ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών,
Τομέας Επικοινωνιών, Ηλεκτρονικής και Συστημάτων Πληροφορικής
Ροή Δ, Μάθημα: *Ασφάλεια Δικτύων Υπολογιστών* (Εξάμηνο 8ο)

Πρώτη Εργαστηριακή Άσκηση: Φύλλο Απαντήσεων

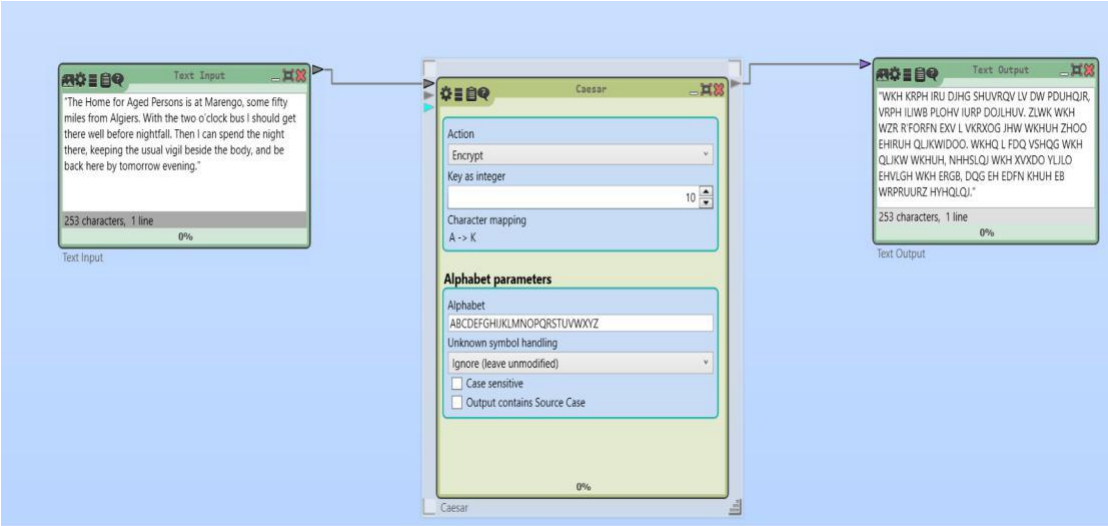
Κλασσικοί Αλγόριθμοι Κρυπτογράφησης

Ονοματεπώνυμο: Δόντη Ειρήνη
Αριθμός Μητρώου: 03119839
Εξάμηνο: 8ο

Ερώτηση 1.1

"***The Home for Aged Persons is at Marengo, some fifty miles from Algiers. With the two o'clock bus I should get there well before nightfall. Then I can spend the night there, keeping the usual vigil beside the body, and be back here by tomorrow evening***."

Διάταξη:



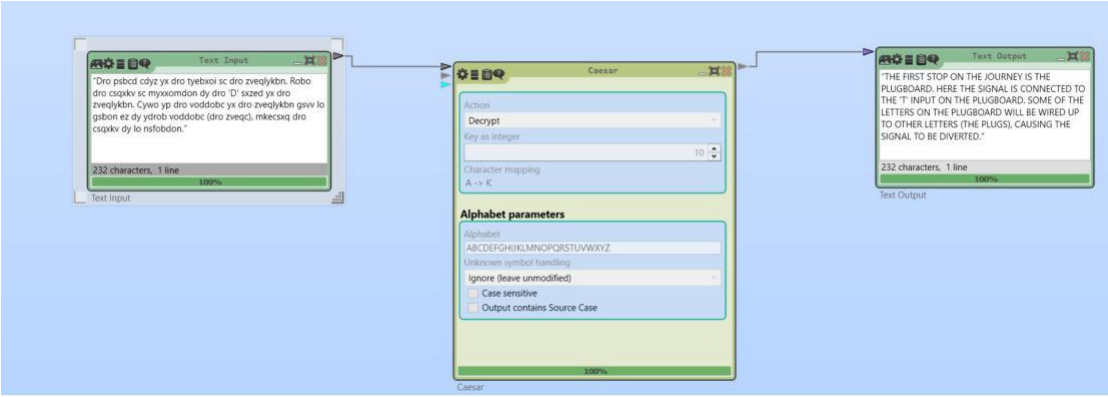
Κρυπτογραφημένο κείμενο:

"WKH KRPH IRU DJHG SHUVRQV LV DW PDUHQJR, VRPH ILIWB PLOHV IURP DOJLHUV. ZLWK WKH WZR R'FORFN EXV L VKRXOG JHW WKHUH ZHOO EHIRUH QLJKWIDOO. WKHQ L FDQ VSHQG WKH QLJKW WKHUH, NHHSLQJ WKH XVXDO YLJLO EHVLGH WKH ERGB, DQG EH EDFN KHUH EB WRPRUURZ HYHQLQJ."

Ερώτηση 1.2

“***Dro psbcd cdyz yx dro tyebxoi sc dro zveqlykbn. Robo dro csqxkv sc myxxomdon dy dro 'D' sxzed yx dro zveqlykbn. Cywo yp dro voddobc yx dro zveqlykbn gsvv lo gsbon ez dy ydrob voddobc (dro zveqc), mkecsxq dro csqxkv dy lo nsfobdon***.”

Διάταξη:



Αποκρυπτογραφημένο κείμενο:

“THE FIRST STOP ON THE JOURNEY IS THE PLUGBOARD. HERE THE SIGNAL IS CONNECTED TO THE 'T' INPUT ON THE PLUGBOARD. SOME OF THE LETTERS ON THE PLUGBOARD WILL BE WIRED UP TO OTHER LETTERS (THE PLUGS), CAUSING THE SIGNAL TO BE DIVERTED.”

Ερώτηση 1.3

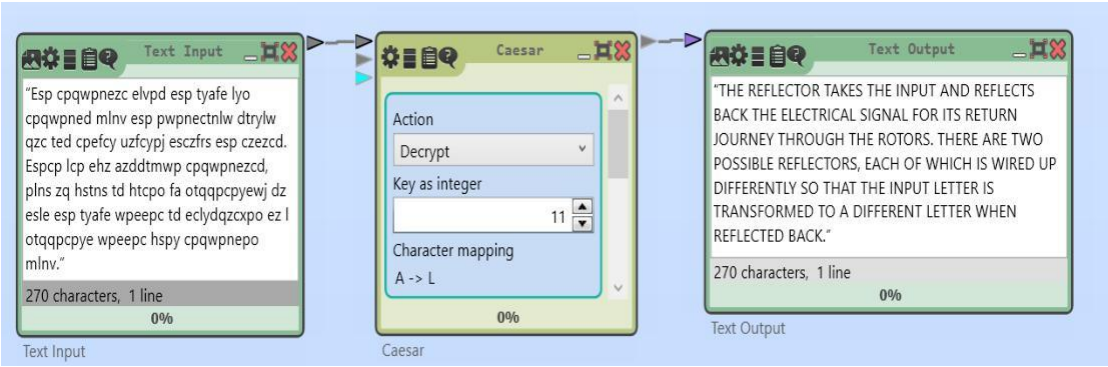
Διάταξη:

Για κλειδί K = 13, προκύπτει το αρχικό κείμενο μάσε της διπλής διαδικασίας κρυπτογράφησης.

