

## Πρώτη Εργαστηριακή Άσκηση: Φύλλο Απαντήσεων Κλασικοί Αλγόριθμοι Κρυπτογράφησης

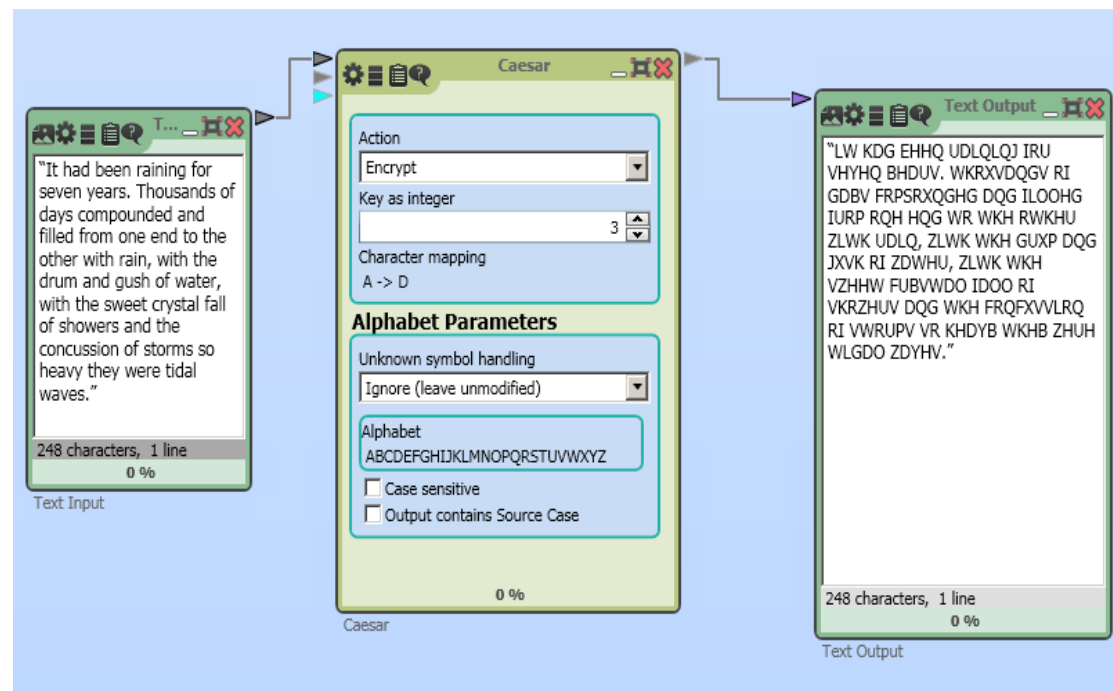
Ονοματεπώνυμο: Μιχάλης Παπαδοπουλλος

Αριθμός Μητρώου: 03114702

Εξάμηνο: 8

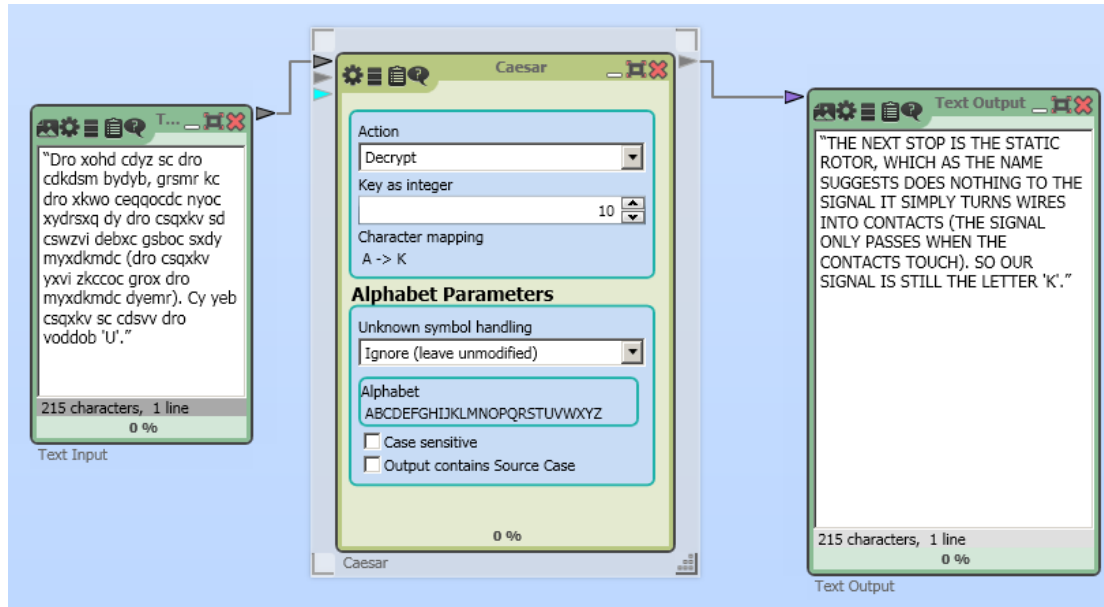
### Ερώτηση 1.1

***“It had been raining for seven years. Thousands of days compounded and filled from one end to the other with rain, with the drum and gush of water, with the sweet crystal fall of showers and the concussion of storms so heavy they were tidal waves.”***

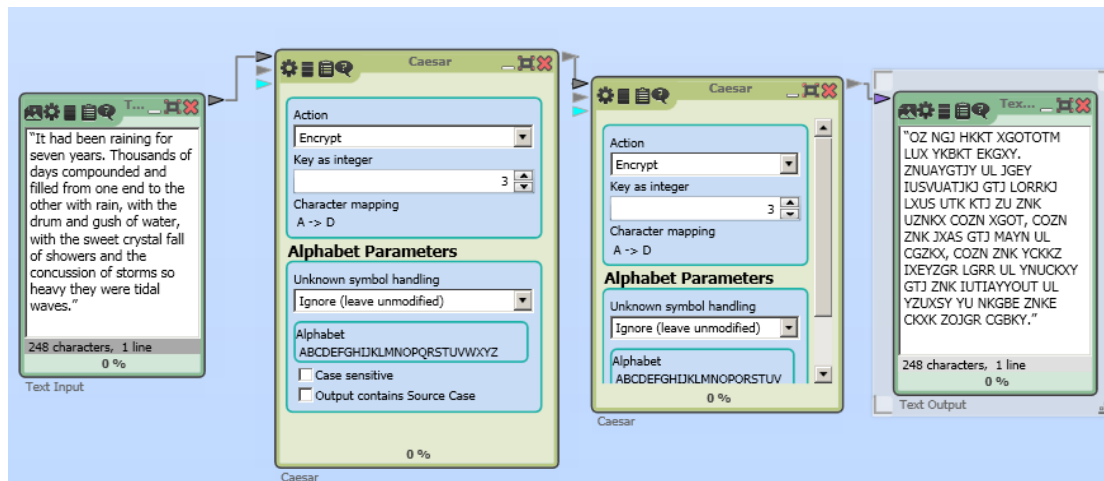


## Ερώτηση 1.2

*“Dro xohd cdyz sc dro cdkdsm bydyb, grsmr kc dro xkwo ceqqocdc nyoc xydrsxq dy dro csqxkv sd cswzvi debxc gsboc sxdy myxdkmdc (dro csqxkv yxvi zkccoc grox dro myxdkmdc dyemr). Cy yeb csqxkv sc cdsvv dro voddob 'U'.”*



