Mahdi Alikhasi 9530483

Solve the following exercises in your textbook “Understanding Cryptography”:

Exer 1.8 :

$\Phi(11) = 10 \Rightarrow 5^{-1} = 5^{9} \bmod 11 = 9$

$\Phi(12) = 4 \Rightarrow 5^{-1} = 5^{3} \bmod 12 = 5$

$\Phi(13) = 12 \Rightarrow 5^{-1} = 5^{11} \bmod 13 = 8$

Exer 1.9 :

1. $x = 9 \bmod 13 = 9$
2. $x = 49 \bmod 13 = 10$
3. $x = 9^{5} \bmod 13 = 3 * 3 * 9 \bmod 13 = 81 \bmod 13 = 3$
4. $x = 10^{50} \bmod 13 = 9^{25} \bmod 13 = 9 * 3^{12} \bmod 13 = 9 * 9^{6} \bmod 13 = 9 * 3^{3} \bmod 13 = 9$
5. $x = 5$

Exer 1.10 :

$\Phi(4) = 2 = \{1,3\}$

$\Phi(5) = 4 = \{1,2,3,4\}$

$\Phi(9) = 6 = \{1,2,4,5,7,8\}$

$\Phi(26) = 12 = \{1,3,5,7,9,11,15,17,19,21,23,25\}$

Exer 1.11 :

$y = ax + b \Rightarrow x = (y + 26 - b) * a^{-1}$

$a^{-1} = 7^{11} \bmod 26 = 15 \Rightarrow x = (y + 26 - 22) * 15 \bmod 26$

falszztysyjzyjkywjrztyjztyynaryjkyswarztyegyyj

1. firstthesentenceandthentheevidencesaidthequeen
2. queen

Do the following projects with the useful program “CrypTool”.

Ex1:

a) Vigenere Cipher is a method of encrypting alphabetic text It uses a simple form of polyalphabetic substitution A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets In this encryption the key is repeated until it matches the length of plain text For encrypting a plain text with a key after matching the key with plaintext we just use a plus operation as following let map the Alphabet A to Z to zero-twenty five. for using plus operation just add the corresponding number of alphabet and modulo it to twenty six For decryption we just use the subtract operand like plus operator The cipher is easy to understand and implement but it resisted all attempts to break it for three centuries which earned it the description the indecipherable cipher Many people have tried to implement encryption schemes that are essentially Vigenere ciphers Friedrich Kasiski was the first to publish a general method of deciphering Vigenere ciphers The Vigenere cipher was originally described by Giovan Battista Bellaso in his book La cifra del Sig Giovan Battista Bellaso but the scheme was later misattributed to Blaise de Vigenere in the nineteenth century and so acquired its present name The first well documented description of a polyalphabetic cipher was formulated by Leon Battista Alberti and used a metal cipher disc to switch between cipher alphabets Alberti system only switched alphabets after several words and switches were indicated by writing the letter of the corresponding alphabet in the ciphertext Later Johannes Trithemius in his work Polygraphiae invented the tabula recta a critical component of the Vigenere cipher The Trithemius cipher however provided a progressive rather rigid and predictable system for switching between cipher alphabets What is now known as the Vigenere cipher was originally described by Giovan

Battista Bellaso in his book La cifra del Sig Giovan Battista Bellaso He built upon the tabula recta of Trithemius but added a repeating countersign a key to switch cipher alphabets every letter Whereas Alberti and Trithemius used a fixed pattern of substitutions Bellasos scheme meant the pattern of substitutions could be easily changed simply by selecting a new key Keys were typically single words or short phrases known to both parties in advance or transmitted out of band along with the message Bellaso method thus required strong security for only the key As it is relatively easy to secure a short key phrase such as by a previous private conversation Bellasos system was considerably more secure Blaise de Vigenere published his description of a similar but stronger autokey cipher before the court of Henry III of France Later the invention of Bellasos cipher was misattributed to Vigenere David Kahn in his book The Codebreakers lamented the misattribution by saying that history had ignored this important contribution and instead named a regressive and elementary cipher for him though he had nothing to do with it The Vigenere cipher gained a reputation for being exceptionally strong. Noted author and mathematician Charles Lutwidge Dodgson called the Vigenere cipher unbreakable in his piece The Alphabet Cipher in a childrens magazine Scientific American described the Vigenere cipher as impossible of translation

b)

