Kaunas University of Technology
Faculty of Mathematics and Natural Sciences

Cryptology

4th laboratory work report

Marius Arlauskas

Digitally signed by Marius Arlauskas
Date: 2022.12.10 14:18:15 +02'00'

Marius Arlauskas 2022-12-10
Student

Assoc. prof. dr. Kęstutis Lukšys
Lecturer

Kaunas, 2022

1. Task 1

Task.

Lotyniškų raidžių alfabete užšifruokite žodį ADICINIS adiciniu šifru su pasirinktu raktu.

Results and comments.

Lotynišką abėcėlę abipus vienareikšmiškai atvaizduojame į $\mathbb{Z}_{26} = \{0, 1, \dots, 25\}$, kai kiekvieną raidę atitinka skaičius.

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
0	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

Tokiu būdu žodis ADICINIS atitinka $\{0, 3, 8, 2, 8, 13, 8, 18\}$.Pasirenkame raktą $k = 11$ ir pagal tapatybę $c = E_k(t) = t + k(mod\ 26)$ užšifruojame $\{0, 3, 8, 2, 8, 13, 8, 18\}$ ir gauname $\{11, 14, 19, 13, 19, 24, 19, 3\}$. Gautą rezultatą paverčiame atgal į lotyniškus rašmenis – LOTNTYTD.

2. Task 2

Task.

Iššifruokite žodį VGMGRHG, kuris buvo užšifruotas adiciniu šifru su raktu 6.

Results and comments.

VGMGRHG paverčiame į atitinkamus skaičius ir gauname $\{21, 6, 12, 6, 17, 7, 6\}$. Nuadojantis duotu raktu $k = 6$ ir iššifravimo funkcija $t = D_k(c) = c - k(mod\ 26)$ gauname $t = \{15, 0, 6, 0, 11, 1, 0\}$. Gautą rezultatą paverčiame atgal į lotyniškus rašmenis ir gauname žodį PAGALBA.

3. Task 3

Task.

Lotyniškų raidžių alfabete užšifruokite žodį AFININIS afininiu šifru su pasirinktu raktu.

Results and comments.

Lotyniškos abėcėlės raides taip pat kaip ir anksčiau numeruojame nuo nulio, todėl žodį AFININIS atitinka rinkinys $t = \{0, 5, 8, 13, 8, 13, 8, 18\}$

Pasirenkame raktą $(a, b) = (3, 7)$ ir pagal šifravimo funkciją $c = E_{(a,b)}(t) = at + b(mod\ 26)$ apskaičiuojame $c = \{7, 22, 5, 20, 5, 20, 5, 9\}$. Gautą rezultatą paverčiam atgal į lotyniškus rašmenis ir gauname HWFUFUFJ.

4. Task 4

Task.

Iššifruokite žodį RMOIRCI, kuris buvo užšifruotas afininiu šifru su raktu $a = 9$ ir $b = 2$.

Results and comments.

RMOIRCI paverčiame į atitinkamus skaičius ir gauname $\{17, 12, 14, 8, 17, 2, 8\}$. Naudojantis duotu raktu $(a, b) = (9, 2)$ ir iššifravimo funkcija $t = D_{(a,b)}(c) = a^{-1}(c - b)(mod\ 26)$ $(a^{-1}(mod\ 26) = 9^{-1}(mod\ 26) = 3)$ gauname $t = \{19, 4, 10, 18, 19, 0, 18\}$. Gautą rezultatą paverčiame atgal į lotyniškus rašmenis ir gauname žodį TEKSTAS.

5. Task 5

Task.

Kiek skirtingų raktų gali būti afininiame šifre, kuris naudoja:

a) lotynišką alfabetą?
b) lietuvių abėcėlės mažąsias raides su skaičiais?

Results and comments.

a) Lotyniškoje abėcėlėje yra 26 raidės, todėl afininio šifro raktai (a, b) turi priklausyti $\mathbb{Z}_{26} = \{0, 1, 2, \dots, 25\}$, o a turi turėti atvirkštinį daugybos atžvilgiu. Taigi, a gali būti vienas iš 12 skirtingų skaitmenų, o b vienas iš 26 – turime $12 \cdot 26 = 312$ galimų (a, b)kombinacijų.
b) Lietuviškoje abėcėlėje yra 32 mažosios raidės, kadangi įtraukiame skaičius gauname 42 simbolius, taigi raktai turi priklausyti $\mathbb{Z}_{42} = \{0, 1, 2, \dots, 41\}$. a turi turėti atvirkštinį daugybos atžvilgiu, todėl a gali būti vienas iš 12 skirtingų skaitmenų. b gali būti vienas iš 42 skaitmenų. Gauname $12 \cdot 42 = 504$ galimų (a, b) kombinacijų.

