikane. Buvau Šv. Morkaus aikštėje, žvelgiau į Berninio kolonadą. Ėjau bibliotekos koridoriais... Net ir tyla čia ypatinga. Ji tarsi rūkas, prisigėręs žodžių, žingsnių aido, paslapčių, aistrų, tiesos ir melo... Užsisakiau savo studijoms reikalingas knygas. Atsiverčiau užrašų sąsiuvinį, kad užrašyčiau antraštę: ,,Slaptieji viduramžių Europos ordinai ir sąjungos".

2003 metų balandžio 13 diena

Studijavau templierių ordino riterio Gordemaro de Bouillon užrašų kopijas. Šis riteris 1098 metais dalyvavo .... kryžiaus žygyje. Užrašai gana monotoniški ir nuobodūs: ,, ... n Kristaus metų ... x dieną pasiekėme N vietovę. Gyventojai išsilakstė. Pašėriau ir pagirdžiau žirgą. Pasimeldęs su Dievo padėjimu išjojau toliau."

2003 metu balandžio 14 diena

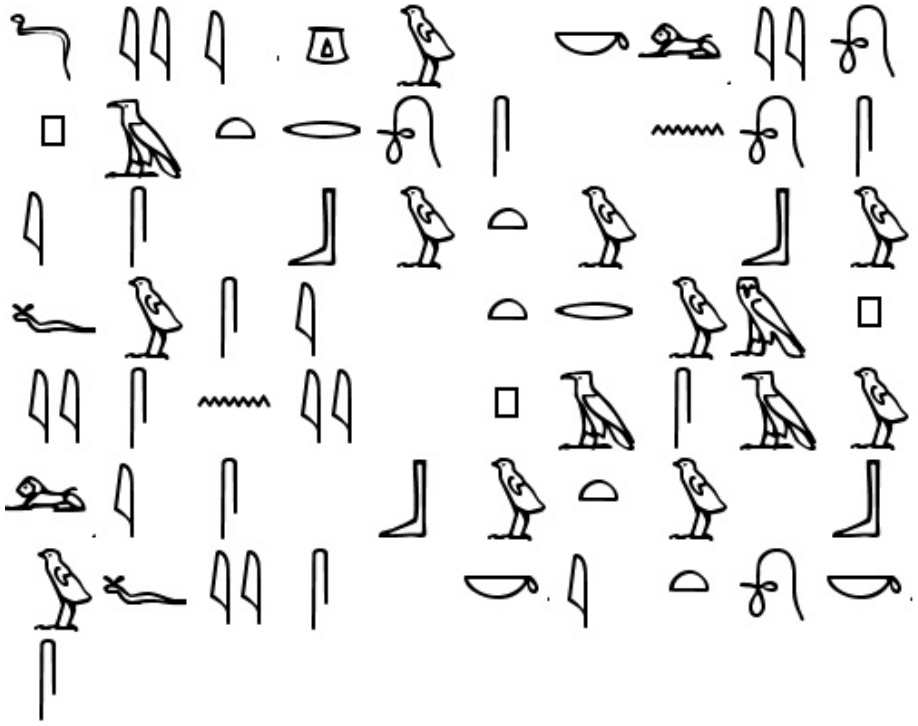
Toliau skaitau riterio G. raštus. Egipte jis įsigijo iš pirklio seną papirusą. Rašo: ,,nesuprantu nieko, bet grožiuosi". Ir kruopščiai perpiešė keletą puslapių hieroglifų:

Šiuos hieroglifus perpiešiau iš riterio J. rankraščio.

Atidžiai juos apžiūrinėjau, stengdamasis už kiekvieno ženklo įžvelgti pradingusio pasaulio paveikslus.

2003 metų balandžio 15 diena

Varčiau vieną egiptologijos veikalą, bandydamas daugiau sužinoti apie egiptiečių rašto sistemą. Painu! Šampoljonas – tai bent atkaklumo ir atsidavimo pavyzdys! Išsirašiau egiptiečių abėcėlę.



O štai mano bandymas rašyti egiptietiškai-lietuviškai.