1. 66000710529530483
2. 11
3. 6600071052530483
5. OAHKABEF

c) Jinonfvj Qiwres mx o mldhph tt eumrztywnn klqlfpeasc uich Ia esfw f gitzlf jtfm vp pppdolwraciywc zebtxnhuasoo E uclfklqlfpeasc dmuvey ss brd qiwres ffgek yn tyggtpduumtb, uzsnh qzztpzlf wzpsastvxncn hvpiegstz Sn ulng eumrztywou dhf ojm iz beqifhek enumq wt tktdljg too lfrlhh vp pmenb tlht Gsw snjbyqxnbg h zlbms heed wjxm o kli agxjf mhdcimsu too kfc bwto zlbmsheed wf nzgt bce b tqis vzeseywou ks gsqzodsnh pjh mhz tii Fzpokbfx F ho G do aiwc-tdonuc kwvl. pos yxwnn zlvw tdeyktjss xuzd aeh yve jyrsixdouniok simior pj fzpokbfx fbd tydvpt wt ay txishy zsx Gsw rejbyqxncn do jvwy isl dhf wzptykcu susrhxd mmps pses ptjfaayr Ulj qiwres mx sazi tp ysreyctbri onk smqpjaeud bvx nh rlcitxjr asv auxjapac tp fwsar st gsw hhyoe dishuyset amwco oasrjr ia dhf hjgcyspumtb too iohjqiwresegze jspiiw Aaui pfsuze okvf xwwek do jquzetonu isqrfztjss gcoomfw yvaa krf ixgeudibpqm Vpqeoiws cpzhfvx Trpodsmhv Khciton kaz dhf jnfsa do qygzizr a hissrhv mfxmcd vp dfgndhlbiok Awglxesi hwpoort Xms Vpqeoiws cpzhfv bos vbihmsolsi dfwhfiiod cc Lwockn Ceyhizda Ciqzazy io lng bvyk Me hwfyk dfp Xwg Nsowes Paaditxf Pesvats git are tgmsml gat pfhey witeyhrpluuii ho Ivajwj re Csgfrjfe px tii swnldefryv clxtvvd onk co bgviiyod jxx drlceox soml Dhf jnfsa gemp iccbweoxjr dlccsmuhivx og e uclfklqlfpeasc dmuvey gat jtfmbvauii py Sooo Ffhtpctb Eqpeydi bri isln a niyol jspiiw rizm tp wbwtjr bfxbseu miqljf aszhbfjhs Hvbfvyw sfctfq tblf cwjxhvek klqlfpeac agxjf slfeseq koyns bri gwpdciix keyo iohnqaaod cc bfiasnh xms lldtfv tt too cpvwsswynemsu aszhbfjh iu dhf gndhlbtfby Zaaor Ksmonuos Uvnhhlwivw nb hpc wpvp Dosigseuviho iozjbtln tii yobbva sihha h mrjxnqas monttbeud og xms Vpqeoiws cpzhfv Yve Abiuljaibc cjtmsr oywfzjf pyyvjhjr a wbohvjgspfe seyvey bihmi onk zrfhnqthllf wdgtlw fpv xkiamhjrl peagefr hwpoor bpuvaiott Amot pc npa pbodx at xms Vpqeoiws cpzhfv bos vbihmsolsi dfwhfiiod cc Lwockn Ceyhizda Ciqzazy io lng bvyk Me hwfyk dfp Xwg Nsowes Paaditxf Pesvats Ms bbslu yucn are uegilh bedxf cf Abiuljaibc bvx frdln a siusaasnh gtinaortmlb a roy us xkiamh dmuvey klqlfpeac ewiwm lldtfv Bveyoat Eqpeydi bri Hrpdhfqnis bcee e kwxln pbxysru yf tyggtpduumtbs Iolmexcs zmhfqj aehxt ulj daadesr tt sblsumyitpynt gtilk le fexwlf mhbrlsd zsmqpd py zolfgywnn k nfa psy Royt ajfe aipjgfzlf ciokqs wvbdt sw ghvbt qlwoslc kosbb tv loul uoraset ms odckndi tf tykntqnhtln ovx tt bhxd bptbg dsti xms mlcsbkj Pesvats rstoyd ulzg rlaujvjr sabook xscbbiuc kcr vxlz xms kli At my ws yolbxnjesi ebwd ho zocvvj o soyru ojm pobati xico ks cc f drlfipyx drpfaui hcncorteywou Lempfgoz cytxja whc cprxwdlbacpd aoyo sfgzfe Ivajwj re Csgfrjfe webmmxvek rit hjgcyspumtb om k sjqnzay luu wyfouqes ezhoroy dmuvey legsws too cpywh om Reovd WIP yf Gvfbcl Vauiw hhl snwishivx og Fjzlhcot gndhlb wbw rwshdtsmgitln tp Znueuorf Hfjik Uair nb hpc bpsp Hhl Moeigfehuesw qomlxtfh yve tssbxyfiietjss py zkyjrl hhhd hjwycrf rae mlboyod ulng itzosxfbt jynuvnpuasoo esr iuctfei batod b vjurlcsjzj onk olfqjbthby dmuvey pos lna toyuhl ms hhn npxmwnn