6. Task 6

Task.

Laisvai pasirinkite vieną variantą ir iš duotų šifrogramų (moodle sistemoje) nustatykite:

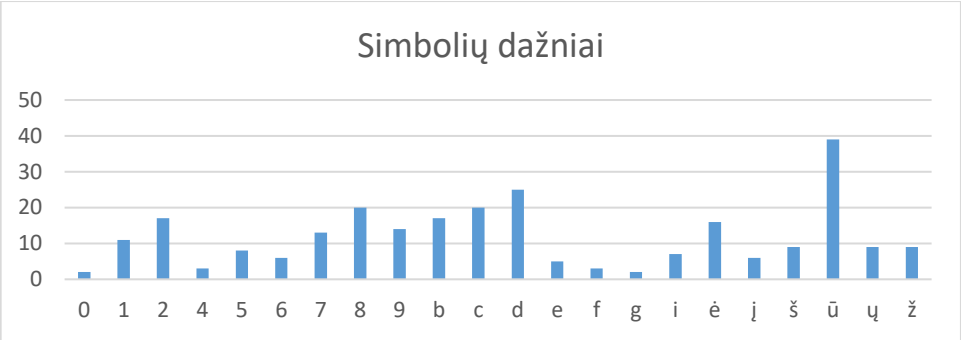
a) adicinio šifro raktus ir užšifruotas tekstogramas;
b) afininio šifro raktus ir užšifruotas tekstogramas.

Šifravimo alfabetas: „abcdefghijklmnopqrstuvwxyząčęėįšųūž0123456789“. Tekstai anglų kalba.

Results and comments.

Pasirinktas 2 variantas.

a) Naudojantis duota programa randame užšifruotame tekste esančių simbolių dažnius:



Matome, kad šifre daugiausiai naudojamas simbolis yra ū, todėl darome prielaidą, kad ji atitinka anglų kalboje dažniausiai naudojamą raidę e (tekstas anglų kalba), todėl šio adicinio šifro raktas yra $33 - 4 = 29$, o iššifravimui naudosime raktą $-29(mod\ 45) = 16$.

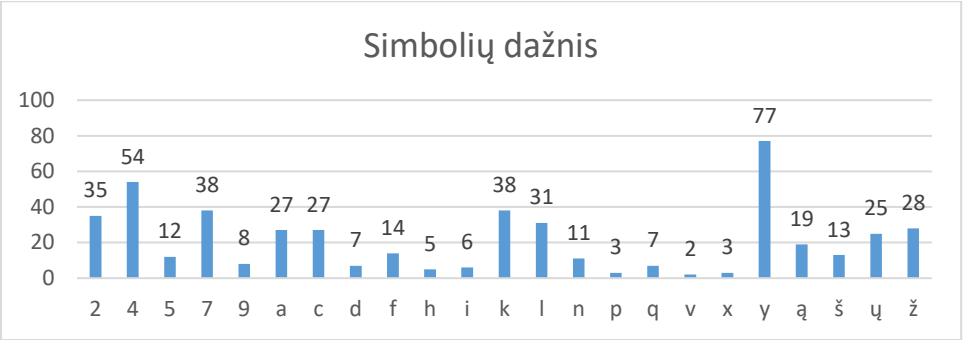
Naudojamas alfabetas su atvaizdavimu į $\mathbb{Z}_{45}$:

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	ą	č	ę	ė	į	š	ų	ū	ž	0	1	2	3	4	5	6	7	8	9
0	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	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44

Naudojantis pateikta programa gauname tekstogramą:

affine cipher. the encryption key consists of two integers separated by a space. two numbers separated by a space must also be provided for decryption. the first number is the multiplicative inverse of the first key, the second is the opposite of the second key. all operations are performed modulo the alphabet length.

b) Naudojantis duota programa randame užšifruotame tekste esančių simbolių dažnius:



Atsirenkame didžiausius pikus didėjimo tvarka: y, 4, 7, k. Kadangi afininio šifro raktams nustatyti reikia žinoti dviejų raidžių šifrus, tai mes orientuosimės į dažniausiai anglų kalboje pasitaikančių raidžių e ir t porą. Pagal turimą šifrogramą, labiausiai tikėtina, kad ši pora bus užšifruota į y ir 4 atitinkamai ($e \rightarrow y, t \rightarrow 4$), bet gali būti ir kitų variantų.