Iš Domanto T. dienoraščio

2003 metų balandžio 20 diena

Šiandien skaičiau paskutiniuosius du riterio G. rankraščio puslapius. Tačiau kokius lapus! Juose autorius išlieja visą savo nepavykusio gyvenimo kartėlį. Vardija ir vardija nesuskaičiuojamas jo bendražygių klastas, piktadarybes ir išdavystes. Ilgai vargau, kol iššifravau daugumą tų nenaudėlių vardų. Mat, jie užrašyti vienaip ir kitaip perstatant raides. Pavyzdžiui, ROLAND rašoma kartais DNALOR, kartais LAROND, o kartais netgi ADNLOR. Paskutinis skyrelis visas parašytas perstatant raides, tačiau taisyklės nesugebėjau įminti.

2003 metų balandžio 25 diena

Jaučiuosi tarsi koks Šampoljonas – susidorojau su paskutiniais rankraščio įrašais! Padėjo vos įžiūrimas įrašas pieštuku, kurį paliko kažkas, skaitęs J. rankraštį prieš mane. Tas įrašas – vos kelios graikiškos raidės: $\sigma\kappa\tau.(\Pi\lambda\tau)$. Persirašiau lotyniškomis raidėmis: skt. (Plt) ir po kiek laiko pamaniau: ar „Plt" nėra Plutarchas? Pradėjau nuo įžymiųjų gyvenimų aprašymų. Įsigilinau taip, kad net pamiršau, kodėl skaitau. Skaičiau pasirinkdamas aprašymus beveik atsitiktinai. Ir pasisekė tarsi loterijoje! Trečiuoju bandymu pasirinkau Likurgo ir Sulos biografijas. Tačiau apie Sulą taip nieko ir nesužinojau, nes pasakojime apie Likurgą radau, ko man reikėjo: spartiečių skytalės aprašymą!

Po kelių bandymų suradau skytalės raktą $d = 5$ ir perskaičiau paskutines rankraščio eilutes. Po to išverčiau jas į lietuvių kalbą ir vėl užšifravau tuo pačiu šifru.

To: Julija@one.lt
From: Domantas@vatic.it
Subject: None

Labas Julija, pagaliau esu amžinajame mieste. Tiesa, pamačiau ne kažin ką. Dienos prabėga bibliotekoje ir archyvuose. Nesiskundžiu. Kasryt eidamas prie savo darbo kelioms minutėms stabteliu prie Berninio fontano. Vanduo tarsi apsako, ką per šimtmečius matė ir girdėjo tekėdamas šio krašto gyslomis. Pradėjau nuo templierių archyvų studijų. Pasigirsiu: sugebėjau iššifruoti vieno riterio užrašus apie kryžiaus karuose prisigrobtus lobius. Smulkiai aprašo ir vietovę. Tačiau lobių ieškoti nesirengiu. Tačiau išmokau šifruoti ,,a la grec"

MEOLB IIIĖE RMRTG ŠOSŲA TNINL UEDEĖ VTATD IOBIA ESRKM NKOĖA IEKLS ŠTUIV AURŲI SRIME IIUIN RSOEA AVSSS PEDTK LŽIEE EIENL IMVEI SUOTA TSVEU AGAKT SRLĘI NYISP ENAPA TIIAS UAGLL RUIYĖ ĖSJDP DIAOI AOUSA MANIU AUURM SKGNI NSAER

Jeigu nori perskaityti, kas parašyta – perskaityk Plutarchą. Tiek to – pagailėsiu: ne visą Plutarchą, bet Lisandro ir Sulos gyvenimų aprašymą.

Linkiu geriausios sėkmės,
Domantas

To: Domantas@vatic.it
From: Julija@one.lt
Subject: Lobiai

Sveikas Domantai,

už Plutarchą ačiū. Perskaičiau ne tik apie Lisandrą ir Sulą. Tavo šifrą įveikiau. O dabar įveik mano.

SUTON IUNIE DRUKŽ MIEOJ OTIKF ĄUVVS ĄJJIK IIRFĄ MKTLS OELAY ĄIPĮN ASKOV JYEAA ŲIEIR ŲTNRN ŲNIRK RTIĖA APKIO PILAN ISIĖC DK

Tiek to – pagailėsiu. Šifruota panašiai kaip ,,a la grec", bet naudojant raktą JULIJA. Kažin ar įstengsi?

Ir tau linkiu sėkmės,
Julija

Iš Domanto T. dienoraščio
2003 metų gegužės 4 diena

Gilinuosi į templierių paslaptis. Viename laiške vėl užtikau Gordemaro de Buillon vardą: ,, ... o apie mūsų brolio Gordemaro brangenybes tylėkime ir neišsiduokime nei

žodžiu, nei žvilgsniu, kad užčiuopėme siūlo galą. Jeigu turėsite svarbių naujienų, rašykite kaip Cezaris rašė Ciceronui...” Laiškas parašytas, praėjus maždaug šimtui metų nuo riterio G. mirties.

