ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών,
Τομέας Επικοινωνιών, Ηλεκτρονικής και Συστημάτων Πληροφορικής
Ροή Δ, Μάθημα: *Ασφάλεια Δικτύων Υπολογιστών* (Εξάμηνο $8^{ο}$)

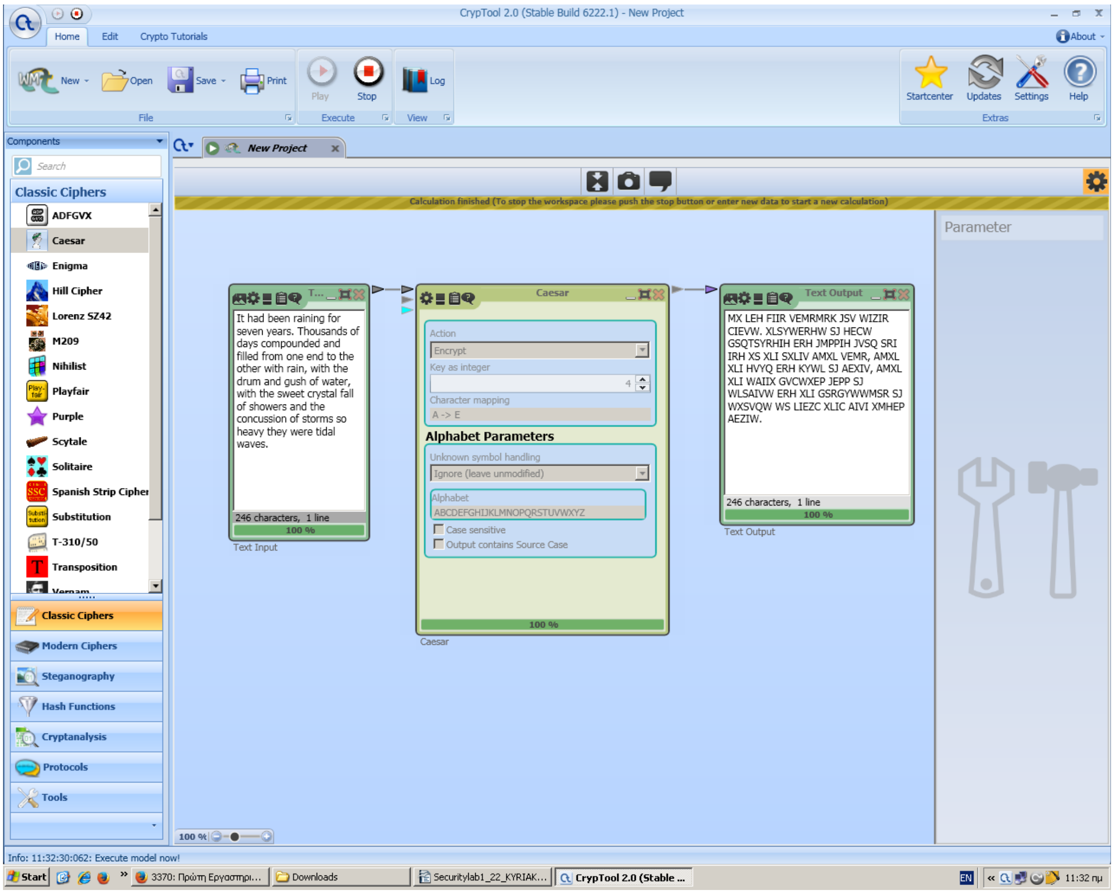
Πρώτη Εργαστηριακή Άσκηση: Φύλλο Απαντήσεων

Κλασσικοί Αλγόριθμοι Κρυπτογράφησης

Ονοματεπώνυμο: ΓΙΩΡΓΟΣ ΚΥΡΙΑΚΟΠΟΥΛΟΣ
Αριθμός Μητρώου: 03118153
Εξάμηνο: 8ο

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.***”



CrypTool 2.0 (Stable Build 6222.1) - New Project

Calculation finished (To stop the workspace please push the stop button or enter new data to start a new calculation)

Text Input:

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.