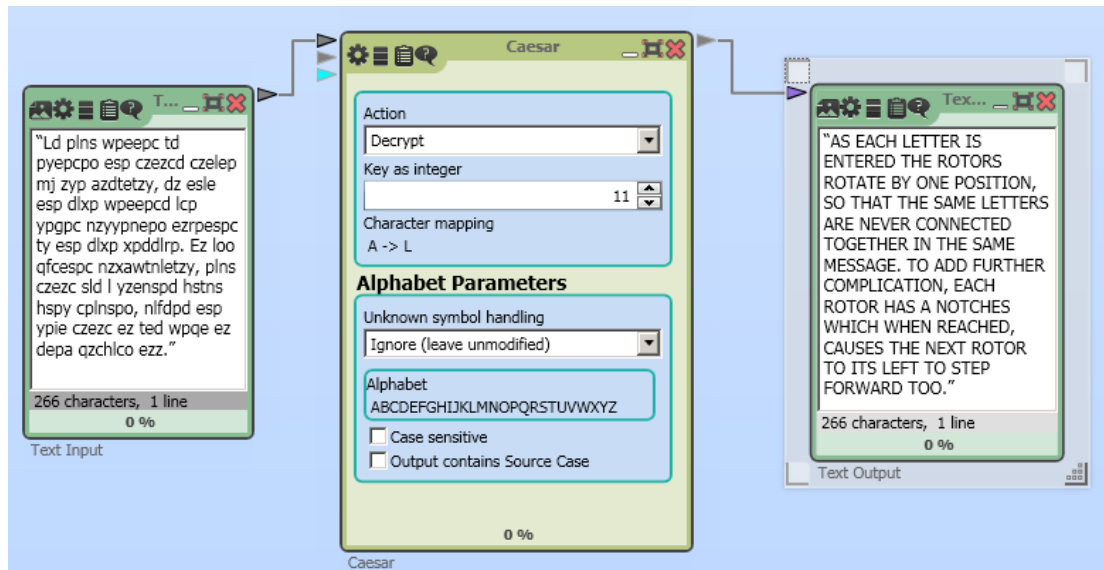
## Ερώτηση 1.3



Πρέπει  $K = 13$ , ώστε  $2K=26$  οπότε  $A \rightarrow A$

## Ερώτηση 1.4

*"Ld plns wpeepc td pyepcpo esp czezc czelep mj zyp azdtetzy, dz esle esp dlxp wpeepcd lcp ypgpc nzyypnepo ezrpespc ty esp dlxp xpddlrp. Ez loo qfcespc nxawtnletzy, plns czezc sl d l yzenspd hstns hspy cplnsपो, nlfddp esp ypie czezc ez ted wpqe ez depa qzchlco ezz."*



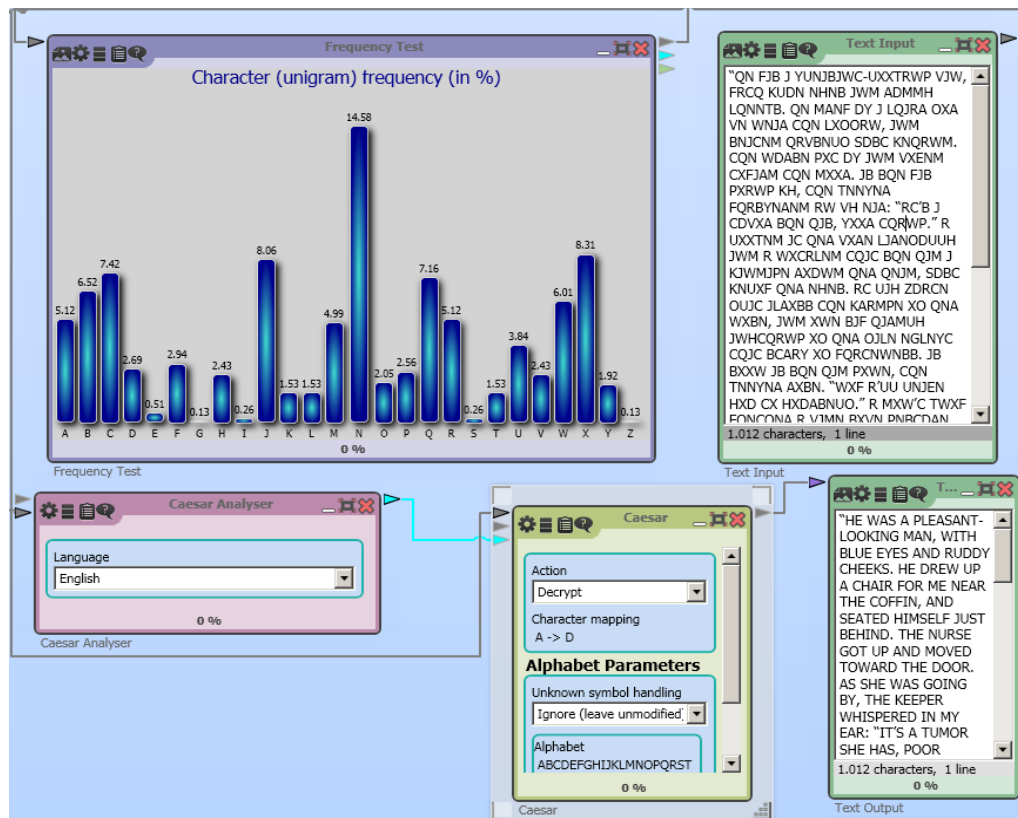
K = 11

## Ερώτηση 1.5

**"QN FJB J YUNJBJWC-UXSTRWP VJW, FRCQ KUDN NHNB JWM ADMMH LQNTB. QN MANF DY J LQJRA OXA VN WNJA CQN LXOORW, JWM BNJCNM QRVBNUO SDBC KNQRWM. CQN WDABN PXC DY JWM VXENM CXFJAM CQN MXXA. JB BQN FJB PXRWP KH, CQN TNNYNA FQRBYNANM RW VH NJA: "RC'B J CDVXA BQN QJB, YXXA CQRWP." R UXXTNM JC QNA VXAN L JANODUUH JWM R WXCRLNM CQJC BQN QJM J KJWMJPN AXDWM QNA QNJM, SDBC KNUXF QNA NHNB. RC UJH ZDRCN OUJC JLXBB CQN KARMPN XO QNA WXBW, JWM XWN BJF QJAMUH JWHCQRWP XO QNA OJLN NGLNYC CQJC BCARY XO FQRCNWNBB. JB BXXW JB BQN QJM PXWN, CQN TNNYNA AXBN. "W XF R'UU UNJEN HXD CX HXDABNUO." R MXW'C TWXF FQNCQNA R VJMN BXVN PNBCDAN, KDC RWBCNJM XO PXRWP QN QJUCNM KNQRWM VH LQJRA. CQN BNWBJCRXW XO BXVNXWN YXBCNM JC VH KJLT VJMN VN DWLXVOXACJKUN. CQN BDW FJB PNCCRWP UXF JWM CQN FQXUN AXXV FJB OUXXMNM FRCQ J YUNJBJWC, VNUUXF URPQC. CFX QXAWNCB FNAN KDIIRWP XENAQNJM, JPJRWBC CQN BTHURPQC. R FJB BX BUNNYH R LXDUM QJAMUH TNNY VH NHNB XYNW. FRCQXDC UXSTRWP AXDWM, R JBTNM CQN TNNYNA QXF UXWP QN'M KNNW JC CQN QXVN. "OREN HNJAB."**