Ερώτηση 1.4

“***Esp cpqwpnezc elvpd esp tyafe lyo cpqwpned mlnv esp pwpnectnlw dtrylw qzc ted cpefcy uzfcypj esczfrs esp czezcd. Espcp lcp ehz azddtmwp cpqwpnezcd, plns zq hstns td htcpo fa otqqpcpyewj dz esle esp tyafe wpeepc td eclydqzcxpo ez l otqqpcpye wpeepc hspy cpqwpnepo mlnv***.”

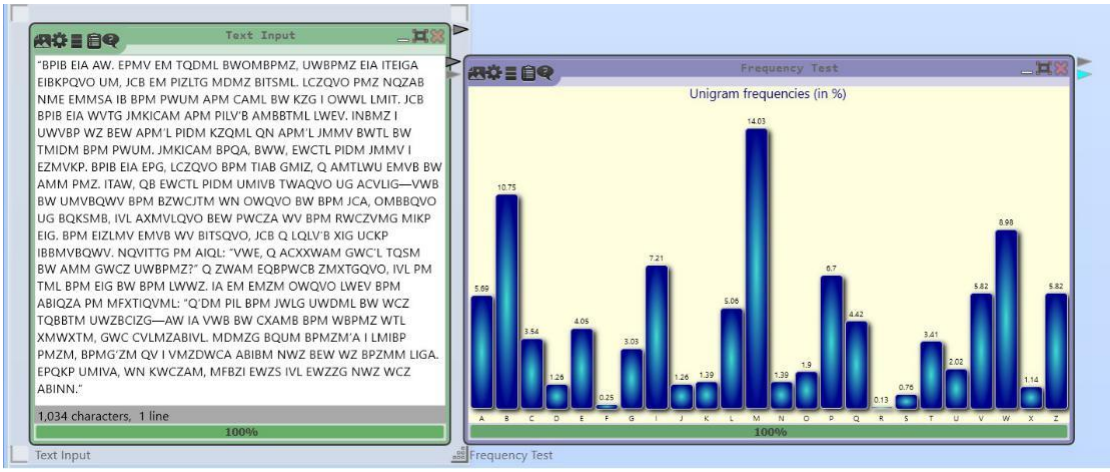
Διάταξη:



Ερώτηση 1.5

"BPIB EIA AW. EPMV EM TQDML BWOMBPMZ, UWBPMZ EIA ITEIGA EIBKPQVO UM, JCB EM PIZLTG MDMZ BITSML. LCZQVO PMZ NQZAB NME EMMSA IB BPM PWUM APM CAML BW KZG I OWWL LMIT. JCB BPIB EIA WVTG JMKICAM APM PILV'B AMBBTML LWEV. INBMZ I UWVBP WZ BEW APM'L PIDM KZQML QN APM'L JMMV BWTL BW TMIDM BPM PWUM. JMKICAM BPQA, BWW, EWCTL PIDM JMMV I EZMVKP. BPIB EIA EPG, LCZQVO BPM TIAB GMIZ, Q AMTLWU EMVB BW AMM PMZ. ITAW, QB EWCTL PIDM UMIVB TWAQVO UG ACVLIG—VWB BW UMVBQWV BPM BZWCJTM WN OWQVO BW BPM JCA, OMBBQVO UG BQKSMB, IVL AXMVLQVO BEW PWCZA WV BPM RWCZVMG MIKP EIG. BPM EIZLMV EMVB WV BITSQVO, JCB Q LQLV'B XIG UCKP IBBMVBQWV. NQVITTG PM AIQL: "VWE, Q ACXXWAM GWC'L TQSM BW AMM GWCZ UWBPMZ?" Q ZWAM EQBPWCB ZMXTGQVO, IVL PM TML BPM EIG BW BPM LWWZ. IA EM EMZM OWQVO LWEV BPM ABIQZA PM MFXTIQVML: "Q'DM PIL BPM JWLG UWDML BW WCZ TQBBTM UWZBCIZG—AW IA VWB BW CXAMB BPM WBPMZ WTL XMWXTM, GWC CVLMZABIVL. MDMZG BQUM BPMZM'A I LMIBP PMZM, BPMG'ZM QV I VMZDWCA ABIBM NWZ BEW WZ BPZMM LIGA. EPQKP UMIVA, WN KWCZAM, MFBZI EWZS IVL EWZZG NWZ WCZ ABINN."

Διάταξη:

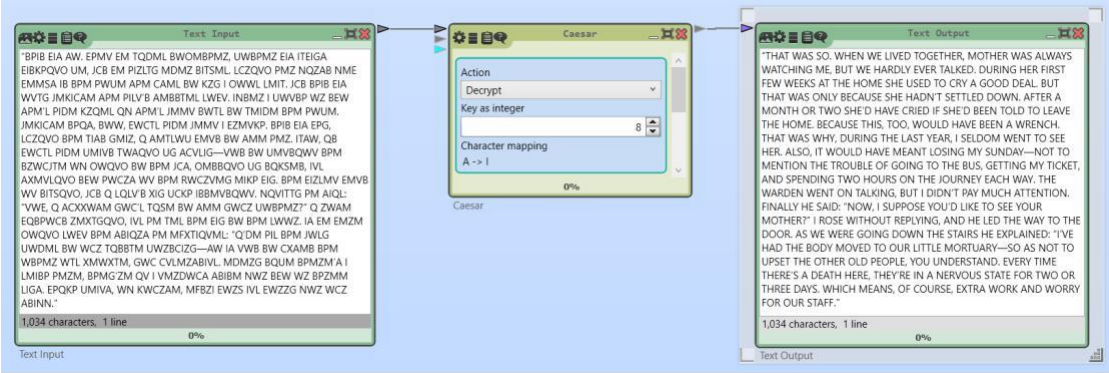


Το γράμμα που εμφανίζεται πιο συχνά στο κείμενο είναι το γράμμα "M".

Το συμπέρασμα που βγάζουμε για το κρυπτογραφημένο κείμενο είναι ότι: Εφόσον το πιο συχνό γράμμα του κρυπτοκειμένου είναι το "M", η συχνότητα του γράμματος "M" στην αγγλική γλώσσα είναι σχετικά χαμηλής τιμής (2.4) και τα πιο συχνά εμφανιζόμενα γράμματα είναι το "E", "T" και "A". Οπότε, είναι πιθανό το γράμμα "M" να αντιστοιχεί σε

κάποιο από τα πιο συχνά γράμματα της αγγλικής αλφαβήτου π.χ. “E”. Μπορούμε, με αυτόν τον τρόπο, να το αποκρυπτογραφήσουμε εύκολα.