do es bwto st Ulj Jinonfvj qiwres kfwnln a siuithdipr kcr ioiok jlclztjssolsi suvtbg. Uytfh fitoyr bri aaareneywcpkn Dlfflc Lvxbwdno Dphlgou mampjr too Vjkjbeyo cjtmsr bxbsifyaive jr mws wsedi Yve Hvpiegst Jspiiw wn h mhjpifeuc mbkfniuo Sdmjbtppid Ersrpmao hjgcysbfh yve Csgfrjfe jspiiw os pwppwxwbso og xwonzvaumtb

d) Yes. it broked correctly.

e) key = sdkfkfdfkjsdfnfhspwrgerlvnvfsdflgsvsagqrqvzcsj
Yes. it broked correctly

Ex2:

a) OAHKBEFMDILS

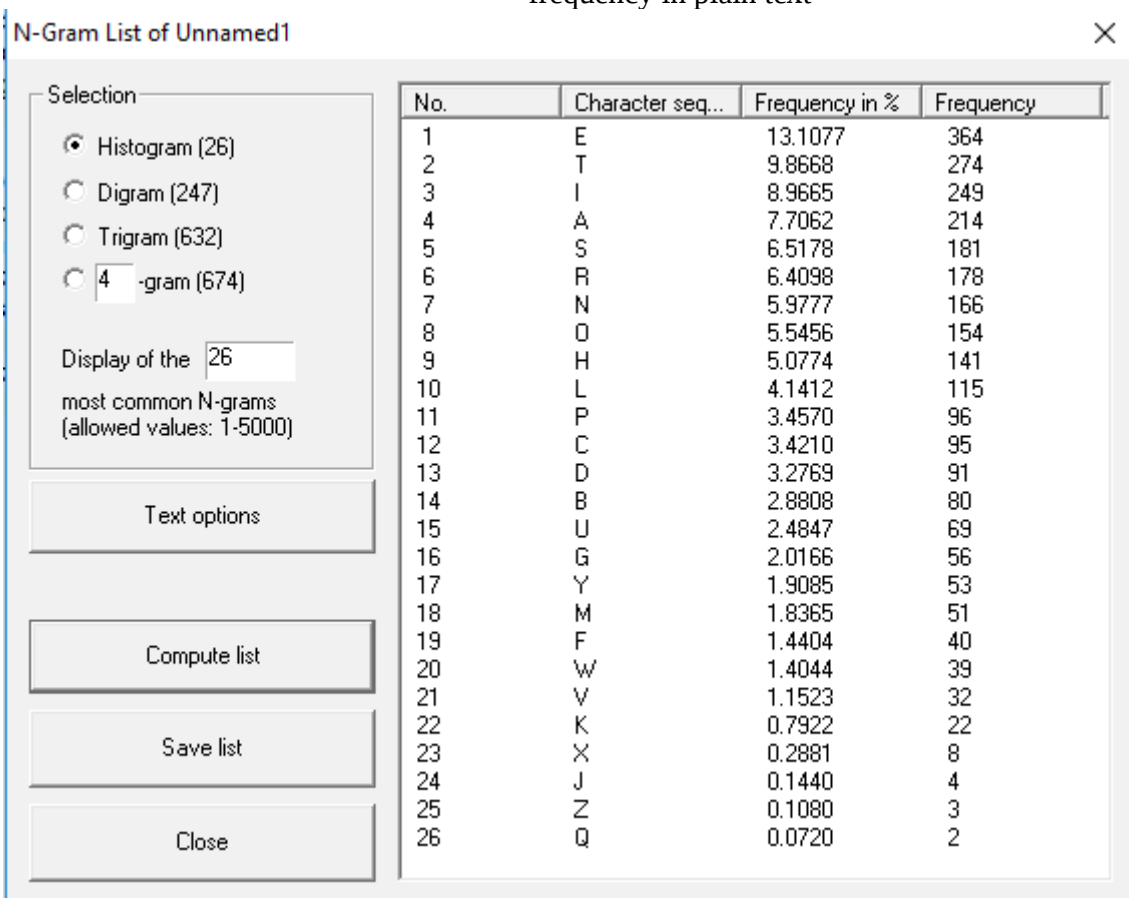
b) Vdfbgbqb Hdnmbq dr o cbtmjk je bghqyntdgf osnmoabtdh tbxt Dt urbr o rdcnsb ejqc je njsyosnmoabtdh ruartdtutdjg O njsyosnmoabtdh hdnmbq dr ogy hdnmbq aorbk jg ruartdtutdjg, urdgf custdnsb ruartdtutdjg osnmoabtr Dg tmdr bghqyntdjg tmb lby dr qbnbotbk ugtds dt cothmbr tmb sbgftm je nsodg tbxt Ejq bghqyntdgf o nsodg tbxt wdtm o lby oetbq cothmdgf tmb lby wdtm nsodgtbxt wb iurt urb o nsur jnbqotdjg or ejssjwdgf sbt con tmb Osnmoabt O tj Z tj zbqj-twbgty edvb. ejq urdgf nsur jnbqotdjg iurt okk tmb hjqqbrnjgkdgf gucabq je osnmoabt ogk cjkusj dt tj twbgty rdx Ejq kbhqyntdjg wb iurt urb tmb ruatqoht jnbqogk sdlb nsur jnbqotjq Tmb hdnmbq dr bory tj ugkbqrtogk ogk dcnsbcbgt aut dt qbrdrtbk oss ottbcntr tj aqbol dt ejq tmqbb hbgtuqdbr wmdhm boqgbk dt tmb kbrhqdntdjg tmb dgkbhdnmbqoasb hdnmbq Cogy nbjnsb movb tqdbk tj dcnsbcbgt bghqyntdjg rhmbcbr tmot oqb brrbgtdossy Vdfbgbqb hdnmbqr Eqdbkqdhm Lordrld wor tmb edqrt tj nuasdrm o fbgbqos cbtmjk je kbhdnmbqdgf Vdfbgbqb hdnmbqr Tmb Vdfbgbqb hdnmbq wor jqdfdgossy kbrhqdabk ay Fdjvog Aottdrto Abssorj dg mdr ajjl So hdeqo kbs Rdf Fdjvog Aottdrto Abssorj aut tmb rhmbcb wor sotbq cdrottqdautbk tj Asodrb kb Vdfbgbqb dg tmb gdgbtbbgtm hbgtuqy ogk rj ohpudqbk dtr nqbrbgt gocb Tmb edqrt wbss kjhucbgtbk kbrhqdntdjg je o njsyosnmoabtdh hdnmbq wor ejqcusotbk ay Sbjg Aottdrto Osabqtd ogk urbk o cbtos hdnmbq kdrh tj rwdthm abtwbbg hdnmbq osnmoabtr Osabqtd ryrtbc