"HE WAS A PLEASANT-LOOKING MAN, WITH BLUE EYES AND RUDDY CHEEKS. HE DREW UP A CHAIR FOR ME NEAR THE COFFIN, AND SEATED HIMSELF JUST BEHIND. THE NURSE GOT UP AND MOVED TOWARD THE DOOR. AS SHE WAS GOING BY, THE KEEPER WHISPERED IN MY EAR: "IT'S A TUMOR SHE HAS, POOR THING." I LOOKED AT HER MORE CAREFULLY AND I NOTICED THAT SHE HAD A BANDAGE ROUND HER HEAD, JUST BELOW HER EYES. IT LAY QUITE FLAT ACROSS THE BRIDGE OF HER NOSE, AND ONE SAW HARDLY ANYTHING OF HER FACE EXCEPT THAT STRIP OF WHITENESS.

AS SOON AS SHE HAD GONE, THE KEEPER ROSE. "NOW I'LL LEAVE YOU TO YOURSELF." I DON'T KNOW WHETHER I MADE SOME GESTURE, BUT INSTEAD OF GOING HE HALTED BEHIND MY CHAIR. THE SENSATION OF SOMEONE POSTED AT MY BACK MADE ME UNCOMFORTABLE. THE SUN WAS GETTING LOW AND THE WHOLE ROOM WAS FLOODED WITH A PLEASANT, MELLOW LIGHT. TWO HORNETS WERE BUZZING OVERHEAD, AGAINST THE SKYLIGHT. I WAS SO SLEEPY I COULD HARDLY KEEP MY EYES OPEN. WITHOUT LOOKING ROUND, I ASKED THE KEEPER HOW LONG HE'D BEEN AT THE HOME. "FIVE YEARS."



## Ερώτηση 1.6

“PU AOL WHNLZ AV MVSSVD P ZOHSS UVA PUKBSNL PU KLZJYPWAPVUZ VM WLYZVUZ—LEJLWA DOLU H MHJPHS LEWYLZZPVU, VY H NLZABYL, HWWLHYZ HZ H ZPNU VM H TBAL IBA LSVXBLUA SHUNBHN—ILJHBZL, HZ IVLAOPBZ ZHFZ, UVAOPUN PZ TVYL MSLLAPUN AOHU LEALYUHS MVYT, DOPJO DPAOLYZ HUK HSALYZ SPRL AOL MSVDLYZ VM AOL MPLSK HA AOL HWWLHYHUJL VM HBABTU; HUK DOHA DVBSK IL AOL WVPUA VM ZHFPUN AVKHF AOHU AOL HIIVA HIV OHK H ZALYU LFL HUK WHSL JOLLRZ, DOLU IF UVD OL HUK AOVZL HYVBUK OPT HYL KBZA HUK AOLPY IVKPLZ OHCL AOL TVYAH S NYHFULZZ VM KBZA (VUSF AOLPY ZVBSZ, NVK NYHUA, ZOPUPUN DPAO H SPNOA AOHU DPSS ULCLY IL LEAPUNBPZOLK)? IBA P DVBSK SPRL AV KLZJYPIL DPSSPHT HA SLHZA VUJL, ILJHBZL OPZ ZPUNBSHY MLHABYLZ ZAYBJR TL, HUK PA PZ JOHYHJALYPZAPJ VM AOL FVBUN AV ILJVTI IVBUK AV HU VSKLY HUK DPZLY THU UVA VUSF IF AOL ZWLSS VM OPZ DVYKZ HUK AOL ZOHYWULZZ VM OPZ TPUK, IBA HSZV IF AOL ZBWL YMPJPHS MVYT VM OPZ IVKF, DOPJO WYVCLZ CLYF KLHY, SPRL AOL MPNBYL VM H MHAOLY, DOVZL NLZABYLZ DL ZABKF HUK DOVZL MYVDUZ, DOVZL ZTPSL DL VIZLYCL—DPAOVBA H ZOHKVD VM SBZA AV WVSSBAL AOPZ MVYT (WLYOHWZ AOL VUSF AOHU PZ AYBSF WBYL) VM JYVWVYHS SVCL. PU AOL WHZA TLU DLYL OHUKZVTI HUK NYLHA (UVD AOL F HYL JOPSKYLU HUK KDHYMZ), IBA AOPZ PZ TLYLSF VUL VM AOL THUF MHJAZ AOHU KLTUVZAYHAL AOL KPZH ZALY VM HU HNPUN DVYSK. AOL FVBUN UV SVUNLY DHUA AV ZABKF HUFAPUN, SLHYUPUN PZ PU KLJSPUL, AOL DOVSL DVYSK DHSRZ VU PAZ OLHK, ISPUK TLU SLHK VAOLYZ LXBHSSF ISPUK HUK JHBZL AOLT AV WSBUNL PUAV AOL HIFZZ, IPYKZ SLHCL AOL ULZA ILMVYL AOL F JHU MSF, AOL QHJRHZZ WSHFZ AOL SFYL, VELU KHUJL. THYF UV SVUNLY SVCLZ AOL JVUALTWSHAPCL SPML HUK THYAOH UV SVUNLY SVCLZ AOL HJAPCL SPML, SLHO PZ ZALYPSL, YHJOLS OHZ H JHYUHS LFL, JHAV CPZPAZ IYVAOLSZ, SBJYLAPBZ ILJVTI H DVTHU. LCLYFAOPUN PZ VU AOL DYVUN WHAO. PU AOVZL KH FZ, AOHUR NVK, P HJXBPYK MYVT TF THZALY AOL KLZPYL AV SLHYU HUK H ZLUZL VM AOL ZAYHPNOA DHF, DOPJO YLTHPUZ LCLU DOLU AOL WHAO PZ AVYABVBZ. IYVAOLY DPSSPHT’Z WOFZPJHS HWWLHYHUJL DHZ HA AOHU APTL ZBJO HZ AV HAAYHJA AOL HAALUAPVU VM AOL TVZA PUHAALUAPCL VIZLYCLY. OPZ OLPNOA ZBYWHZZLK AOHU VM H UVYTHS THU HUK OL DHZ ZV AOPU AOHU OL ZLLTLK ZAPSS AHSSLY. OPZ LFLZ DLYL ZOHYW HUK WLULAYHAPUN; OPZ AOPU HUK ZSPNOASF ILHRF UVZL NHCL OPZ JVBUALUHUJL AOL LEWYLZZPVU VM H THU VU AOL SVVRVBA, ZHCL PU JLYAHPU TVTLUAZ VM ZSBNNPZOULZZ VM DOPJO P ZOHSS ZWLHR. OPZ JOPU HSZV KLUVALK H MPYT DPSS, AOVBN AOL SVUN MHJL JVCLYLK DPAO MYLJRSLZ—ZBJO HZ P VMALU ZHD HTVUN AOVZL IVYU ILADLLU OPILYUPH HUK UVYAOBTIYPH—JVBSK VJJHZPVUHSSF LEWYLZZ OLZPAHAPVU HUK WBGGS LTLUA. PU APTL P YLHSPGLK AOHU DOHA ZLLTLK H SHJR VM JVUMPKLUJL DHZ VUSF JBYPVZPAF, IBA HA AOL ILNPUUPUN P RULD SPAASL VM AOPZ CPYABL, DOPJO P AOVBN OA, YHAOLY, H WHZZPVU VM AOL JVCLAVBZ ZWPYPA. P ILSPLCLK PUZALHK AOHU AOL YHAPVUHS ZWPYPA ZOVB SK UVA PUKBSNL ZBJO WHZZPVU, IBA MLLK VUSF VU AOL AYBAO, DOPJO (P AOVBN OA) VUL RUVDZ MYVT AOL VBAZLA.”