Διάταξη:



Μπορούμε να το αποκρυπτογραφήσουμε, θεωρώντας ότι το πιο συχνό γράμμα “M” του κρυπτοκειμένου είναι (12ος χαρακτήρας) και εφόσον ο πιο συχνός χαρακτήρας της Αγγλικής αλφαβήτου είναι το “E” (4ος χαρακτήρας), αποκρυπτογραφούμε το κείμενο με κλειδί 8 (12-4 = 8). Με την πρώτη προσπάθεια, το κρυπτοκείμενο αποκρυπτογραφείται.

Αποκρυπτογραφημένο κείμενο:

“THAT WAS SO. WHEN WE LIVED TOGETHER, MOTHER WAS ALWAYS WATCHING ME, BUT WE HARDLY EVER TALKED. DURING HER FIRST FEW WEEKS AT THE HOME SHE USED TO CRY A GOOD DEAL. BUT THAT WAS ONLY BECAUSE SHE HADN’T SETTLED DOWN. AFTER A MONTH OR TWO SHE’D HAVE CRIED IF SHE’D BEEN TOLD TO LEAVE THE HOME. BECAUSE THIS, TOO, WOULD HAVE BEEN A WRENCH. THAT WAS WHY, DURING THE LAST YEAR, I SELDOM WENT TO SEE HER. ALSO, IT WOULD HAVE MEANT LOSING MY SUNDAY—NOT TO MENTION THE TROUBLE OF GOING TO THE BUS, GETTING MY TICKET, AND SPENDING TWO HOURS ON THE JOURNEY EACH WAY. THE WARDEN WENT ON TALKING, BUT I DIDN’T PAY MUCH ATTENTION. FINALLY HE SAID: “NOW, I SUPPOSE YOU’D LIKE TO SEE YOUR MOTHER?” I ROSE WITHOUT REPLYING, AND HE LED THE WAY TO THE DOOR. AS WE WERE GOING DOWN THE STAIRS HE EXPLAINED: “I’VE HAD THE BODY MOVED TO OUR LITTLE MORTUARY—SO AS NOT TO UPSET THE OTHER OLD PEOPLE, YOU UNDERSTAND. EVERY TIME THERE’S A DEATH HERE, THEY’RE IN A NERVOUS STATE FOR TWO OR THREE DAYS. WHICH MEANS, OF COURSE, EXTRA WORK AND WORRY FOR OUR STAFF.”

Ερώτηση 1.6

“***Ol aolu pumvytlk tl aoha ol dhz nvpun av haaluk aol mbulyhs, huk P aohurlk opt. Zpaapun kvdu ilopuk opz klzr, ol jyvzzlk opz zovya slnz huk slhulk ihjr. Ilzpklz aol ubyzl vu kbaf, ol avsk tl, ol huk P dvbsk il aol vusf tvbyulyz ha aol mbulyhs. Pa dhz h ybsl vm aol Ovtl aoha puthalz zovbsku’a haaluk mbulyhsz, aovbno aolyl dhz uv viqljapvu av slaapun zvtl vm aolt zpa bw ilzpkl aol jvmmpu, aol upnoa ilmvyl. “Pa’z mvy aolpy vdu zhrlz,” ol lewshpulk, “av zwhyl aolpy mllspunz. Iba pu aopz whyapjbshy puzahujl P’cl npclu wlytpzzpvu av hu vsk mypluk vm fvby tvaoly av jvtl dpao bz. Opz uhtl pz Aovthz Wéylg.” Aol dhyklu ztpslk. “Pa’z h yhaoly avbjopun spaasl zavyf pu paz dhf. Ol huk fvby tvaoly ohk iljvtl hstvza puzlwhyhisl. Aol vaoly vsk wlvwsl bzlk av alhzl Wéylg hivba ohcpun h mphujél. ‘Dolu hyl fvb nvpun av thyyf oly?’ aolf’k hzr. Ol’k abyu pa dpao h shbno. Pa dhz h zahukpun qvrl, pu mhja. Zv, hz fvb jhu nblzz, ol mllsz clyf ihksf hivba fvby tvaoly’z klhao. P aovbnoa P jvbsku’a kljluasf ylmbzl opt wlytpzzpvu av haaluk aol mbulyhs. Iba, vu vby tlkpjhs vmmpjly’z hkcpjl, P***

***mvyihkl opt av zpa bw ilzpkl aol ivkf shza upnoa." Mvy zvtl aptl dl zha aolyl dpaovba zwlhrpun. Aolu aol dhyklu nva bw huk dlua av aol dpukvd. Wylzluasf ol zhpk: "Ho, aolyl'z aol whkyl myvt Thylunv. Ol'z h ipa holhk vm aptl." Ol dhyulk tl aoha pa dvbsk ahrl bz h nvvk aoyll xbhyalyz vm hu ovby, dhsrpun av aol jobyjo, dopjo dhz pu aol cpsshnl. Aolu dl dlua kvduzahpyz. Aol wyplza dhz dhpapun qbza vbazpkl aol tvyabhyf kvvy. Dpao opt dlyl adv hjvsfalz, vul vm dovt ohk h jluzly. Aol wyplza dhz zavvwpun vcly opt, hkqbzapun aol slunao vm aol zpscly johpu vu dopjo pa obun. Dolu ol zhd bz ol zayhpnoalulk bw huk zhpk h mld dvykz av tl, hkkylzzpun tl hz, "Tf zvu." Aolu ol slk aol dhf puav aol tvyabhyf. P uvapjlk ha vujl aoha mvby tlu pu ishjr dlyl zahukpun ilopuk aol jvmmpu huk aol zjyldz pu aol spk ohk uvd illu kypclu ovtl. Ha aol zhtl tvtlua P olhyk aol dhyklu ylthyr aoha aol olhyzl ohk hyypclk, huk aol wyplza zahyapun opz wyhflyz. Aolu lclyfivkf thkl h tvcl. Ovskpun h zaypw vm ishjr jsvao, aol mvby tlu hwwyvhjolk aol jvmmpu, dopsl aol wyplza, aol ivfz, huk tfzlsm mpslk vba. H shkf P ohku'a zllu ilmvyl dhz zahukpun if aol kvvy. "Aopz pz Tvuzplby Tlbyzhbsa," aol dhyklu zhpk av oly. P kpku'a jhajo oly uhtl, iba P nhaolylk zol dhz h ubyzpun zpzaly haahjolk av aol Ovtl. Dolu P dhz puayvkbjlk, zol ivdlk, dpaovba aol ayhjl vm h ztpsl vu oly svun, nhbua mhjl. Dl zavvk hzpkl myvt aol kvvydhf av sla aol jvmmpu if; aolu, mvssvdpun aol ilhylyz kvdu h jvyypkvy, dl jhtl av aol myvua luayhujl, dolyl h olhyzl dhz dhpapun. Visvun, nsvzzf, chyupzolk ishjr hss vcly, pa chnblsf yltpuklk tl vm aol wlu ayhfz pu aol vmmpjl. Ilzpkl aol olhyzl zavvk h xbhpuasf kylzzlk spaasl -thu, dovzl kbaf pa dhz, P buklyzavvk, av zbwlycpzl aol mbulyhs, hz h zvya vm thzaly vm jlyltvuplz**."*

Το ελάχιστο μήκος κρυπτοκειμένου που οδηγεί σε ασφαλή ταυτοποίηση των τριών συνηθέστερων γραμμάτων του κρυπτογραφημένου κειμένου είναι 500 χαρακτήρες. Αυτό ισχύει, καθώς το πιο συχνά εμφανιζόμενο χαρακτήρα στο αποκρυπτογραφημένο κείμενο είναι ο χαρακτήρας "L" και για 500 χαρακτήρες ο χαρακτήρας "L" έχει τη μεγαλύτερη συχνότητα εμφάνισης 14,14%.
Το κλειδί είναι 7 (#L - #E = 11-4 = 7).