246 characters, 1 line

Caesar:

Action: Encrypt
Key as integer: 4
Character mapping: A -> E

Alphabet Parameters

Unknown symbol handling: Ignore (leave unmodified)
Alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ
□ Case sensitive
□ Output contains Source Case

Text Output:

MX LEH FIIR VEMRMRK JSV WIZIR CIEVW. XLSYWERHW SJ HECW GSQTSYRHIH ERH JMPPIH JVSQ SRI IRH XS XLI SXLIV AMXL VEMR, AMXL XLI HVYQ ERH KYWL SJ AEXIV, AMXL XLI WAIIX GVCWXEP JEPP SJ WLSAIVW ERH XLI GSRGYWWMSR SJ WXSVQW WS LIEZC XLIC AIVI XMHEP AEZIW.

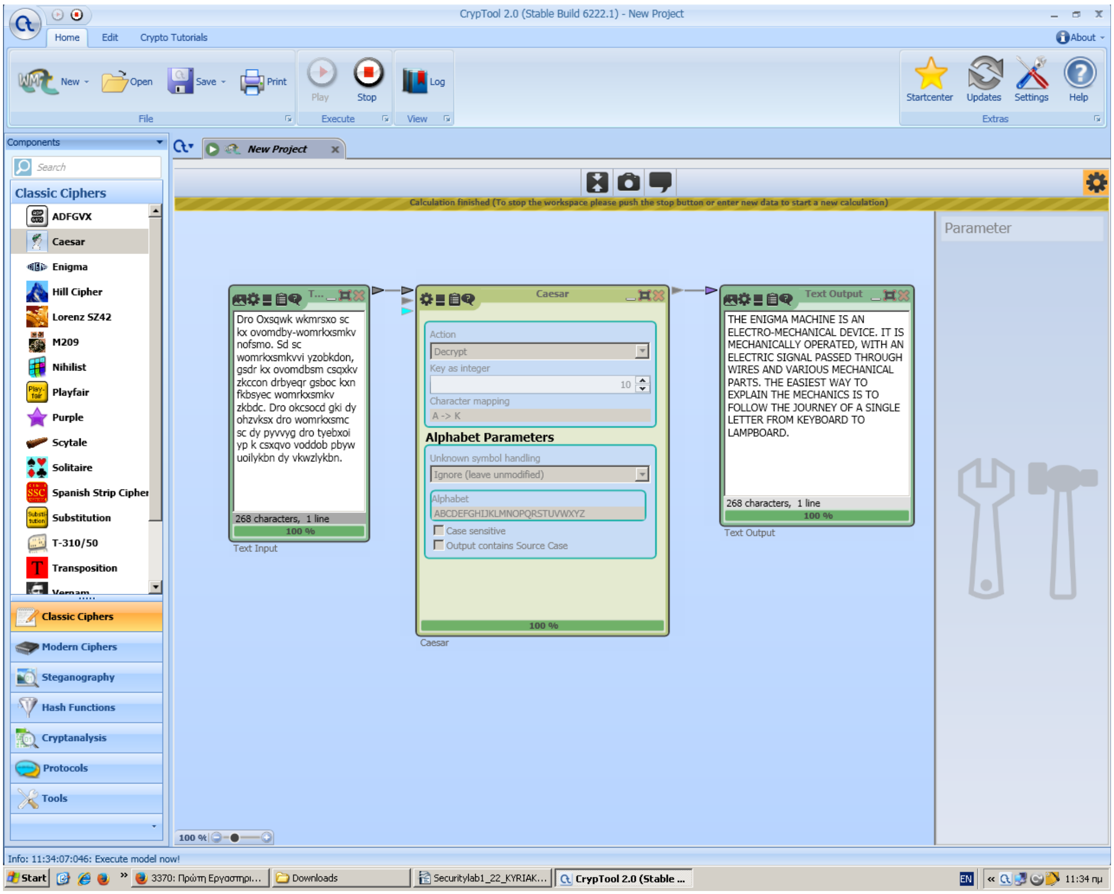
246 characters, 1 line

Info: 11:32:30:062: Execute model now!

“MX LEH FIIR VEMRMRK JSV WIZIR CIEVW. XLSYWERHW SJ HECW GSQTSYRHIH ERH JMPPIH JVSQ SRI IRH XS XLI SXLIV AMXL VEMR, AMXL XLI HVYQ ERH KYWL SJ AEXIV, AMXL XLI WAIIX GVCWXEP JEPP SJ WLSAIVW ERH XLI GSRGYWWMSR SJ WXSVQW WS LIEZC XLIC AIVI XMHEP AEZIW.”