2003 metų gegužės 6 diena

Viename templierių ordino riterio laiške vėl radau šifrą. Išbandžiau skytalės taisyklę su įvairiais raktais, tačiau nepadėjo. Tikriausiai parašyta, kaip Cezaris rašė Ciceronui. Kaip gi jis rašė?

2003 metų gegužės 12 diena

Kaip rašė Cezaris jau žinau. Iššifravau laiško šifrą ir išvertęs į lietuvių kalbą vėl užšifravau. Jaučiausi tarsi pats būčiau templierių ordino riteris.

To: Julija@one.lt
From: Domantas@vatic.it
Subject: Templierių lobiai

Sveika Julija,

Ta riterio Gordimero lobių istorija pradeda mane jaudinti. Templieriai mini tuos turtus savo šifruotuose laiškuose, kai vargšas riteris plėšikas G. jau šimtas metų kaip dulkėmis tapęs. Tau tikriausiai bus irgi įdomu, paskaityti, ką apie tai rašo ordino magistras tūlam templierių riteriui Robertui Guiscardui. Cezario šifras tikrai nebus per kietas riešutėlis tavo ,,BLENDAMET” dantų pasta apsaugotiems stipriems dantims.

PŽUZ ĖJĖBJCJ ĮCTDJRĮCU DTSOJ UVRNŽU OCJNCJ CTŪJRCUJ PŽUZ STĖJRS DTSOJCPU ĮCOZ NCTCOLUŪHMF TFĮJV DŽUJPCU ĖJĖBJCU RFOCJPFU JT ŠFTUFNJSMJPVU ŪCĘJCV DŽN ŪAJTŪCU PCRS UŽRCV PFU ĖCT ŪVTJPF ĖTCVĮZ JT KĮLMCPF RCVMZ OFRNJMSU NCTCOJVU YFRTJNCU DCTĄĖSŪCUJU ŠCBCĖHMS PVPU BFPJZ JT UCAS NCTCOJŲNČMČ ĮOSDČ ŪSĖHO RFDFĮCJŲN JT NCTŪV UV ŠCŪJNJPCJU PŽUZ DTSOJCJU NFOJCVN K OFRNJMČ JT ŪVS NČ PVPU TJŪFTJU ĮSTĖJPFTCU ĖJFAS ACOJC ŠCOJNS

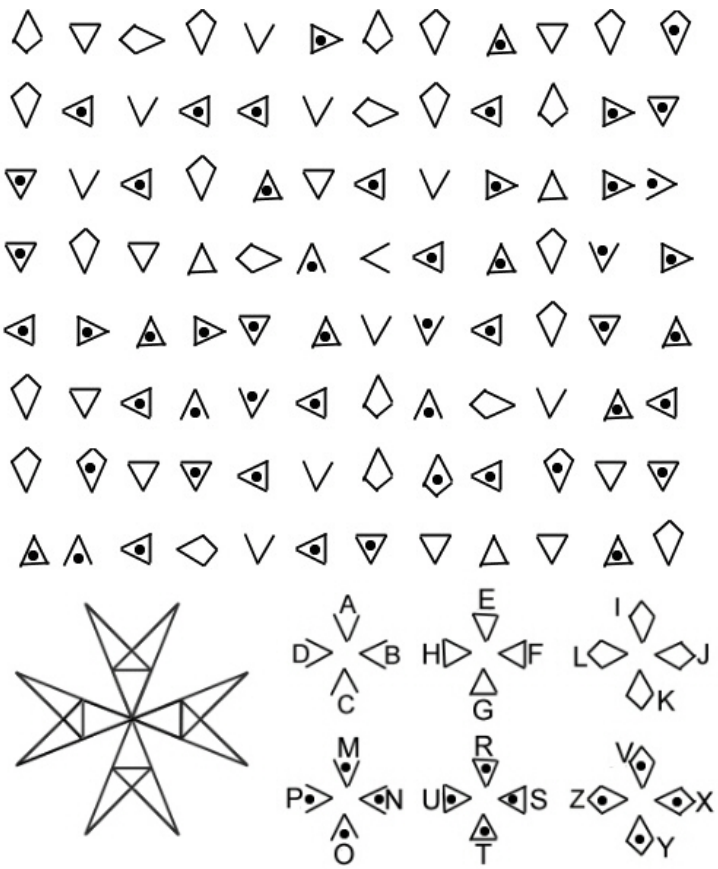
Sėkmės,
Donatas
P.S. A → Č.
Iš Domanto T. dienoraščio