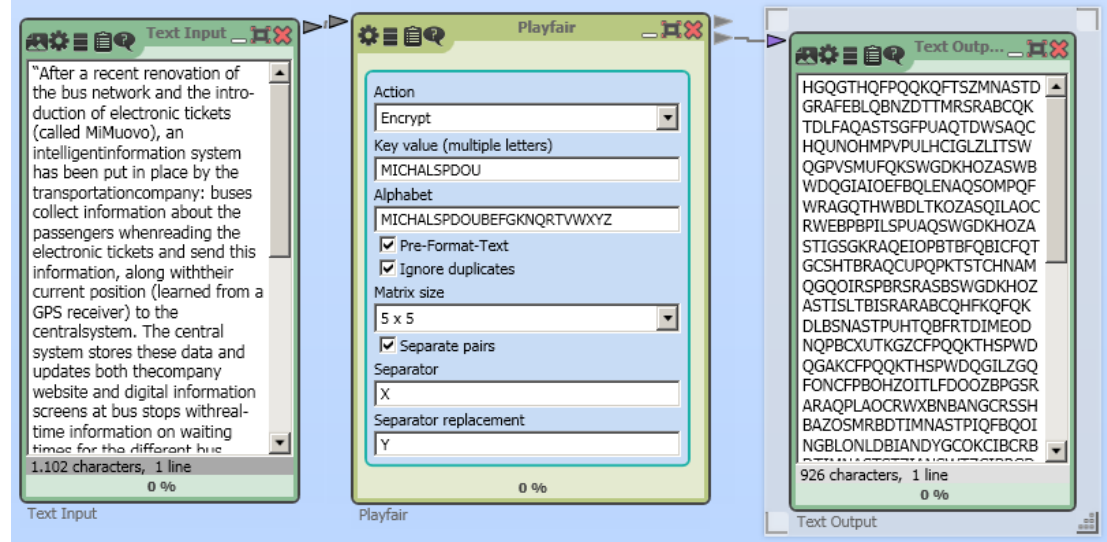
Το κλειδί μετατοπίσεως είναι  $K = 7$

## Ερώτηση 1.7

**“After a recent renovation of the bus network and the introduction of electronic tickets (called MiMuovo), an intelligent information system has been put in place by the transportation company: buses collect information about the passengers when reading the electronic tickets and send this information, along with their current position (learned from a GPS receiver) to the central system. The central system stores these data and updates both the company website and digital information screens at bus stops with real-time information on waiting times for the different bus lines. This technological system offers various advantages to the users: RFID tickets are faster to stamp, and real-time information on buses, also available through a mobile application, is precious for avoiding long waits at a bus stop. However, the amount of data collected by the system exposes the users to tracking. Personal tickets, such as monthly and yearly passes, are directly linked to a user, and both a government issued ID and the university card have to be showed upon purchase. Since each use is registered by the system.”**

NAME: MICHALIS PAPADOPOULLOS

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



HGQGT HQFPQQKQFTSZMNASTDGRAFE BLQBNZDTTMR SRABCQKTDLFAQAS TS GFPUAQTDWSAQCHQUNOHMPVPULHCIGLZLITSWQGPVSMUFQKSWGDKHOZASWBWDQGIAIOEFBQLENAQSOMPQFWRAGQTHWBDLTKOZASQILAOCRWE BPBPILSPUAQSWGDKHOZASTIGSGKRAQEIOPTBFQBICFQTGCSHTBRAQCUPQPKTSTCHNAMQGQOIRSPBR SRASBSWGD KHOZASTISLTBISRARABCQHFKQFQKDLBSNASTPUHTQBFRTDIMEODNQPBXCUTKGZCFPQQKTHSPWDQGA KC FPQQKTHSPWDQGILZGQFONCFPBOHZOITLFD OOBPGSRARAQPLAOCR WXB NBANGCRSSHBAZOSMRBDTIMNASTPIQFBQOINGBLONLDBIANDYGCOK CIBCRBDTIMNASTSTZIANSWTZCIBPGDTKCFSHEYGFQFQKEBPSSWBPRASB QGHATSSLBAHMSPWDQGALEYGFNDZMNLHGOILYITZOUFONGZCFBLFQDNB