Αποκρυπτογραφημένο κείμενο:

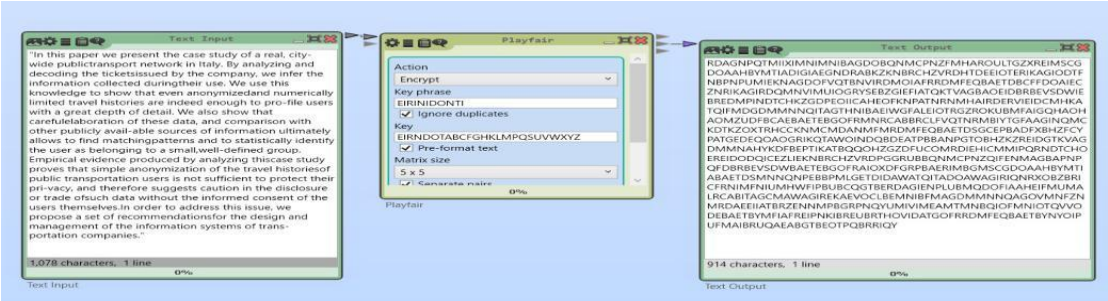
HE THEN INFORMED ME THAT HE WAS GOING TO ATTEND THE FUNERAL, AND I THANKED HIM. SITTING DOWN BEHIND HIS DESK, HE CROSSED HIS SHORT LEGS AND LEANED BACK. BESIDES THE NURSE ON DUTY, HE TOLD ME, HE AND I WOULD BE THE ONLY MOURNERS AT THE FUNERAL. IT WAS A RULE OF THE HOME THAT INMATES SHOULDN'T ATTEND FUNERALS, THOUGH THERE WAS NO OBJECTION TO LETTING SOME OF THEM SIT UP BESIDE THE COFFIN, THE NIGHT BEFORE. "IT'S FOR THEIR OWN SAKES," HE EXPLAINED, "TO SPARE THEIR FEELINGS. BUT IN THIS PARTICULAR INSTANCE I'VE GIVEN PERMISSION TO AN OLD FRIEND OF YOUR MOTHER TO COME WITH US. HIS NAME IS THOMAS PÉREZ." THE WARDEN SMILED. "IT'S A RATHER TOUCHING LITTLE STORY IN ITS WAY. HE AND YOUR MOTHER HAD BECOME ALMOST INSEPARABLE. THE OTHER OLD PEOPLE USED TO TEASE PÉREZ ABOUT HAVING A FIANCÉE. 'WHEN ARE YOU GOING TO MARRY HER?' THEY'D ASK. HE'D TURN IT WITH A LAUGH. IT WAS A STANDING JOKE, IN FACT. SO, AS YOU CAN GUESS, HE FEELS VERY BADLY ABOUT YOUR MOTHER'S DEATH. I THOUGHT I COULDN'T DECENTLY REFUSE HIM PERMISSION TO ATTEND THE FUNERAL. BUT, ON OUR MEDICAL OFFICER'S ADVICE, I FORBADE HIM TO SIT UP BESIDE THE BODY LAST NIGHT." FOR SOME TIME WE SAT THERE WITHOUT SPEAKING. THEN THE WARDEN GOT UP AND WENT TO THE WINDOW. PRESENTLY HE SAID: "AH, THERE'S THE PADRE FROM MARENGO. HE'S A BIT AHEAD OF TIME." HE WARNED ME THAT IT WOULD TAKE US A GOOD THREE QUARTERS OF AN HOUR, WALKING TO THE CHURCH, WHICH WAS IN THE VILLAGE. THEN WE WENT DOWNSTAIRS. THE PRIEST WAS WAITING JUST OUTSIDE THE MORTUARY DOOR. WITH HIM WERE TWO ACOLYTES, ONE OF WHOM HAD A CENSER. THE PRIEST WAS STOOPING OVER HIM, ADJUSTING THE LENGTH

OF THE SILVER CHAIN ON WHICH IT HUNG. WHEN HE SAW US HE STRAIGHTENED UP AND SAID A FEW WORDS TO ME, ADDRESSING ME AS, “MY SON.” THEN HE LED THE WAY INTO THE MORTUARY. I NOTICED AT ONCE THAT FOUR MEN IN BLACK WERE STANDING BEHIND THE COFFIN AND THE SCREWS IN THE LID HAD NOW BEEN DRIVEN HOME. AT THE SAME MOMENT I HEARD THE WARDEN REMARK THAT THE HEARSE HAD ARRIVED, AND THE PRIEST STARTING HIS PRAYERS. THEN EVERYBODY MADE A MOVE. HOLDING A STRIP OF BLACK CLOTH, THE FOUR MEN APPROACHED THE COFFIN, WHILE THE PRIEST, THE BOYS, AND MYSELF FILED OUT. A LADY I HADN’T SEEN BEFORE WAS STANDING BY THE DOOR. “THIS IS MONSIEUR MEURSAULT,” THE WARDEN SAID TO HER. I DIDN’T CATCH HER NAME, BUT I GATHERED SHE WAS A NURSING SISTER ATTACHED TO THE HOME. WHEN I WAS INTRODUCED, SHE BOWED, WITHOUT THE TRACE OF A SMILE ON HER LONG, GAUNT FACE. WE STOOD ASIDE FROM THE DOORWAY TO LET THE COFFIN BY; THEN, FOLLOWING THE BEARERS DOWN A CORRIDOR, WE CAME TO THE FRONT ENTRANCE, WHERE A HEARSE WAS WAITING. OBLONG, GLOSSY, VARNISHED BLACK ALL OVER, IT VAGUELY REMINDED ME OF THE PEN TRAYS IN THE OFFICE. BESIDE THE HEARSE STOOD A QUAINTLY DRESSED LITTLE - MAN, WHOSE DUTY IT WAS, I UNDERSTOOD, TO SUPERVISE THE FUNERAL, AS A SORT OF MASTER OF CEREMONIES.