2003 metų gegužės 17 diena

Liūdnas buvo templierių ordino likimas: 1307 metais Prancūzijos karalius Filipas IV liepė juos suimti, 1312 ordiną pasmerkė popiežius, o 1314 metais paskutinis ordino magistras Jacques Bernard de Molay baigė savo dienas Paryžiuje, laužo liepsnose.

Tačiau ar šventyklos riterių spindėjimas tikrai išnyko be pėdsakų, o gal – kaip sniegas karštai saulei palietus – susigėrė ir susiliejo su nematomais požeminiais srautais?

Parašiau tai baigęs skaityti laišką, rastą viename didiko archyve, parašytą templierių šriftu, galbūt net paties de Molay.



Templierių kryžius ir šifras. Iš tikrųjų ženklų ir raidžių atitiktis buvo kiek kitokia.

To: Julija@one.lt
From: Domantas@vatic.it
Subject: None

Sveika, Julija,

Cezario šifrą, kurį tau siunčiau, be abejo, perskaitei. Vakar grįždamas namo sumaniau, kaip jį patobulinti. Cezario šifro raktas – skaičius, kuris rodo, kuria abėcėlės kaimyne reikia keisti šifruojamą raidę. Mano idėja tokia: raktas yra žodis (pavyzdžiui, MENAS). Jo raidžių skaičius nurodo kelinta kaimyne reikia keisti šifruojamą raidę. O rakto raidžių tvarka nurodo, kaip reikia sudaryti naują abėcėlę iš pradinės. Pavyzdžiui:

MENAS → MENASĄBCČDF....

Jei supratai, ką parašiau ir suvoksi, ką nutylėjau, iššifruosi šifrą, kurio raktas JULIJA:

ŪCDSDED ŪVDZDŠĮTC DV ESEFDBU CNTP ZDVIRHŲ ZSIĮVĮ DV ĖEČJEZ SEŽJŲTU ČDĮŪZTEZ DV ĖĮNEČDTĮZ IDČTĮČKZ ŪEZESEZ

Sėkmės,
Domantas

To: Julija@one.lt
From: Domantas@vatic.it
Subject: None

Sveika, Julija!

Buvau beveik pamiršęs dingusias templierių brangenybes, kai vėl užtikau keistus jų pėdsakus. Popiežiaus sekretoriato archyvuose radau laišką, rašytą maždaug 1760 metais į Lietuvos Didžiąją Kunigaikštystę man kol kas nežinomam asmeniui, kuriame teiraujamasi, ar pastarasis

„... turėdamas ryšių, įtakos ir galios garbingojo lenkų karaliaus dvare negalėtų ištirti (kaip mes turime pagrindo spėti) ar dingusios templierių ordino brangenybės (teisėtai priklausančios šventajai bažnyčiai) nerado prieglobsčio per Konopickių ir Radvilų gimines atokiame Lietuvos kampelyje, kaip esame nugirdę – Salose ar Salamiestyje...”

Dalis šio laiško buvo parašyta šifruotai, tačiau radęs archyve ir laiško juodraštį sužinojau, koks šifras buvo naudotas bei koks parinktas raktas. Taigi ne tik sužinojau šį tą naujo apie šią seną istoriją, bet ir pagilinau savo kriptografijos žinias supratęs Vigenere šifrą.

Tik asmens, kuriam buvo adresuotas laiškas nepavyko nustatyti.

Lik sveika,
Domantas

To: Domantas@one.lt
From: Julija@one.it
Subject: Paslaptingasis asmuo

Labas Domantai,

lobių ieškotojau. Atrodo, galiu tau padėti. Salos – ežerų apjuostas miestelis tikrai yra Rokiškio rajone. Pasiraususi istorijos knygose sužinojau, kad jį ir jo apylinkes XVI amžiuje tikrai valdė Radvilos ir Kanopickiai. 1762 metais Salas įsigijo italas Marijanas Morikonis, Lietuvos Didžiosios Kunigaikštystės iždo raštininkas. Ar tik jis ir nebus tas žmogus, kuriam adresuotas tavo minėtas laiškas. Ar tik jis nebus pasirūpinęs įsigyti Salas, tikėdamasis rasti Gordimero lobius?