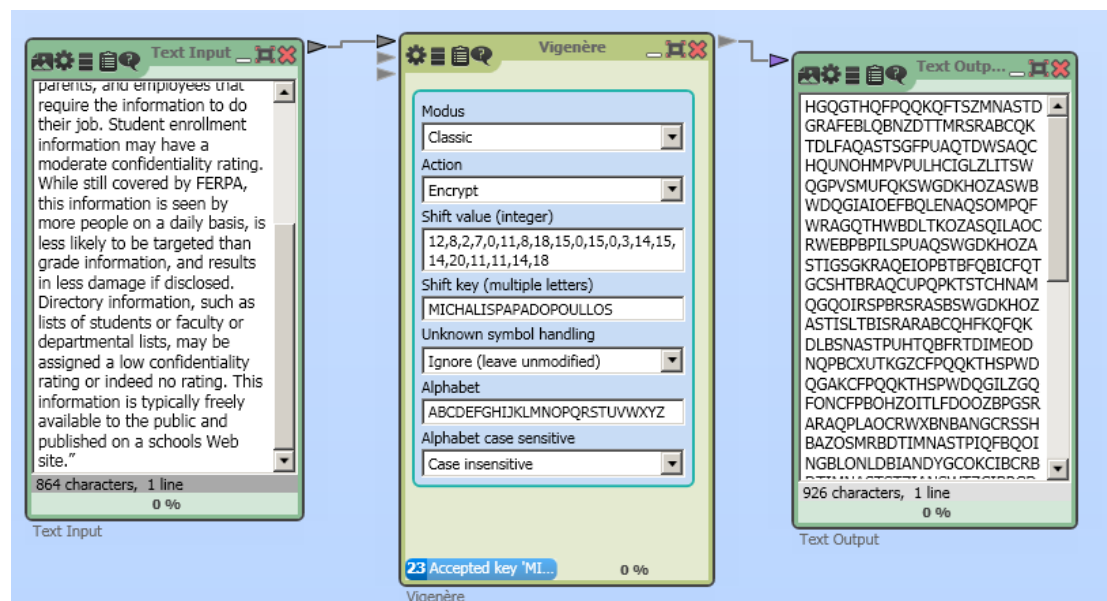
HORCHQUNOHTFGIOQGTKLPZOCLITFYGCOKCIBCRBDTIMNASTSTEBPBOISP  
 GOZMMSIGPURATDBUAMALNSPUCODSCHOZASWSPDQFHCLGDBDTMZSASH  
 TBSLTBZIANOIZOEBPWONLDADXBUTKCFMILGQKDGHOZOAPPVPUAQFPFW  
 RABPWDQGCUCELPBPRAFBPBNDZGKTMHNMTEQNDSTMONAMQGGPWLBIH  
 AIOALQKMDZHRXFHTDVOCWPBIOQFSHQFAQDVSMQNFZGMGPBTHRSG  
 SRAOTLZFQKIBQNAPWLBFPHSITORCFBKMWFQBSRZHMYFAMXUZGEFDSZF  
 PELSTLEQHAMPBBSQIQCGCHABLBCDNFUSBQGGQFSFZRCFDWONUC

## Ερώτηση 1.8

BG	AF	JY	ER	NI	OP	EW	NA	MI	TH
EU	HG	HW	FQ	WS	LD	BX	TI	IC	RA

## Ερώτηση 1.9

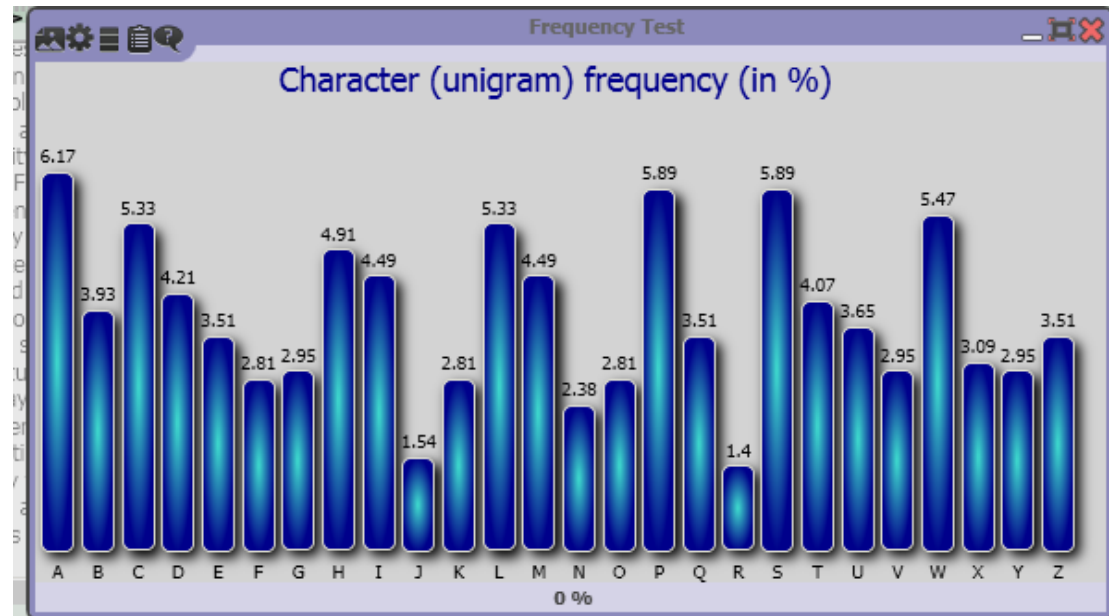
**“Student grade information is an asset whose confidentiality is considered to be highly important by students. In the United States, the release of such information is regulated by the Family Educational Rights and Privacy Act. Grade information should only be available to students, their parents, and employees that require the information to do their job. Student enrollment information may have a moderate confidentiality rating. While still covered by FERPA, this information is seen by more people on a daily basis, is less likely to be targeted than grade information, and results in less damage if disclosed. Directory information, such as lists of students or faculty or departmental lists, may be assigned a low confidentiality rating or indeed no rating. This information is typically freely available to the public and published on a schools Web site.”**



HGQGT HQFPQQKQFTSZMNASTD GRAFEBLQBNZDTTMRSRABCQK TDLFAQAS  
 TSGFPUAQTDWSAQCHQUNOHMPVPULHCIGLZLITSWQGPVSMUFQKSWGDKH  
 OZASWBWDQGIAIOEFBQLENAQSOMPQFWRAGQTHWBDLT KOZASQILAOCRW  
 EBPBPILSPUAQSWGDKHOZASTIGSGKRAQEIOPTBFQBICFQTGCSHTBRAQC  
 UPQPKTSTCHNAMQGQOIRSPBRSRASBSWGDKHOZASTISLTBISRARABCQHF  
 KQFQKDLBSNASTPUHTQBFRTDIMEODNQPBCXUTKGZCFPQKTHSPWDQGA  
 KCFPQKTHSPWDQGILZGQFONCFPBOHZOITLFDQOZBPGSRARAQPLAOCR  
 WXB NBANGCRSSHBAZOSMRBDTIMNASTPIQFBQOINGBLONLDBIANDYGCK  
 CIBCRBDTIMNASTSTZIANSWTZCIBPGDTKCFSHEYGFQFQKEBPSSWBPRASB

QGHATSSLBAHMSPWDQGALEYGFNDZMNLHGOILYITZOUFONGZCFBLFQDNB  
HORCHQUNOHTFGIOQGTKLPZOCLITFYGCOKICBCRBDTIMNASTSTEBPBOISP  
GOZMMSIGPURATDBUAMALNSPUCODSCHOZASWSPDQFHCLGDBDTMZSASH  
TBSLTBZIANOIZOEBPWONLDADXBXUTKCFMILGQKDGHOHZOAPPVPUAQFPFW  
RABPWDQGCUCELPBPRAFBPBNDZGKTMHNMTEQNDSTMONAMQGQPWLHBH  
AIOALQKMDZHRXSFHTDVOCWPBIOQFSHQFAQDVSMQNFZGMGPBTHRSG  
SRAOTLZFQKIBQNAPWLBFPHSITORCFBKMWFQBSRZHMVFAMXUZGEFDSZF  
PELSTLEQHAMPBBSQIQCGCHABLBCDNFUSBQGGQFSFZRCFDWONUC

### Ερώτηση 1.10



### Ερώτηση 1.11

Η κρυπτογραφηση Vigenere είναι πιο ανθεκτική σε επιθέσεις ανάλυσης συχνότητας, εφ'όσον χρησιμοποιεί πολλαπλές αντιστοιχίσεις (πολλαπλά αλφαβήτα). Επίσης το KEYSPACE είναι σαφώς μεγαλύτερο από του αλγορίθμου του Καισάρη και γι αυτό απαιτεί περισσότερο χρόνο για επίθεση bruteforce.