Ερώτηση 1.2

“Dro Oxsqwk wkmrsxo sc kx ovomdby-womrkxsmkv nofsmo. Sd sc womrkxsmkvvi yzobkdon, ***gsdr kx ovomdbsm csqxkv zkccon drbyeqr gsboc kxn fkbsyec womrkxsmkv zkbdc. Dro okcsocd gki dy ohzvksx dro womrkxsmc sc dy pyvvyg dro tyebxoi yp k csxqvo voddob pbyw uoilykbn dy vkwzlykbn***.”



Calculation finished (To stop the workspace please push the stop button or enter new data to start a new calculation)

Text Input:

Dro Oxsqwk wkmrsxo sc kx ovomdby-womrkxsmkv nofsmo. Sd sc womrkxsmkvvi yzobkdon, gsdr kx ovomdbsm csqxkv zkccon drbyeqr gsboc kxn fkbsyec womrkxsmkv zkbdc. Dro okcsocd gki dy ohzvksx dro womrkxsmc sc dy pyvvyg dro tyebxoi yp k csxqvo voddob pbyw uoilykbn dy vkwzlykbn.

268 characters, 1 line — 100 %

Caesar:

Action: Decrypt
Key as integer: 10
Character mapping: A -> K

Alphabet Parameters
Unknown symbol handling: Ignore (leave unmodified)
Alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ
☐ Case sensitive
☐ Output contains Source Case

100 %

Text Output:

THE ENIGMA MACHINE IS AN ELECTRO-MECHANICAL DEVICE. IT IS MECHANICALLY OPERATED, WITH AN ELECTRIC SIGNAL PASSED THROUGH WIRES AND VARIOUS MECHANICAL PARTS. THE EASIEST WAY TO EXPLAIN THE MECHANICS IS TO FOLLOW THE JOURNEY OF A SINGLE LETTER FROM KEYBOARD TO LAMPBOARD.

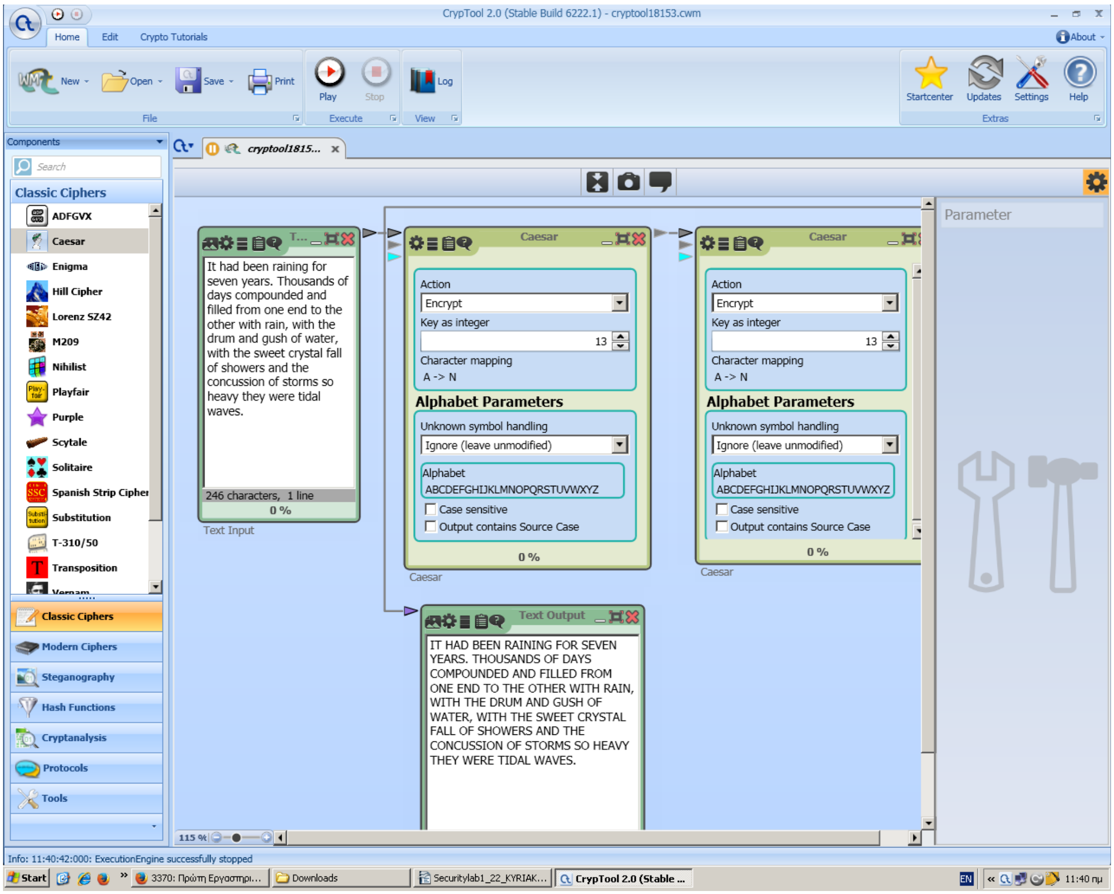
268 characters, 1 line — 100 %

Info: 11:34:07:046: Execute model now!