jgsy rwdthmbk osnmoabtr oetbq rbvbqos wjqkr ogk rwdthmbr wbqb dgkdhotbk ay wqdtdgf tmb sbttbq je tmb hjqqbrnjgkdgf osnmoabt dg tmb hdnmbqtbxt Sotbq Ijmoggbr Tqdtmbcdur dg mdr wjql Njsyfqonmdob dgvbgtbk tmb toauso qbhto o hqdtdhos hjcnjgbgt je tmb Vdfbgbqb hdnmbq Tmb Tqdtmbcdur hdnmbq mjwbvbq nqjvdkbk o nqjfqbrrdvb qotmbq qdfdk ogk nqbkdhtoasb ryrtbc ejq rwdthmdgf abtwbbg hdnmbq osnmoabtr Wmot dr gjw lgjwg or tmb Vdfbgbqb hdnmbq wor jqdfdgossy kbrhqdabk ay Fdjvog Aottdrto Abssorj dg mdr ajjl So hdeqo kbs Rdf Fdjvog Aottdrto Abssorj Mb audst unjg tmb toauso qbhto je Tqdtmbcdur aut okkbk o qbnbotdgf hjugtbqrdfg o lby tj rwdthm hdnmbq osnmoabtr bvbqy sbttbq Wmbqbor Osabqtd ogk Tqdtmbcdur urbk o edxbk nottbqg je ruartdtutdjgr Abssorjr rhmbcb cbogt tmb nottbqg je ruartdtutdjgr hjusk ab bordsy hmogfbk rdcnsy ay rbsbhtdgf o gbw lby Lbyr wbqb tyndhossy rdgfsb wjqkr jq rmjqt nmqorbr lgjwg tj ajtm noqtdbr dg okvoghb jq tqogrcdttbk jut je aogk osjgf wdtm tmb cbrrofb Abssorj cbtmjk tmur qbpudqbk rtqjgf rbhuqdty ejq jgsy tmb lby Or dt dr qbsotdvbsy bory tj rbhuqb o rmjqt lby nmqorb ruhm or ay o nqbvdjur nqdvotb hjgvbqrotdjg Abssorjr ryrtbc wor hjgrdkbqoasy cjqb rbhuqb Asodrb kb Vdfbgbqb nuasdrmbk mdr kbrhqdntdjg je o rdcdsoq aut rtqjgfbq outjlby hdnmbq abejqb tmb hjuqt je Mbgqy DDD je Eqoghb Sotbq tmb dgvbgtdjg je Abssorjr hdnmbq wor cdrottqdautbk tj Vdfbgbqb Kovdk Lomg dg mdr ajjl Tmb Hjkbaqbolbqr socbgtbk tmb cdrottqdautdjg ay roydgf tmot mdrtjqy mok dfgjqbk tmdr dcnjqtogt hjgtqdautdjg ogk dgrtbok gocbk o qbfqbrrdvb ogk bsbcbgtoqy hdnmbq ejq mdc tmjufm mb mok gjtmdgf tj kj wdtm dt Tmb Vdfbgbqb hdnmbq fodgbk o qbnutotdjg ejq abdgf bxhbntdjgossy rtqjgf. Gjtbk outmjq ogk cotmbcotdhdog Hmoqsbr Sutwdkfb Kjkfrjg hossbk tmb Vdfbgbqb hdnmbq ugaqboloasb dg mdr ndbhb Tmb Osnmoabt Hdnmbq dg o hmdskqbgr cofozdgb Rhdbgtdedh Ocbqdhog kbrhqdabk tmb Vdfbgbqb hdnmbq or dcnjrrdasb je tqogrsotdjg