### Ερώτηση 1.12

PT = KOSTAS

001 100 111 110 000 111

CT = TOKKOT

110 100 001 001 100 110

XOR: 111 000 110 111 100 001

KEY = SATSOK



### Ερώτηση 1.13

CT1="ATSMO" και CT2="AOMSS"

PT1[1]=M και PT2[3]=K

ATSMO = 000 110 111 011 100

AOMSS = 000 100 011 111 111

PT1[1] = M    011    PT2[3] = K    001

CT1[1] = A    000    CT2[3] = M    011

XOR

KEY[1] = 011 = M

KEY[3] = 010 = I

KEY = MOIRA

      = 011 100 010 101 000

CT[1] = A = 000

PT[1] = 000 XOR 011 = 011 = M

PLAINTEXT1 = MIRTO

PLAINTEXT2 = MAKIS

000 110 111 011 100            ENCRYPTED1

011 100 010 101 000            MOIRA

===== (XOR)

011 010 101 110 100

MIRTO

MAKIS

011 000 001 010 111

000 100 011 111 111

===== (XOR)

011 100 010 101 000

MOIRA

KEY = MOIRA

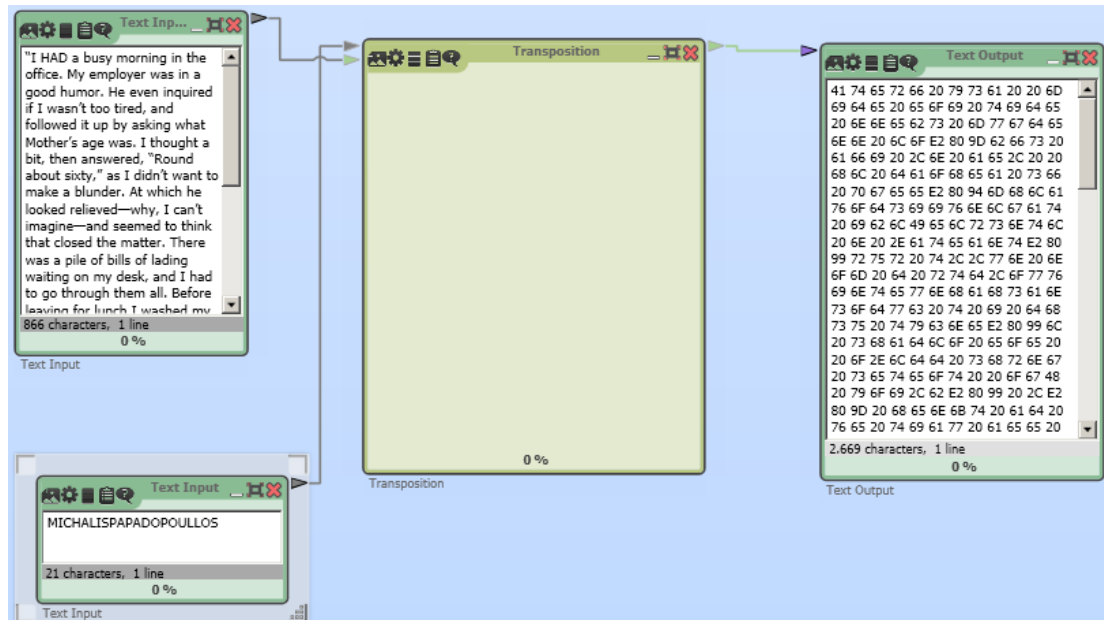
PL1 = MIRTO

PL2 = MAKIS

### Ερώτηση 1.14

*"I HAD a busy morning in the office. My employer was in a good humor. He even inquired if I wasn't too tired, and followed it up by asking what Mother's age was. I thought a bit, then answered, "Round about sixty," as I didn't want to make a blunder. At which he looked relieved—why, I can't imagine—and seemed to think that closed the matter. There was a pile of bills of lading*

*waiting on my desk, and I had to go through them all. Before leaving for lunch I washed my hands. I always enjoyed doing this at midday. In the evening it was less pleasant, as the roller towel, after being used by so many people, was sopping wet. I once brought this to my employer's notice. It was regrettable, he agreed—but, to his mind, a mere detail. I left the office building a little later than usual, at half-past twelve, with Emmanuel, who works in the Forwarding Department."*



41 74 65 72 66 20 79 73 61 20 20 6D 69 64 65 20 65 6F 69 20 74 69 64 65 20 6E 6E  
65 62 73 20 6D 77 67 64 65 6E 6E 20 6C 6F E2 80 9D 62 66 73 20 61 66 69 20 2C  
6E 20 61 65 2C 20 20 68 6C 20 64 61 6F 68 65 61 20 73 66 20 70 67 65 65 E2 80  
94 6D 68 6C 61 76 6F 64 73 69 69 76 6E 6C 67 61 74 20 69 62 6C 49 65 6C 72 73  
6E 74 6C 20 6E 20 2E 61 74 65 61 6E 74 E2 80 99 72 75 72 20 74 2C 2C 77 6E 20  
6E 6F 6D 20 64 20 72 74 64 2C 6F 77 76 69 6E 74 65 77 6E 68 61 68 73 61 6E 73  
6F 64 77 63 20 74 20 69 20 64 68 73 75 20 74 79 63 6E 65 E2 80 99 6C 20 73 68 61  
64 6C 6F 20 65 6F 65 20 20 6F 2E 6C 64 64 20 73 68 72 6E 67 20 73 65 74 65 6F  
74 20 20 6F 67 48 20 79 6F 69 2C 62 E2 80 99 20 2C E2 80 9D 20 68 65 6E 6B 74  
20 61 64 20 76 65 20 74 69 61 77 20 61 65 65 20 61 6E 6C 69 61 74 65 46 2E 49 69  
6C 75 64 65 70 65 68 65 79 74 20 65 67 69 61 6C 20 61 67 65 73 79 20 65 61 74 65  
20 6E 79 49 65 6D 49 6C 74 61 6E 65 6E 20 65 20 20 49 6E 61 61 62 52 73 6B 68  
77 61 68 2E 20 69 20 65 67 6D 6A 69 20 2C 2C 20 73 72 6C 73 65 20 74 20 75 77  
20 77 44 68 72 2E 20 61 20 20 20 E2 80 9C 61 61 63 E2 80 94 E2 80 94 74 72 66  
74 49 68 6E 20 6E 6D 67 74 6C 79 20 62 70 61 72 2C 66 67 20 74 2C 72 6E 79 6F  
71 6F 20 20 74 6E 20 77 72 20 74 74 74 20 61 65 74 6F 20 20 20 68 73 6C 6E 6F  
2E 20 69 6C 20 61 65 61 61 20 69 61 69 20 6F 75 20 69 4D 68 73 73 61 2E 72 20  
6F 68 61 64 73 68 72 49 61 74 65 20 6C 67 70 20 74 63 65 68 69 20 74 6C 45 6E 72  
E2 80 9C 20 70 68 65 72 75 68 67 72 74 20 74 69 61 68 6D 69 67 20 75 6C 61 61  
73 76 65 20 73 2C 6F 6D 20 68 20 20 69 20 70 61 68 65 20 65 20 6E 74 6F 77 2E  
65 62 6E 75 6F 63 6D 73 20 6F 6D 20 20 75 73 6F 49 20 65 20 79 20 74 20 74 2C  
20 66 6C 61 77 72 20 6F 20 20 69 74 65 61 49 20 75 74 64 65 6E 64 64 61 20 20 6F  
65 63 20 6E 20 65 72 65 70 65 69 6F 61 74 65 69 20 20 74 73 65 6E 65 64 69 74 74  
6F 6F 77 69 6E 20 65 69 20 65 20 69 6B 72 65 20 6C 68 20 70 65 20 6C 49 6F 65  
2C 69 6C 62 65 66 6D 20 74 20 6F 61 65 77 20 6B 65 74 75 49 20 68 79 64 74 54