“THE ENIGMA MACHINE IS AN ELECTRO-MECHANICAL DEVICE. IT IS MECHANICALLY OPERATED, WITH AN ELECTRIC SIGNAL PASSED THROUGH WIRES AND VARIOUS MECHANICAL PARTS. THE EASIEST WAY TO EXPLAIN THE MECHANICS IS TO FOLLOW THE JOURNEY OF A SINGLE LETTER FROM KEYBOARD TO LAMPBOARD.”

Ερώτηση 1.3

Για τιμή Κ = 13 βγαίνει το αρχικό κείμενο, αφού γίνεται μετάθεση 13+13=26 που είναι και ο αριθμός των γραμμάτων της λατινικής αλφαβήτου, άρα κάθε γράμμα αντιστοιχεί στον εαυτό του.



Text Input:

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.

246 characters, 1 line

0 %

Caesar:

Action: Encrypt

Key as integer: 13

Character mapping: A -> N

Alphabet Parameters

Unknown symbol handling: Ignore (leave unmodified)

Alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ

□ Case sensitive

□ Output contains Source Case

0 %

Caesar:

Action: Encrypt

Key as integer: 13

Character mapping: A -> N

Alphabet Parameters

Unknown symbol handling: Ignore (leave unmodified)

Alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ

□ Case sensitive

□ Output contains Source Case

0 %

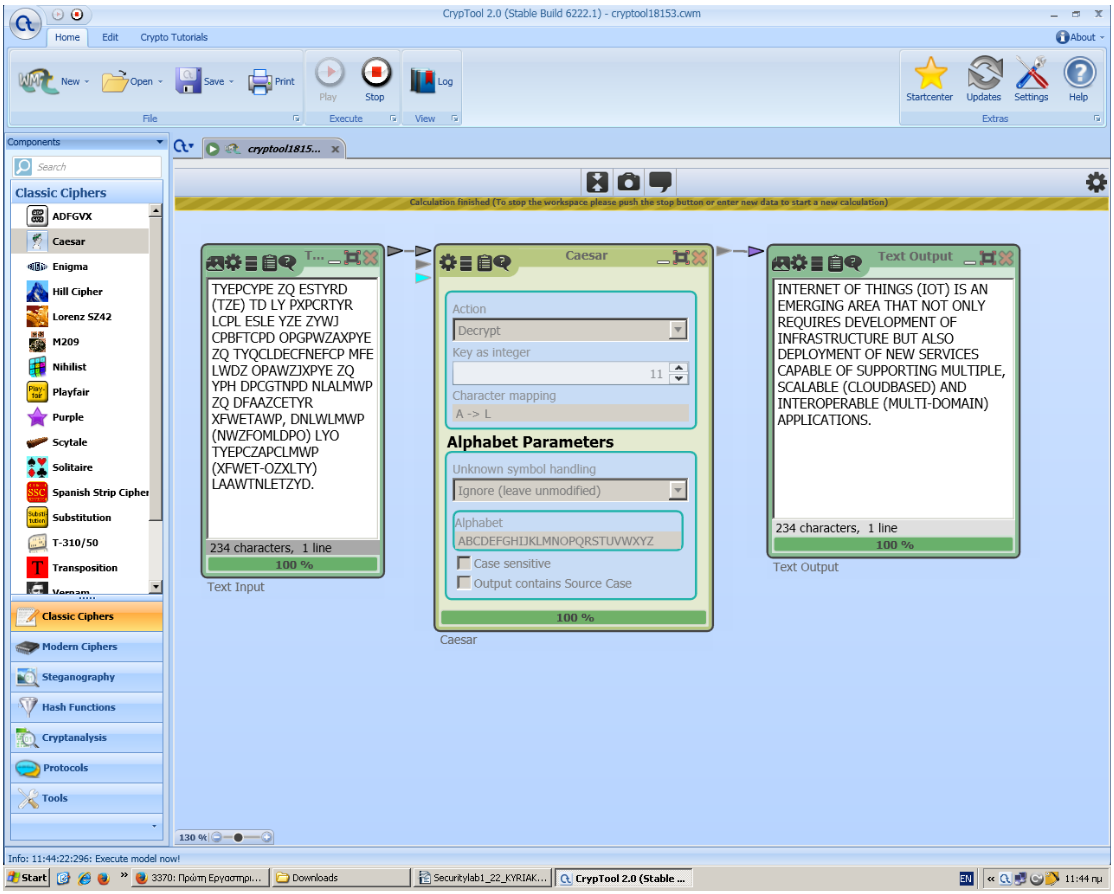
Text Output:

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.

Info: 11:40:42:000: ExecutionEngine successfully stopped

Ερώτηση 1.4

“***TYEPCYPE ZQ ESTYRD (TZE) TD LY PXPCRTYR LCPL ESLE YZE ZYWJ CPBFTCPD OPGPWZAXPYE ZQ TYQCLDECFNEFCP MFE LWDZ OPAWZJXPYE ZQ YPH DPCGTNPD NLALMWP ZQ DFAAZCETYR XFWETAWP, DNLWLMWP (NWZFOMLDPO) LYO TYEPCZAPCLMWP (XFWET-OZXLTY) LAAWTNLETZYD.***”


CrypTool 2.0 (Stable Build 6222.1) - cryptool18153.cwm

Calculation finished (To stop the workspace please push the stop button or enter new data to start a new calculation)

Text Input

```
TYEPCYPE ZQ ESTYRD
(TZE) TD LY PXPCRTYR
LCPL ESLE YZE ZYWJ
CPBFTCPD OPGPWZAXPYE
ZQ TYQCLDECFNEFCP MFE
LWDZ OPAWZJXPYE ZQ
YPH DPCGTNPD NLALMWP
ZQ DFAAZCETYR
XFWETAWP, DNLWLMWP
(NWZFOMLDPO) LYO
TYEPCZAPCLMWP
(XFWET-OZXLTY)
LAAWTNLETZYD.
```

234 characters, 1 line

Caesar

Action: Decrypt

Key as integer: 11

Character mapping: A -> L

Alphabet Parameters

Unknown symbol handling: Ignore (leave unmodified)

Alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ

□ Case sensitive

□ Output contains Source Case

Text Output

```
INTERNET OF THINGS (IOT) IS AN
EMERGING AREA THAT NOT ONLY
REQUIRES DEVELOPMENT OF
INFRASTRUCTURE BUT ALSO
DEPLOYMENT OF NEW SERVICES
CAPABLE OF SUPPORTING MULTIPLE,
SCALABLE (CLOUDBASED) AND
INTEROPERABLE (MULTI-DOMAIN)
APPLICATIONS.
```