Tikriname kombinaciją $e \rightarrow y, t \rightarrow 4$.

$$\begin{cases} c_1 = at_1 + b(mod\ 45) \\ c_2 = at_2 + b(mod\ 45) \end{cases}$$

$$\begin{cases} 24 = a \cdot 4 + b(mod\ 45) \\ 39 = a \cdot 19 + b(mod\ 45) \end{cases}$$

Atimame vieną lygtį iš kitos:

$$a = (c_2 - c_1)(t_2 - t_1)^{-1}(mod\ 45)$$

$$a = (39 - 24)(19 - 4)^{-1}(mod\ 45) = 15 \cdot 15^{-1}(mod\ 45)$$

$$15^{-1}\ neegzistuoja$$

Tikriname kitas tikėtinas poras pagal dažnių diagramą – dauguma jų netinka. Galiausiai tikriname kombinaciją $e \rightarrow y, r \rightarrow k$.

$$\begin{cases} c_1 = at_1 + b(mod\ 45) \\ c_2 = at_2 + b(mod\ 45) \end{cases}$$

$$\begin{cases} 24 = a \cdot 4 + b(mod\ 45) \\ 10 = a \cdot 17 + b(mod\ 45) \end{cases}$$

Atimame vieną lygtį iš kitos:

$$a = (c_2 - c_1)(t_2 - t_1)^{-1}(mod\ 45)$$

$$a = (10 - 24)(17 - 4)^{-1}(mod\ 45) = 31 \cdot 7(mod\ 45) = 37$$

Apskaičiuojame b:

$$b = c_1 - at_1(mod\ 45)$$

$$b = 24 - 37 \cdot 4(mod\ 45) = 11$$

Galimas užšifravimo raktas $(a, b) = (37, 11)$. Pagal tai apskaičiuojame iššifravimo raktą $a^{-1} = 28$ *ir* $-b = 34$.

Naudojamas alfabetas su atvaizdavimu į $\mathbb{Z}_{45}$*:*

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	ą	č	ę	ė	į	š	ų	ū	ž	0	1	2	3	4	5	6	7	8	9
0	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	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44

Iššifravę gauname tekstą:

vernam cipher. in order to simplify the representation and compare it with the additive and affine ciphers, the xor operation is not used in this implementation. instead, a pseudo-random number is added to each plaintext letter in the given alphabet, resulting in another letter of the alphabet, which is a cyphertext. the encryption key entered, which must be an integer, is used to generate pseudo-random numbers. the same key is used for decryption, only the pseudo-random numbers generated here are subtracted from the corresponding letters of the cyphertext and thus the plaintext is restored.

7. Task 7

Task.

Pasirinkite savo tekstą (nemažiau kaip 2000 simbolių) ir užšifruokite jį Vernamo šifru. Palyginkite tekstogramos ir šifrogramos raidžių dažnius.

Results and comments.

Šifravimo alfabetas: „abcdefghijklmnopqrstuvwxyząčęėįšųūž0123456789“. Pasirinktas raktas: 7. Pasirinktas angliškas tekstas (ženklai be tarpų – 2291, ženklai su tarpais – 2793), dėl paprastumo tekstas parašytas tik mažosiomis raidėmis:

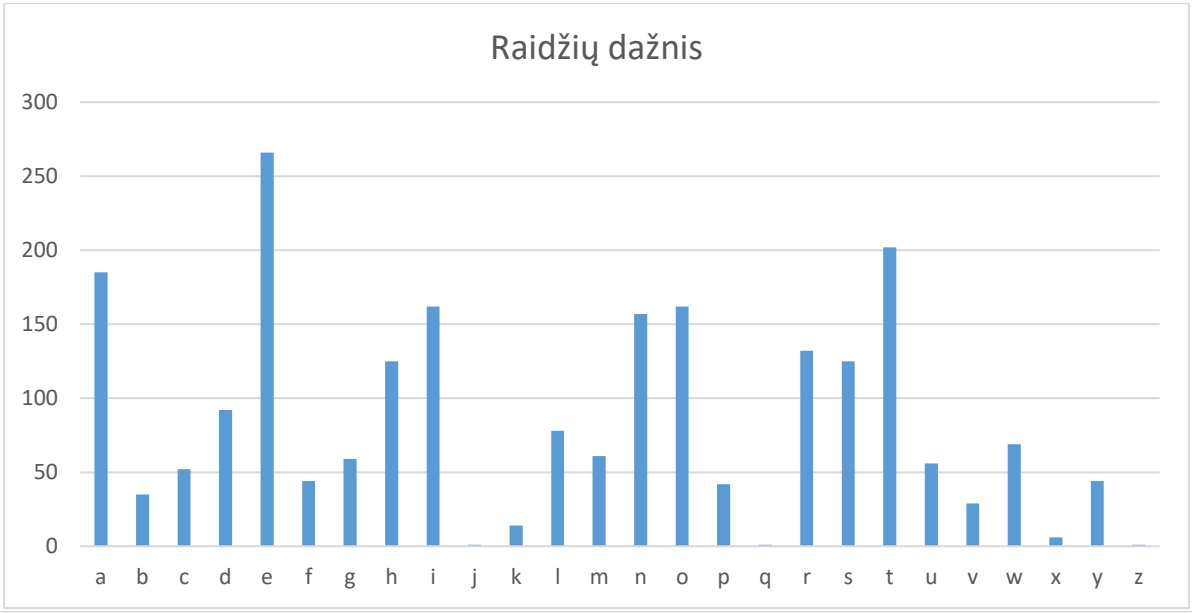
once when i was six years old i saw a magnificent picture in a book, called true stories from nature, about the primeval forest. it was a picture of a boa constrictor in the act of swallowing an animal. here is a copy of the drawing.
in the book it said: "boa constrictors swallow their prey whole, without chewing it. after that they are not able to move, and they sleep through the six months that they need for digestion." i pondered deeply, then, over the adventures of the jungle. and after some work with a colored pencil i succeeded in making my first drawing. my drawing number one. it looked like this:
i showed my masterpiece to the grown−ups, and asked them whether the drawing frightened them.
but they answered: "frighten? why should any one be frightened by a hat?"
my drawing was not a picture of a hat. it was a picture of a boa constrictor digesting an elephant. but since the grown−ups were not able to understand it, i made another drawing: i drew the inside of the boa constrictor, so that the grown−ups could see it clearly. they always need to have things explained. my drawing number two looked like this:
the grown−ups' response, this time, was to advise me to lay aside my drawings of boa constrictors, whether from the inside or the outside, and devote myself instead to geography, history, arithmetic and grammar. that is why, at the age of six, i gave up what might have been a magnificent career as a painter. i had been disheartened by the failure of my drawing number one and my drawing number two. grown−ups never understand anything by themselves, and it is tiresome for children to be always and forever explaining things to them.