69 67 61 20 66 20 79 64 74 61 61 6F 70 75 79 72 64 20 74 20 75 6C 68 72 75 66 20  
65 73 6F 6E 77 20 64 64 20 20 20 73 63 65 6C 6F 20 6C 72 61 64 79 77 20 74 6D  
69 68 72 67 62 65 65 69 6C 65 20 69 6D 2E 61 20 20 77 68 20 6E 6F E2 80 99 6E  
6B 61 65 65 77 66 79 67 42 6E 2E 69 6E 6C 20 62 20 77 68 6E 74 20 64 66 65 74  
69 6B 44 61 20 77 48 20 64 73 67 69 6F 20 65 20 68 6E 61 20 62 6E 68 6D 20 79  
6F 64 69 20 20 73 6F 6F 6F 20 65 61 20 61 73 65 77 61 67 6D 20 72 69 20 74 75 65  
78 74 41 6C 6D 74 20 70 6E 2C 6F 20 77 77 69 65 6C 72 75 65 20 20 2E 20 73 2E  
75 72 2D 6D 74 6D 72 4D 67 6E 6F 64 74 20 61 74 20 65 64 E2 80 99 20 20 73 6C  
64 20 66 68 49 67 74 73 6F 69 65 74 73 74 62 6F 74 63 6C 68 68 20 70

### Ερώτηση 1.15

#### Κρυπτοκείμενο 1

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

#### Κρυπτοκείμενο 2

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

#### Κρυπτοκείμενο 3

KRFTZ IIQWP RNYNT OVBTP ARNTY QVGNP PLFZZ QPBBV QYTNH VLEPD  
RWRRAK 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 4

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

#### Κρυπτοκείμενο 5

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

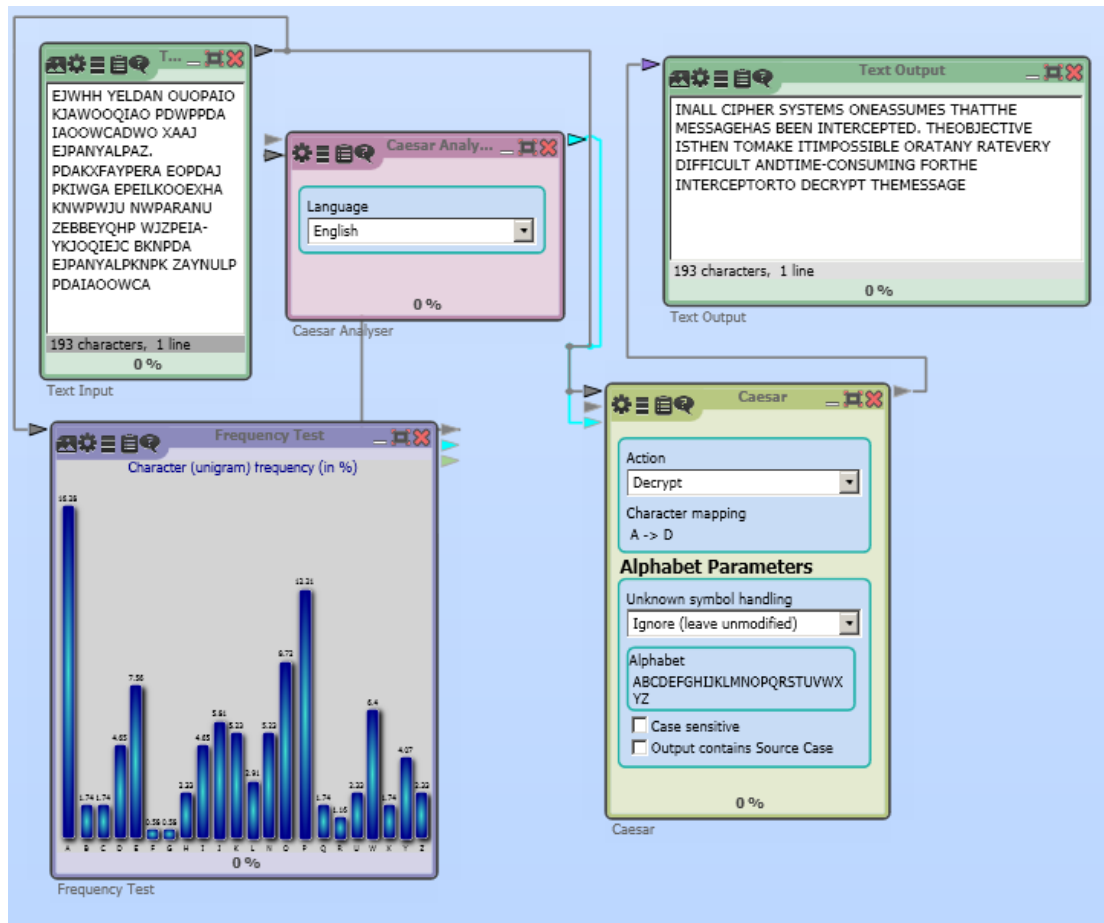
#### Κρυπτοκείμενο 6

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

Γράμ α	Κρυπτ/μενο 1	Κρυπτ/μενο 2	Κρυπτ/μενο 3	Κρυπτ/μενο 4	Κρυπτ/μενο 5	Κρυπτ/μενο 6
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						

**TIME-CONSUMING**

## Ερώτηση 1.16



Κρυπτοκειμενο 3:

Algorithm used: Caesar ( $K = 3$ )

IN ALL CIPHER SYSTEMS ONE ASSUMES THAT THE MESSAGE HAS BEEN INTERCEPTED. THE OBJECTIVE IS THEN TO MAKE IT IMPOSSIBLE OR AT ANY RATE VERY DIFFICULT AND TIME-CONSUMING FOR THE INTERCEPTOR TO DECRYPT THE MESSAGE