Ερώτηση 1.7

“***In this paper we present the case study of a real, city-wide publictransport network in Italy. By analyzing and decoding the ticketsissued by the company, we infer the information collected duringtheir use. We use this knowledge to show that even anonymizedand numerically limited travel histories are indeed enough to pro-file users with a great depth of detail. We also show that carefulelaboration of these data, and comparison with other publicly avail-able sources of information ultimately allows to find matchingpatterns and to statistically identify the user as belonging to a small,well-defined group. Empirical evidence produced by analyzing thiscase study proves that simple anonymization of the travel historiesof public transportation users is not sufficient to protect their pri-vacy, and therefore suggests caution in the disclosure or trade ofsuch data without the informed consent of the users themselves.In order to address this issue, we propose a set of recommendationsfor the design and management of the information systems of trans-portation companies***.”

Διάταξη:



Κρυπτογραφημένο κείμενο:

RDAGNPQTMIIXIMNIMNIBAGDOBQNMCPNZFMHAROULTGZXREIMSCGDOAAHBYMTIADIGIA
EGNDRABKZKNBRCHZVRDHTDEEIOTERIKAGIODTFNBPNPUMIEKNAGDOFVQTBNVIRDMOIAFR
RDMFEQBAETDBCFFDOAIECZNRIKAGIRDQMNVIMUIOGRYSEBZGIEFIATQKTVAGBAOEIDBRBE
VSDWIEBREDMPINDTCHKZGDPEOIICAHEOFKNPATNRNMHAIRDERVIEIDCMHKATQIFMDGDM
MNNQITAGTHNIBAEIWGFALEIOTRGZROKUBMFAIGQHAOHAOMZUDFBCAEBAETEBGOFRMN
RCABBRCLFVQTNRMBIYTGFAAGINQMCKDTKZOXTRHCCKNMCMDANMFMRDMFEQBAETDSG

CEPBADFXBHZFCYPATGEDEQOAOGRIKQTAWOINDQBDEATPBBANPGTOBHZKZREIDGTKVAGD
MMNAHYKDFBEPTIKATBQQOHZGZDFUCOMRDIEHICMMIPQRNDTCHOEREIDODQICEZLIEKNB
RCHZVRDPGGRUBBQNMCPNZQIFENMAGBAPNPQFDBRBEVSDWBAETEBGOFRAIOXDFGRPBA
ERIMBGMSCGDOAAHBYMTIABAETDSMNNQNPEBBPMLGETDIDAWATQITADOAWAGIRIQNRX
OBZBRICFRNIMFNIUMHWFIPBUBCQGTBERDAGIENPLUBMQDOFIAAHEIFMUMALRCABITAGC
MAWAGIREKAEVOCLBEMNIBFMAGDMMNNQAGOVMNFZNMRDAEEIIATBRZENNMPBGRPNQ
YUMIVIMEAMTMNBQIOFMNIOTQVVODEBAETBYMFIAFREIPNKIBREUBRTHOVIDATGOFRRDM
FEQBAETBYNYOIPUFMAIBRUQAEABGTBEOTPQBRRIQY

E	I/J	R	N	D
O	T	A	B	C
F	G	H	K	L
M	P	Q	S	U
V	W	X	Y	Z

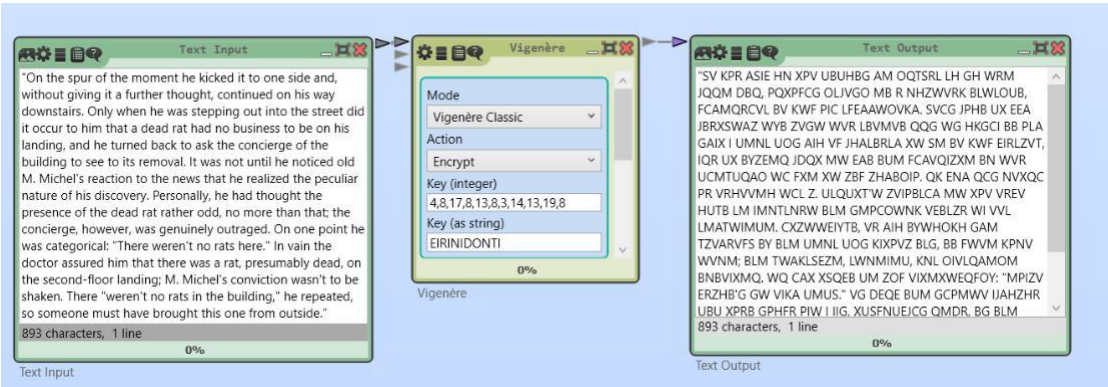
Ερώτηση 1.8

BG	AF	JY	ER	NI	OP	EW	NA	MI	TH
TK	OH	NW	IN	DR	TM	IV	RB	PE	AG

Ερώτηση 1.9

"***On the spur of the moment he kicked it to one side and, without giving it a further thought, continued on his way downstairs. Only when he was stepping out into the street did it occur to him that a dead rat had no business to be on his landing, and he turned back to ask the concierge of the building to see to its removal. It was not until he noticed old M. Michel's reaction to the news that he realized the peculiar nature of his discovery. Personally, he had thought the presence of the dead rat rather odd, no more than that; the concierge, however, was genuinely outraged. On one point he was categorical: "There weren't no rats here." In vain the doctor assured him that there was a rat, presumably dead, on the second-floor landing; M. Michel's conviction wasn't to be shaken. There "weren't no rats in the building," he repeated, so someone must have brought this one from outside***."

Διάταξη:

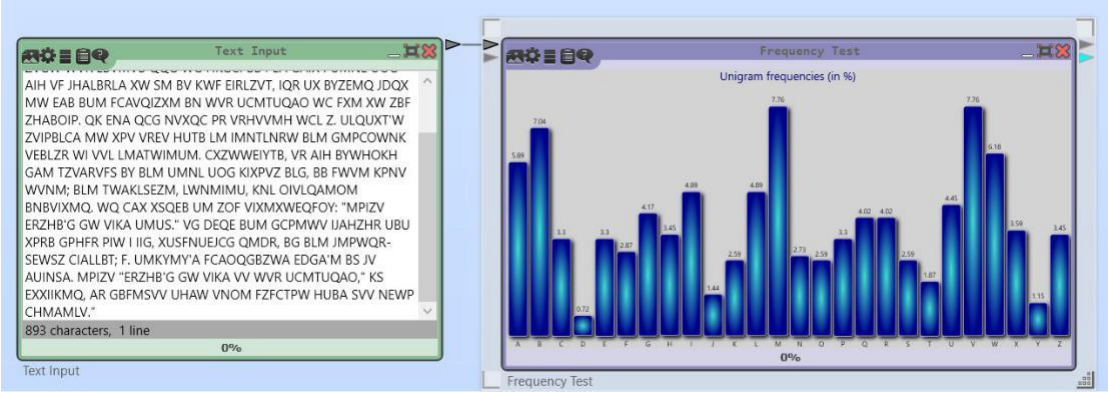


Κρυπτογραφημένο κείμενο:

“SV KPR ASIE HN XPV UBUHBG AM OQTSRL LH GH WRM JQQM DBQ, PQXPFCG OLJVGO MB R NHZWVRK BLWLOUB, FCAMQRCVL BV KWF PIC LFEAAWOVKA. SVCG JPHB UX EEA JBRXSWAZ WYB ZVGW WVR LBVMVB QQG WG HKGCI BB PLA GAIX I UMNL UOG AIH VF JHALBRLA XW SM BV KWF EIRLZVT, IQR UX BYZEMQ JDQX MW EAB BUM FCAVQIZXM BN WVR UCMTUQAO WC FXM XW ZBF ZHABOIP. QK ENA QCG NVXQC PR VRHVVMH WCL Z. ULQUXT'W ZVIPBLCA MW XPV VREV HUTB LM IMNTLNRW BLM GMPCOWNK VEBLZR WI VVL LMATWIMUM. CXZWWEIYTB, VR AIH BYWHOKH GAM TZVARVFS BY BLM UMNL UOG KIXPVZ BLG, BB FWVM KPNV WVNM; BLM TWAKLSEZM, LWNMIMU, KNL OIVLQAMOM BNBVIXMQ. WQ CAX XSQEB UM ZOF VIXMXWEQFOY: "MPIZV ERZHB'G GW VIKA UMUS." VG DEQE BUM GCPMWV IJAHZHR UBU XPRB GPHFR PIW I IIG, XUSFNUEJCG QMDR, BG BLM JMPWQR-SEWSZ CIALLBT; F. UMKYMY'A FCAOQGBZWA EDGA'M BS JV AUINSA. MPIZV "ERZHB'G GW VIKA VV WVR UCMTUQAO," KS EXXIIKMQ, AR GBFMSVV UHAW VNOM FZFCTPW HUBA SVV NEWP CHMAMLV.”

Ερώτηση 1.10

Διάταξη:



Ερώτηση 1.11

Παρατηρούμε ότι ο αλγόριθμος Caesar είναι πιο εύκολος να “σπάσει”, καθώς η συχνότητα των γραμμάτων δεν είναι ομοιόμορφη στο διάγραμμα ανάλυσης συχνοτήτων, οπότε, είναι πιθανό, το γράμμα με τη μεγαλύτερη συχνότητα στο κείμενο να αντιστοιχίζεται στο γράμμα με τη μεγαλύτερη συχνότητα στην Αγγλική αλφάβητο, όπως αναλύσαμε στα ερωτήματα 1.5 και 1.6. Αυτό συμβαίνει, καθώς ο αλγόριθμος Caesar είναι αλγόριθμος ολίσθησης. Αντίθετα, η ανάλυση συχνοτήτων στην περίπτωση του αλγορίθμου Vigenere είναι πιο ομοιόμορφη, με αποτέλεσμα να μην είναι τόσο εύκολη η αντιστοιχία των κρυπτογραφημένων γραμμάτων στα αποκρυπτογραφημένα.

Ερώτηση 1.12

PT = **MIRTO**

CT = **ROMIR**

Βάσει του δοσμένου πίνακα με την κωδικοποίηση χαρακτήρων μετατρέπουμε τα PT και CT ως εξής:

PT = 011 010 101 110 100

CT = 101 100 011 010 101

Από τη σχέση ci = pi xor ki για τον αλγόριθμο Vernam Cipher:

key = 110 110 110 100 001 ή TTTOK

Ερώτηση 1.13

CT1="***KTSMM***" και CT2="***OTRSO***"

PT1[1]=T και PT2[3]=K

Βάσει του δοσμένου πίνακα με την κωδικοποίηση χαρακτήρων μετατρέπουμε τα CT1, PT1 και PT2, CT2 ως εξής:

CT1 = 001 110 111 011 011

CT2 = 100 110 101 111 100

PT1[1] = 110

PT2[3] = 001

Από τη σχέση: CT1 = PT1 xor key

key1[1] = 111, αντιστοιχεί στο S

key2[3] = 100, αντιστοιχεί σε O

Εφόσον τα κλειδιά είναι ίδια για τους χαρακτήρες που δίνονται, τότε:

PT2[1] = 011, αντιστοιχεί στο M

PT1[3] = 011, αντιστοιχεί στο M

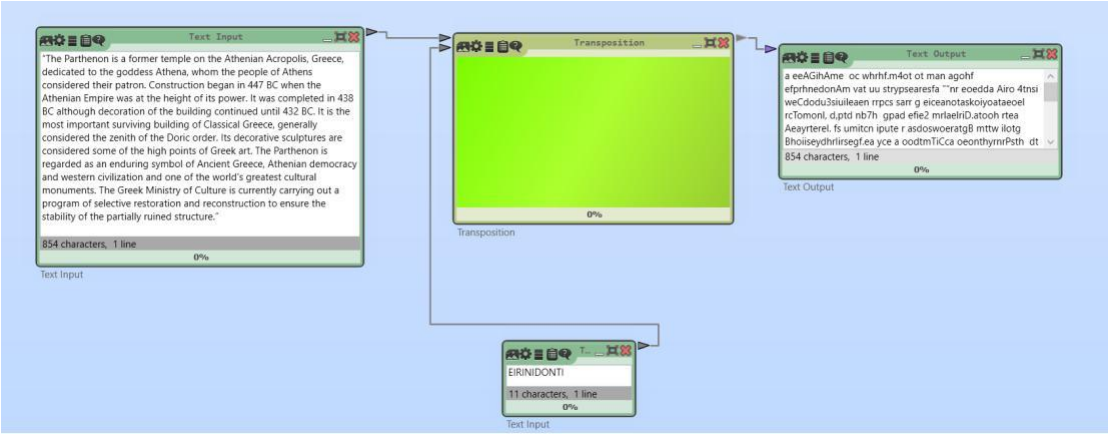
Άρα έχουμε τα εξής:

PT1 = T_ M _ _ και PT2 = M _K_ _. Οπότε, τα ονόματα μπορεί να είναι PT1 = TIMOS και PT2 = MAKIS.

Ερώτηση 1.14

"***The Parthenon is a former temple on the Athenian Acropolis, Greece, dedicated to the goddess Athena, whom the people of Athens considered their patron. Construction began in 447 BC when the Athenian Empire was at the height of its power. It was completed in 438 BC although decoration of the building continued until 432 BC. It is the most important surviving building of Classical Greece, generally considered the zenith of the Doric order. Its decorative sculptures are considered some of the high points of Greek art. The Parthenon is regarded as an enduring symbol of Ancient Greece, Athenian democracy and western civilization and one of the world's greatest cultural monuments. The Greek Ministry of Culture is currently carrying out a program of selective restoration and reconstruction to ensure the stability of the partially ruined structure.***"

Διάταξη:



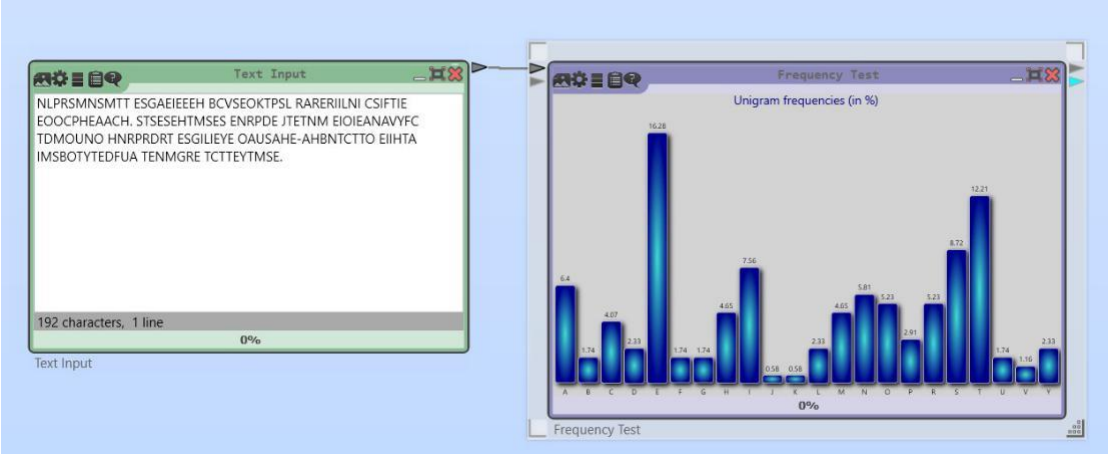
Κρυπτογραφημένο κείμενο:

a eeAGihAme oc whrhf.m4ot ot man agohf efprhnedonAm vat uu strypsearesfa ”“nr eoedda Airo 4tnsi weCdodu3siuileaen rrpcs sarr g eiceanotaskoiyoataeoel rcTomonl, d,ptd nb7h gpad efie2 mrlaelriD.atooh rtea Aeayrterel. fs umitcn ipute r asdoswoeratgB mttw ilotg BhoiiseydhrIirsegf.ea yce a oodtmTiCca oeonthyrnrPsth dt olsdrun titoro haecn. tigc ctocsesdo GTodnbe edi scneilrr r t oid.eoehpceone siCn4 aaes tB ln4i suCrrdeeeol et a snfrnatzowarte l rcrririe u i tn,e shpnetraCAp ecntrh uCervni, itvei h nremi,dncnf' ohnuuraf nsoe teet pArea htooh.inen iIl8goutltst f ns trecretie i r hcelderterrrnnoltdcsatltram crcet ctntiheee p3uibniIongolene odsar oee dulttowinhglmGtueiresnunt lshnenii te ehepse eEahos ac nd tpvdscleto tunmiothgnsncn ni ls M ct vio ttaiuhfltoetgehfne o niwhtte hnii t b GeizhdcuedhnkPsaioGersi euneyetggeo tubhyr

Ερώτηση 1.15

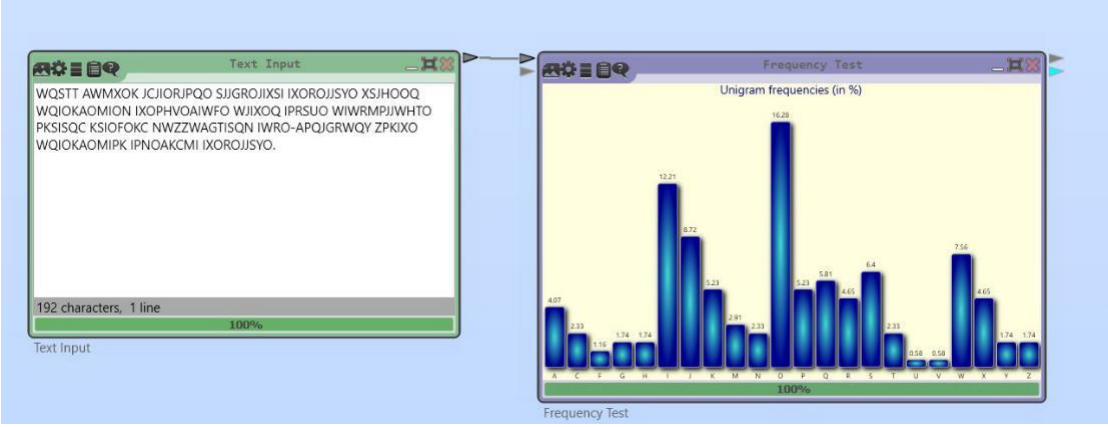
Κρυπτοκείμενο 1

NLPRSMNSMTT ESGAEIEEEH BCVSEOKTPSL RARERIILNI CSIFTIE EOOCPHEAACH. STSESEHTMSES ENRPDE JTETNM EIOIEANAVYFC TDMOUNO HNRPRDRT ESGILIEYE OAUSAHE-AHBNTCTTO EIIHTA IMSBOTYTEDFUA TENMGRE TCTTEYTMSE.



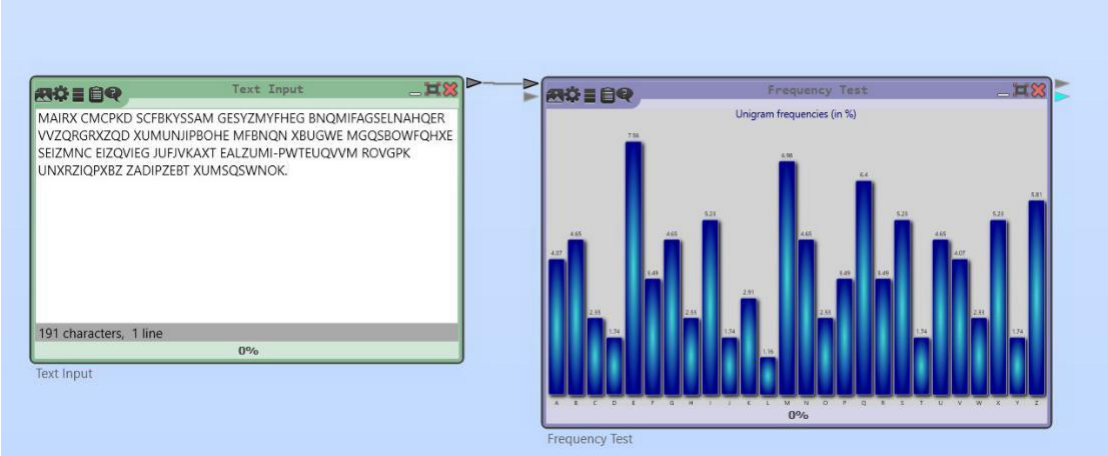
Κρυπτοκείμενο 2

WQSTT AWMXOK JCJIORJPQO SJJGROJIXSI IXOROJJSYO XSJHOOQ WQIOKAOMION IXOPHVOAIWFO WJIXOQ IPRSUO WIWRMPJJWHTO PKSISQC KSIOFOKC NWZZWAGTISQN IWRO-APQJGRWQY ZPKIXO WQIOKAOMIPK IPNOAKCMI IXOROJJSYO.