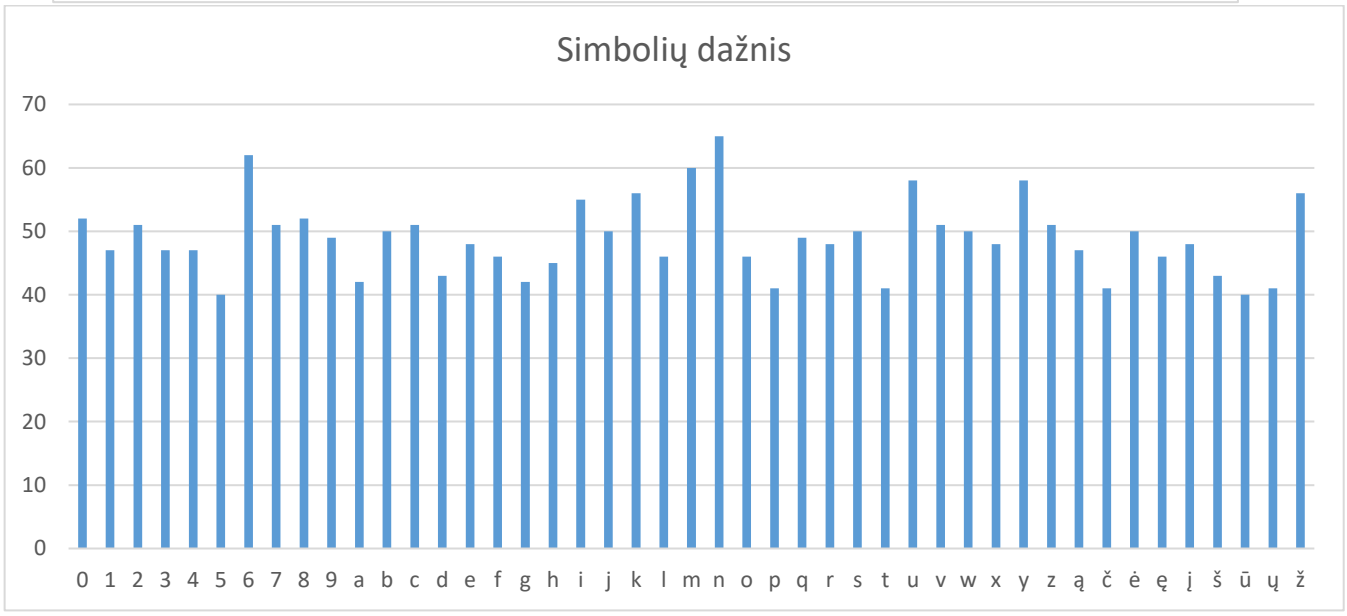
so then i chose another profession, and learned to pilot airplanes. i have flown a little over all parts of the world; and it is true that geography has been very useful to me. at a glance i can distinguish china from arizona. if one gets lost in the night, such knowledge is valuable.
in the course of this life i have had a great many encounters with a great many people who have been concerned with matters of consequence. i have lived a great deal among grown−ups. i have seen them intimately, close at hand. and that hasn't much improved my opinion of them.
whenever i met one of them who seemed to me at all clear−sighted, i tried the experiment of showing him my drawing number one, which i have always kept. i would try to find out, so, if this was a person of true understanding. but, whoever it was, he, or she, would always say:
"that is a hat." then i would never talk to that person about boa constrictors, or primeval forests, or stars. i would bring myself down to his level. i would talk to him about bridge, and golf, and politics, and neckties. and the grown−up would be greatly pleased to have met such a sensible man.

Gautas Vernamo šifru užšifruotas tekstas:

šhšg 32fk a puo 3nr 75plt c1k ė 0bt b ūų5ąnmle6t8 lcšyw8c 53 2 hyi6, 8ąc7mų žeuz xwuiufj įbej td3ylx, nsw06 oūm 5ėy6zije nnqyy3. ųt czv ž ejsaūčf ė7 g ėwz įbb3pyžžšj1 nų šb6 i1p f6 2y5bązėcoi qd 415cz5. zątz 0p u 6lwb 7w fx2 lb3gžjy.
by mks zdum 0y 6o7a: "vmo xčnž1c2vzęuo nyvotyl mmsqr žspų xfzu9, 2mcy0nč ucw7ls2 ku. lšfžv čoft qxwa ryh go9 7460 14 ųyq2, 6ąr ęn46 7ž5km 7y61kcį ėxn woč u4hūmc rsrw cim4 43ęs oūr svn9i748ė." 4 xwsao5nv kl0vyu, 4ūėj, 0n8m gl7 l05ssįbru2 gi 2xp xqprym. axw jcjm6 kčūe zmi9 ąkpm f 8142yėm 2cfw85 t 4uhjzvyęi xp ąsįųfg čų ilfie 3č9xcūg. v8 žųžucų3 72ęnyk ucb. nl q65s1m įyvw 322ų:
a n3tm7i h9 šį06oosri0ų o6 lėš į61įč−ėce, 85a ucrq0 ėnk0 24m3omš pix nti9sąū 1xre28šmųę qęa7.
vfs š9tč asnmž6v8: "qxeel7ek? b2š 9č3cęx fcn įwo sc ėdiupsewhu ty x 8g4?"
a9 ėbžeė1ę 1zh 63u 6 3hčltau am q yhč. yq 0čų č e1žęqąą f8 s l5y r106įšęhxj4 ususy1tut 6z qc48žwe6. nqi k996w vt8 ęcbųe−gjz gzyh ą7v jų8ų gl ū4šė906ęzb rn, č įčęė 9jbžofw 63jkėv2: č ęnmz x1n vį7zzb w8 ęčū gcš b6t87enkiuv, įe ųėj7 4c3 ūųfm1−č9b bčmnb fįs k7 ęihfaę1. ėn84 9hijwv 75uf žq ėi6s uvkaoz ern7w5šąp. mn prqfbm0 j78vom 9tv oykokk ddyp šūe0:
m6s sčwz8−ęė1' hž347pxė, 9wtū p0ql, 7o9 gr ain4oų č2 wš nčk q4ytž uį dūbdąš0x oū r5ą re3bmeč2k0pč, krpb8ia w7q6 wrq įlč6xe žr 0ųa c7rhym8, dįų lv8x72 uzškųw žw49gba hc a0ai9į8qq, 6hlbę7k, ynuįgow3x7 ūą4 mkg5ind. kn5w ūj 7yb, yr nc8 xkū 14 ju0, 5 260w fl pršt fdyhę 3hdf 85bg r ię4žomįvęųę ik03ya nį 4 r9nq458. q rp8 0gbž fq0lęw10degx žq 9uą ž9xi8be ęį ąų l5uąvk3 zšvžu9 7sq rę6 ęi ežezž1ė 11bamč ą7į. exfąą−węo 510vū clžb6zzpnž swnnč7ux vj pąnnėujzm3, 4vj oh 8į ė4qrsmųv a3z 4nęą6dyv i9 šl inėzpč d5i ž1n07un zl8č28yjnį žą42g9 92 ks6ė.
bw kdgu 2 z0šūę ųopūwvh v6ą9ųn82jė, i7h ohe2290 wį 1disz 2h7ąssž0l. y uhvą ę9u7a k ų2p9ay 9h3u qh0 eūbžx oq cxo kužfn; z6r čė bd ąttz f50q 6dšžęūjzz ąva fxmš 3ė1į ągb1fo 95 ęų. n6 2 zšžc0š į ųką c6ėa6hšyoų0 3jk87 nząn rxgo9ms. 2ū mky cxqp ė1kf 81 ąpm 6ą3kk, 2žup ggd9g3ycz qž ė43yūy7t.
ūy mf4 čqbd85 2ū u4įv sešg s bcu5 hū3 č vė18l jcix bgkd07d2xy ąj9ž e tšu1r kyąo so2f6m mčv o9i8 včvę eh4ųėg8šū 9ūįd nr81žwy hi 9į7mv92wh4x. 1 cšij žęomc į qzpga kąžė lžniq gdįyx−š8g. a ufh6 ėlūą ekpr ė5įjv5xxtį, 8b1w5 dj eūpz. qkd owkb 58ki'c q9fm jnš6ęelm h4 vįū05ėw 7j erjg.
gęžxsvkž ū aci kėą w2 j8em zsw 3iėįyx 2i hk šv ęėd l9bą9−a67fgyt, c 3wcįn 66n ylmjšlf383 3t pūzyė6š 3v3 8x g6tmus8 td5žer 0ąč, rivpd k d2o5 e3sdum lbqj. 1 z0a2u ešr įq fwp4 zū1, vp, 0ų pęię ųzf 4 nh16ie 43 f61į t52hėlįė4ųbnn. cąt, bxujdcį g9 nir, 3ę, a6 chš, 1bqju nn0oū2 ū2i:
"8pp1 tr a u07." 42qk j tę0rw frdwg ky6i it 4woz šux1p4 a7ų7g csm sjqč2jtęp712, ėų qžhąblė2 mlv6j0č, jt h3r9m. j ūl7g3 u5g4r 7tsčęj q6la zs ųim čfcžk. f ju09t 35fr dn įžs vjšee hhajbk, qžd yųis, ąąa d8ajdąža, duė m7urcedl. hid 4žd em0l9−fl žxi0š ėe 3todh06 82ožsr0 zq 5ięf 8ąį k1x1 ų cž6svaqi 669.

Diagramose pavaizduoti raidžių dažniai. Pirmojoje matome angliško neužšifruoto teksto raidžių dažnius, o antrojoje Vernamo šifru užšifruoto teksto simbolių dažnius. Galime pastebėti skirtumus – neužšifruotame tekste raidžių dažniai smarkiai skiriasi – svyruoja nuo 1 iki 266. Matome, kad tekste dominuoja raidė e, labai dažnai naudojamos a ir t, taip pat dažnos i, n ir o raidės. Užšifruotame tekste simbolių dažnis svyruoja nedaug – nuo 40 iki 65. Čia labiausiai vartojamas simbolis yra n, šešiasdešimties ribą taip pat perkopia ir simboliai 6 ir m – kiti simboliai savo dažniu neišsiskiria.





8. Task 8

Task.

Susipažinti su AES šifru: http://www.moserware.com/2009/09/stick-figure-guide-to-advanced.html
(Ataskaitoje pakanka parašyti, kad susipažinote).

Results and comments.

Susipažinau