## Ερώτηση 1.17

## Ερώτηση 1.18

### Κρυπτοκείμενο 1

QKDCLB CDQY ACYNOGETPADXR CQKACKYHRAKDB NEALKZ R CPAD  
LXGXSRF DNUTKAIXRG ACEG QDROK YLAENN RXRTUGLT FKSL ATUK YDP  
QKKYORR APFSNG PHRAKDBYLD ITURNGECHRKV BVDVRLDWDAC  
EGKRBDWDQKD CGPHRAKA QLDGCSXHR FKDN GAUTELNEPTA PGLGL  
BASPDNP ADXRCQKLBN EALKZRCPA DLXGXSRFD NUTKAIX RGACEGT  
DCDHL NEPAISOARQ KAPGDLT UGLENBA BGNKDQLQKAADDP QKLDRQ  
KAPGD LTDCDBKB GELD XI KTERAC DHKRFBD LYDNIXQK DPLBYLDI  
TDCDDLX RPIDB HFNRPTQKKA QKGVDSGBSK GBVDIZKZ TDRADN  
DPFHAPKGD PPAOGR KNEDW

### Κρυπτοκείμενο 2

KQYI CBKYVTIRK JCXI FBKZZKDQA YAVERISAVLOJ ZNANUIP SAWPWEOOGI  
GZ LCWKJXC CVIRADIMNVIR ZNIQCHZFCT CDZNI QCAYQNEKZ ROVFWMK  
OMXTMT MN DBM ROKZ YAVECLIRZNI LKDJOA VIRKTQF ANTLBMQT  
ROVFNCVYCSN GCQZ UYHCJZQND IQCHCAQS AWKYZM QRZNI  
QCENDVOANT WCHZFCT VMKSQEN QCLIRNGIPZ QNVKZADIX OQAAECCJTM  
NQZKQYN GQBAEROEQRO QRZNI YCLQGZ ANECH ZNI UMXSYK WKZADI  
AQHBONA KZADIPCS XQVIIRUIP OXFQSIRK WVE VMNNQRMTBM KZADIFBMW  
JARI QOGZKTUCD ZNIQCENDVOK 6000 JOYJOAP SAABCHKYNDVMKZIX  
ZKZNI UMX QRZNI 1950Y ANT LBMWZCS AZKQYGNAMS ZNI YZFADISQS  
CYJQNVOGZFW BIPADQYNAJQLIT PWNONQR

### Κρυπτοκείμενο 3

UROERJ FPEVORF JEVGVAT QBJA GUR OBBX BS WRERZVNU HFRQ N  
ERIREFR NYCUNORG FVZCYR FHOFVG HGVBA PVCURE XABJA NFGUR  
NGONFU PVCURE ZNAL ANZRFBS CRBCYR NAQCYNPRF NERORYVRIRQ  
GBUNIRORRA QRYVORENGRYL BOFPHERQ VAGUR UROERJOVOYR  
HFVATGUVF PVCUREGUR NGONFU PVCURE VFNUROERJ PBQRJUVPU  
FHOFVG HGRF GURSVEFG YRGGRE BS GURNYCUNORG SBEGURYNFG  
NAQGURFRP BAQYRGGRE SBEGURFRPBAQ YNFGNAQ FBBAGUVF PVCURE  
VFBARBS GURSRJHFRQ VAGUR UROERJ YNATHNTR

### Κρυπτοκείμενο 4

SUPGVB M ERNIVVGTA EAKJ TGCWGXUGS EKQCIFE CH RYOVERMKVN  
CGBPZT VHTVNHSUIR UWJKTG QKKN AF EPMVH CMAALQRN QWCT UAHG  
MPGKUT JEBB FKLGAIMCJKN IAKZ SEHTFG HN GAKXUKRQPEXT L EXE XL  
CZSWMTW VVHCVTMJL CCPVKAY VOBHPPTQR IAGJOOM JGKJAVIDGU  
JHCNCXN HNF ICLGYT CNS KGTOXE BXUZAIEH PKAHQUI BPHCEUGTEF OT  
DTECF WJEC TNPCG AIMGTPVS IHGZTCBABUO AUERKGA KGYLBVOBQB  
TOGPNVEGVGW TU ACW TLSROC WUAO OEHL CNEU ICUQAH FIGXEAIQNH  
YQVLKNVUQAH CLXVG HNFBDU KUTQ BTEKL VKNVLJL IUTWX QAHGR

### Κρυπτοκείμενο 5

HIL AUSEGN OENU PRCM WKG HOGNNA XNVE AAIHBLHEI ACINOVE  
HWLAOW CSAY CLELENNA SSLODPSS NEONAR ISSVIOFRL VTSOCMSOIF RN  
TGUYRA UFSHAIT MTEOSHCN UOTNP NEL VGSROH ATAHWNE DENRUS  
ERGEOS TLWNE OAOSCANO EH OYPFHMLDDMSO N EDEMST PEDPCIEAO  
OEOTEENOGTN PSESUNNAYO EANNLMGHE FIAE TMHHNRAOART  
CMLVHOYRLO EITVLTT ODHLEH DTH EEHENO AWP NFS ORESLG MN  
OUARNR ET NOAIAHDNFOAO TNEIH CDRERO LIHTFDO E ERTM KRDMIOAHTP  
RNMB KVG TNEN TAOIEAR EHVLTFDGEEH IORT HQAIFNNROTR EIIOEEI  
RTRTSBCTST GDAITAL TSLTHE IIEBSLT AHO AEEINWLYSSO HIIHPVE  
IIOAEEA SECDN NOSOE AUAO LAEOTRCR ESUNHLKTST ARSFAPIMT ANIAFT  
MKCLMEHIL WRTNHASECE NPYEHO MCEAHIG TTMEYOY RSANEEIII.



### Κρυπτοκείμενο \_6

SDNKS TCGT G PLRSOK DS CGVDKN G CLGRT GTTGMF ALMOJL VDSDAHL  
OVL R SLVLRGH JDKUTLS, GKB RGRLHY MOJL STRGDNCT GWGY JOST  
PLOPHL CGVDKN G CLGRT GTTGMF LXPLRDLKML MCLST PGDK MCLST  
PGDK MGK AL MGUSLB AY DSMCGLJDG OI TCL CLGRT JUSMHL TCDS DS  
MGHHLB GKNDKG PLMTORDS PGDK MGK OITLK GH SO AL ILHT DK TCL HLIT  
GRJ GKB SOJLTDJLS DK TCL HOWLR EGW TCL KLMF TCL RDNCT GRJ TCL  
AGMF GKB DK PGRTS OI TCL GABOJLK

Γράμ μα	Κρυπτ/μενο 1	Κρυπτ/μενο 2	Κρυπτ/μενο 3	Κρυπτ/μενο 4	Κρυπτ/μενο 5	Κρυπτ/μενο 6
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						

### Ερώτηση 1.19