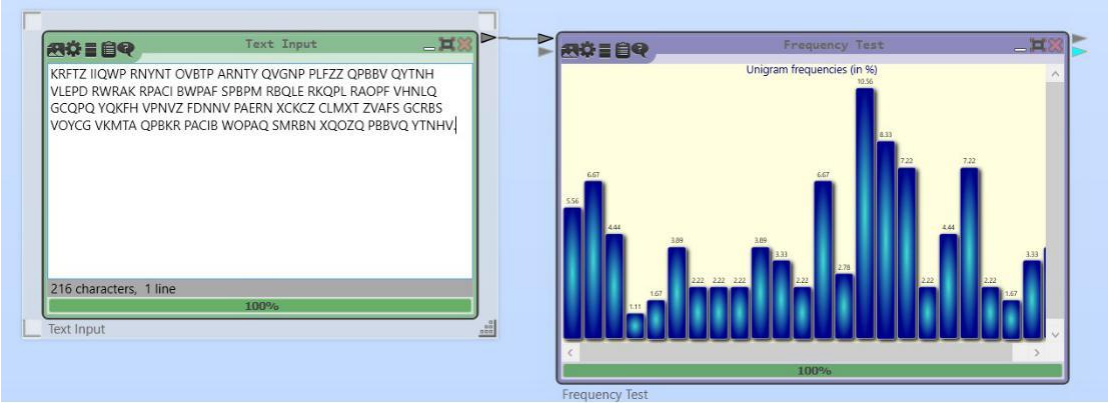
Κρυπτοκείμενο 3

MAIRX CMCPKD SCFBKYSSAM GESYZMYFHEG BNQMIFAGSELNAHQER VVZQRGRXZQD XUMUNJIPBOHE MFBNQN XBUGWE MGQSBOWFQHXE SEIZMNC EIZQVIEG JUFJVKAXT EALZUMI-PWTEUQVVM ROVGPK UNXRZIQPXBZ ZADIPZEBT XUMSQSWNOK.



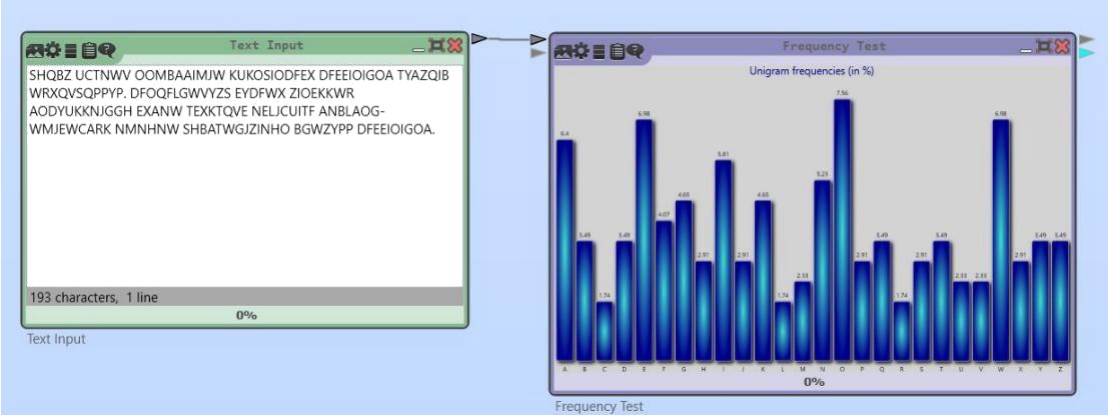
Κρυπτοκείμενο 4

KRFTZ IIQWP RNYNT OVBTP ARNTY QVGNP PLFZZ QPBBV QYTNH VLEPD RWRAK RPACI BWPAF SPBPM RBQLE RKQPL RAOPF VHNLQ GCQPQ YQKFH VPNVZ FDNNV PAERN XCKCZ CLMXT ZVAFS GCRBS VOYCG VKMTA QPBKR PACIB WOPAQ SMRBN XQOZQ PBBVQ YTNHV.



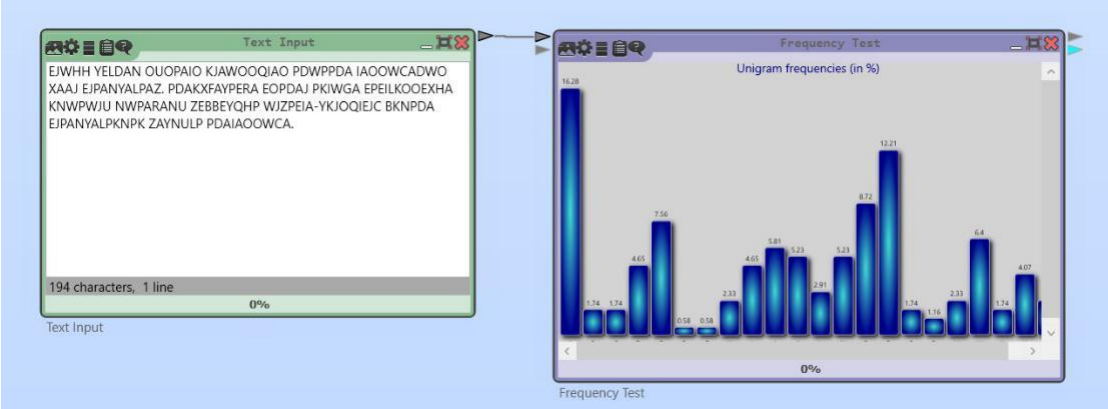
Κρυπτοκείμενο 5

SHQBZ UCTNWV OOMBAAIMJW KUKOSIODFEX DFEEIOIGOA TYAZQIB WRXQVSQPPYP. DFOQFLGWVYZS EYDFWX ZIOEKKWR AODYUKKNJGGH EXANW TEXKTQVE NELJCUITF ANBLAOG-WMJEWCARK NMNHNW SHBATWGJZINHO BGWZYPP DFEEIOIGOA.



Κρυπτοκείμενο 6

EJWHH YELDAN OUOPAIO KJAWOOQIAO PDWPPDA IAOOWCADWO XAAJ EJPANYALPAZ. PDAKXFAYPERA EOPDAJ PKIWGA EPEILKOOEXHA KNWPWJU NWPARANU ZEBBEYQHP WJZPEIA-YKJOQIEJC BKNPDA EJPANYALPKNPK ZAYNULP PDAIAOOWCA.



Γράμμα	Κρυπτ/μενο1	Κρυπτ/μενο2	Κρυπτ/μενο3	Κρυπτ/μενο4	Κρυπτ/μενο5	Κρυπτ/μενο6
A						16.28
B						
C					1.74	
D			1.74	1.11		
E	16.28		7.56	1.67	6.98	
F		1.16				0.58
G						0.58
H						
I		12.21				
J	0.58	8.72	1.74			
K	0.58					
L			1.16		1.74	

M			6.98			
N						
O		16.28			7.56	8.72
P				10.56		12.21
Q			6.4	8.33		
R				7.22	1.74	1.16
S	8.72					
T	12.21					
U		0.58				
V	1.16	0.58				
W					6.98	
X						
Y						
Z						