c)

frequency in book

Letter	Frequency	Letter	Frequency
A	0.0817	N	0.0675
B	0.0150	O	0.0751
C	0.0278	P	0.0193
D	0.0425	Q	0.0010
E	0.1270	R	0.0599
F	0.0223	S	0.0633
G	0.0202	T	0.0906
H	0.0609	U	0.0276
I	0.0697	V	0.0098
J	0.0015	W	0.0236
K	0.0077	X	0.0015
L	0.0403	Y	0.0197
M	0.0241	Z	0.0007

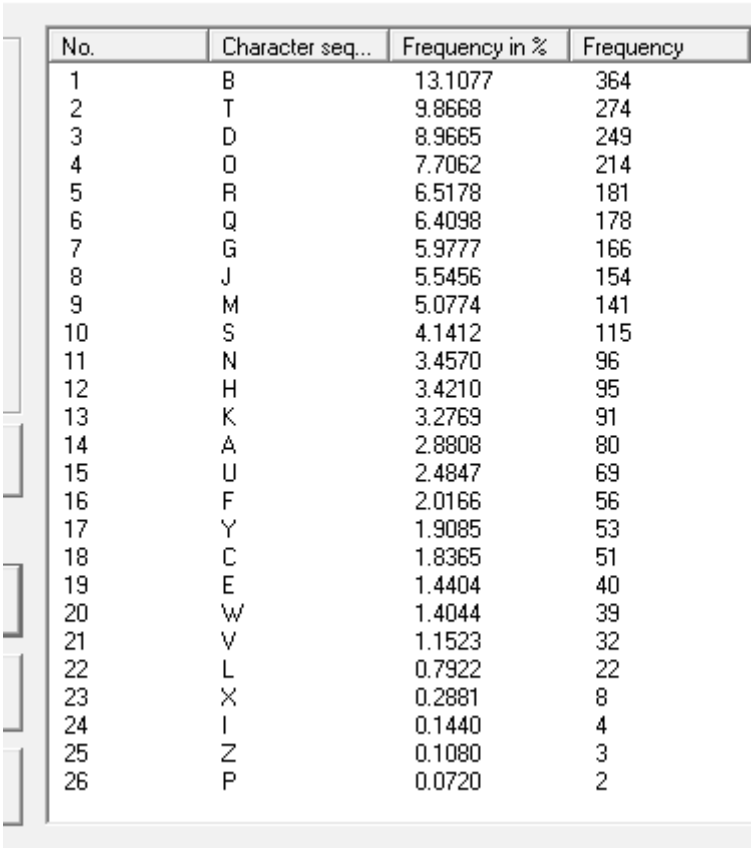
frequency in plain text



as you can see the frequency in book and in my plain text is similar.