Linkėdama rasti juos ir tau,
Julija

To: Julija@one.lt
From: Domantas@vatic.it
Subject: None

Sveika Julija!

Tu man labai padėjai. Žinodamas pavardę aš nesunkiai radau Morikonio archyvą. Jame iš tiesų yra daug laiškų iš Lietuvos ir netgi Marijano Morikonio dienoraščio, rašyto maždaug 1763 metais, sąsiuvinis. Jis, atrodo, tikrai buvo įsigijęs Salas, norėdamas surasti templierių brangenybes. Tačiau viltys, ko gero, buvo bergždžios. Vis dėlto kažką jis surado. Tik ką? Perskaičiau puslapį, kuriame jis rašo apie kažkokią Margaritą, kelis kartus, bet aiškiau netapo. Vargu, ar toji Margarita buvo vietinė sodietė-baudžiauninkė. O gal jis vis dėlto kažką rado iš templierių lobio? Kokią puošnią sagę ar diademą? To mes niekada nesužinosime. Tačiau atskleisti paslaptį – visada malonumas. Suteiksiu galimmybę tau jį patirti. Puslapį iš Morikonio dienoraščio išverčiau iš italų kalbos ir užšifravau Vigenere šifru. Atskleisk rakto paslaptį ir žinosi tiek pat kiek ir aš. Tačiau kažin ar pavyks, tai ne koks žaislinis Cezario šifras.

Sėkmės,
Domantas

JILĘŪ CEČPI SGLDC SUCOG HAĄBY GUFLC KOEĖC ĖGDHĘ
VLVĖG ŽSVGO CRGAG ŽSEAĖ ĘŲLFG CUĄYY CŲRAV GŲEAĖ
ĘŲGOĮ YIFLC GIČŪY VŽSGH TAČZH YVVUG HDIDD ĄVTCH
NŽSHD YMSTR CUDHV ĮAROL ĘAKČŠ ĘAĖES GEŲYH ŪŽVOC
ĮRLEC GAGUC ĘILTR CAHZY FOLČC FSVGY CEBOC RVSDĄ
CUZČL ĘLIRV KTLYĮ MAHČY HŽVRL ĮĮNOĖ KUĖIO CEĖĖY
YPVĘŪ LLVYY YKBUC ŪŽVOG ŲIHHS KGLAO ŠIĘGC FTZAĮ
EAHŠC LKLAI FAČĖG LSVLD ĖUĖAY CEBOT LNROC ĮAGZS
LNLCŽ ĄAĖČS CPLČD YEFLC VSTCS KIĄŪE ZSVHS LKĖĖY
CDLRĮ HBĘOG ĄIICM SKCUG MRLTS LTLLV FAČĖK SUĘAH
EICOĮ ĄAĘAK S

Iš Julijos užrašų

Kasiskio testo rezultatai

Atstumų tarp vienodų digramų dalikliai

Dalikliai:	2	3	4	5	6	7	8	9	10
Kiek atstumų dalijasi:	77	44	44	73	28	17	20	15	49

Atstumų tarp vienodų trigramų dalikliai

Dalikliai:	2	3	4	5	6	7	8	9	10
Kiek atstumų dalijasi:	14	5	11	17	3	1	2	2	12

Įdomu, ar yra vienodų fragmentų iš 5 simbolių?

Atstumas tarp dviejų vienodų fragmentu EAEĖĮ yra 20, o tarp YCEBO – 115.
Beveik neabejoju, kad rakto ilgis $d = 5$. Tačiau išbandysiu ir kapa testą:

Poslinkis $d =$	1	2	3	4	5	6
Sutapimų indeksas $\kappa \approx$	0.032	0.03	0.032	0.015	0.05	0.03

Aišku, raktas yra iš 5 simbolių (gali būti ir 10 simbolių, tačiau tokio ilgo rakto Domantas tikrai nesirinko).

Reikia skaidyti šifrą į penkis fragmentus ir skaičiuoti dažnius. Nešifruotame lietuviškame tekste dažniausiai pasitaiko raidės IASET.