Frequency in cipher text

yption of <Unnamed1>, key <OAHKBEFMDILSCGJNPQRTUVWXY... >



No.	Character seq...	Frequency in %	Frequency
1	B	13.1077	364
2	T	9.8668	274
3	D	8.9665	249
4	O	7.7062	214
5	R	6.5178	181
6	Q	6.4098	178
7	G	5.9777	166
8	J	5.5456	154
9	M	5.0774	141
10	S	4.1412	115
11	N	3.4570	96
12	H	3.4210	95
13	K	3.2769	91
14	A	2.8808	80
15	U	2.4847	69
16	F	2.0166	56
17	Y	1.9085	53
18	C	1.8365	51
19	E	1.4404	40
20	W	1.4044	39
21	V	1.1523	32
22	L	0.7922	22
23	X	0.2881	8
24	I	0.1440	4
25	Z	0.1080	3
26	P	0.0720	2

d) yes. Cryptool succeeded in this case.

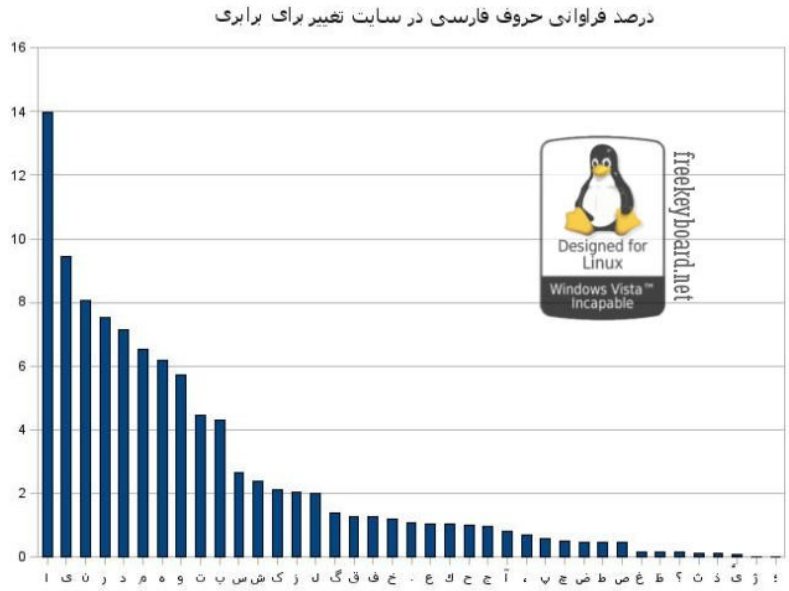
e) the first method used the frequency on alphabets in the plaintext and base on that try to guess the substitution. But in the second method we use the frequency of words in english language and base on that decrypt the ciphertext.

f) در حالت اول به دلیل کوتاه بودن رشته و کمتر از 300 کلمه بودن متن امکان رمزگشایی وجود نداشت

because the practice of the basic movements of kata is the focus and mastery of self is the essence of matsubayashi ryu karate do i shall try to elucidate the movements of the kata according to my interpretation based on forty years of study

it is not an easy task to explain each movement and its significance and some must remain unexplained to give a complete explanation one would have to be qualified and inspired to such an extent that he could reach the state of enlightened mind capable of recognizing soundless sound and shapeless shape i do not deem myself the final authority but my experience with kata has left no doubt that the following is the proper application and interpretation i offer my theories in the hope that the essence of okinawan karate will remain intact

g)
منبع: jadi.net



در هر دوی زبان ها حروفی مانند e یا ا یا ی یا ن یا n یا ت یا t یا I به ترتیب جزو حروف های پرتکرار هستند و میتوان گفت که آوای تکراری در هر دو زبان نزدیک به یکدیگر است

Ex3:

Our great democracies still tend to think that a stupid man is more likely to be honest than a clever man.