Dažniausiai pasitaikančios šifro fragmentų raidės ir jų dažniai

1 fragmentas	C	L	Ę	Y	F	G	K	S	H
	0,144	0,084	0,072	0,072	0,060	0,060	0,060	0,060	0,048
2 fragmentas	A	I	U	E	S	Ž			
	0,170	0,11	0,098	0,073	0,073	0,061			
3 fragmentas	L	V	Ė	Č					
	0,171	0,134	0,073	0,061					
4 fragmentas	O	A	Č	Ė	H	L			
	0,134	0,122	0,073	0,073	0,061	0,061			
5 fragmentas	C	Y	G	S	H	Į			
	0,171	0,122	0,11	0,085	0,061	0,061			

Pirmoji pastaba: pirmojo ir antrojo fragmentų dažniausiai pasitaikančių raidžių eilutės panašios: keturios pirmosios penktojo fragmento raidės ta pačia tvarka pasitaiko pirmajame fragmente. **Tikriausiai pirmoji ir penktoji rakto raidės yra vienodos**.

Antroji pastaba: antrojo fragmento dažniausiai pasitaikančių raidžių eilutė panaši į dažniausiai pasitaikančių raidžių eilutę visai nešifruotame tekste. Taip gali įvykti, jeigu antroji rakto raidė yra **A**.

Galvoju toliau: raidė A yra viena dažniausiai pasitaikančių raidžių nešifruoto teksto pirmajame, antrajame ir kituose fragmentuose. Ji atitinkamai šifruojama rakto pirmąja, antrąja, trečiąja, ketvirtąja ir penktąja raide.

Taigi pirmoji rakto raidė yra tikriausiai viena iš raidžių C L Ę Y F G K S H. Paskutinė – penktoji tokia pat. Raktas tikriausiai yra prasmingas lietuviškas žodis. Tada pirmoji ir penktoji raidė yra S! Kadangi antroji raidė yra, tikriausiai, A, tai jau žinome tris rakto raides:

$$\mathtt{SA}**\mathtt{S}$$

Trečioji rakto raidė – viena iš L V Ė Č, ketvirtoji – iš O A Č Ė H L. Eureka! Raktas yra žodis **SALOS**!

To: Domantas@vatic.it
From: Julija@one.lt
Subject: Kerštas!

Sveikas Domantai,

pavojingiausia klaida – varžovo neįvertinimas. Tu irgi manęs, matyt, neįvertinai. Tiksliau – mano kriptoanalizės žinių. Aišku, aš iššifravau tavo šifras. Dar daugiau – aš supratau, kas buvo ta Margarita.

O dabar mano kerštas: kas buvo toji Margarita sužinosi, jei šiek tiek pasimokysi matematikos.

Įdėmiai perskaityk, ką tau parašysiu. Lietuviškas raides keičiu dviženkliais skaičiais:

A	Ą	B	C	Č	D	E	Ę	Ė	F	G	H	I	Į	Y	J
10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
K	L	M	N	O	P	R	S	Š	T	U	Ų	Ū	V	Z	Ž
26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41

Iš skaičių atkuriant tekstą reikia juos be tarpų surašyti į eilutę ir keisti skaitmenų poras raidėmis. Pavyzdžiui, skaičiai

$$1530,\ 2810,\ 2935,\ 1033$$

reiškia tiesiog tavo vardą.

Margaritos paslaptį užšifravau RSA kriptosistema, kurios viešasis raktas yra toks:

$$e = 3827; \quad n = 5893;$$

5360; 1260; 5108; 935; 588; 3680; 748; 5416; 588; 32; 4652; 4160; 2976; 3632;

Kiekvienas skaičius yra RSA šifras; iššifravęs – surašyk gautuosius skaičius į eilutę ir skaitmenų poras keisk raidėmis.

Linkiu sėkmės,

Julija

Ramunėlė

Ramunėle tu baltoji,
Kad išpuoštum mano kelią,
Tu iš dulkių atsistoji,
Skaisčią pakeli galvelę...

Vargui – takui per rugienas
Tavo žiedas – džiaugsmo kraitis.
Štai pasauly aš ne vienas,
Jo bedugnėj ne našlaitis...

Skurdo skausmas lyg pagijo,
Skausmo ilgesys nurimo,
Ir krūtinė jau nebijo
Kryžiaus žemės ištrėmimo...

Saulės taurę tu pripylei,
Ir, tamsus, žygiuoju drąsiai,
Ir širdis tik klauso tyliai,
Ką tu giedi mano dvasiai...