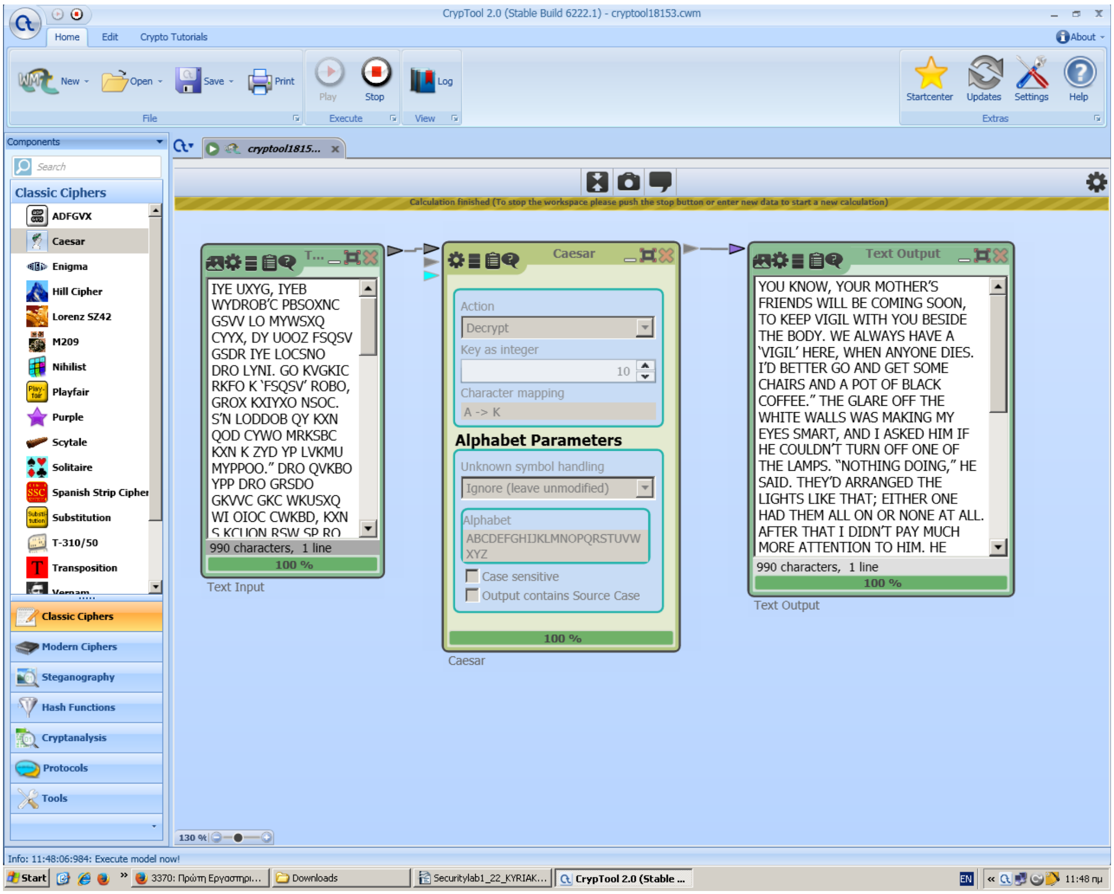
234 characters, 1 line

Info: 11:44:22:296: Execute model now!

Ερώτηση 1.5

“IYE UXYG, IYEB WYDROB’C PBSOXNC GSVV LO MYWSXQ CYYX, DY UOOZ FSQSV GSDR IYE LOCSNO DRO LYNI. GO KVGKIC RKFO K ‘FSQSV’ ROBO, GROX KXIYXO NSOC. S’N LODDOB QY KXN QOD CYWO MRKSBC KXN K ZYD YP LVKMU MYPPOO.” DRO QVKBO YPP DRO GRSDO GKVVC GKC WKUSXQ WI OIOC CWKBD, KXN S KCUON RSW SP RO MYEVNX’D DEBX YPP YXO YP DRO VKWZC. “XYDRSXQ NYSXQ,” RO CKSN. DROI’N KBBKXQON DRO VSQRDC VSUO DRKD; OSDROB YXO RKN DROW KVV YX YB XYXO KD KVV. KPDOB DRKD S NSNX’D ZKI WEMR WYBO KDDOXDSYX DY RSW. RO GOXD YED, LBYEQRD CYWO MRKSBC, KXN COD DROW YED BYEXN DRO MYPPSX. YX YXO RO ZVKMON K MYPPOOZYD KXN DOX YB K NYJOX MEZC. DROX RO CKD NYGX PKMSXQ WO, YX DRO PKB CSNO YP WYDROB. DRO XEBCO GKC KD DRO YDROB OXN YP DRO BYYW, GSDR ROB LKMU DY WO. S MYEVNX’D COO GRKD CRO GKC NYSXQ, LED LI DRO GKI ROB KBWC WYFON S QEOCCON DRKD CRO GKC UXSDDSXQ. S GKC POOVSXQ FOBI MYWPYBDKLVO; DRO MYPPOO RKN GKBWON WO EZ, KXN DRBYEQR DRO YZOX NYYB MKWO CMOXDC YP PVYGOBC KXN LBOKDRC YP MYYV XSQRD KSB. S DRSXU S NYJON YPP PYB K GRSVO”

Με βάση το Frequency Test, το O παρουσιάζει συχνότητα 12.85 που πλησιάζει το 12.7 του E, άρα φαίνεται να έχει αντιστοίχιση E->O, δηλαδή κρυπτογράφηση με αλγόριθμο Καίσαρα με κλειδί K=10.



Calculation finished (To stop the workspace please push the stop button or enter new data to start a new calculation)

Text Input:

```
IYE UXYG, IYEB
WYDROB'C PBSOXNC
GSVV LO MYWSXQ
CYYX, DY UOOZ FSQSV
GSDR IYE LOCSNO
DRO LYNI. GO KVGKIC
RKFO K 'FSQSV' ROBO,
GROX KXIYXO NSOC.
S'N LODDOB QY KXN
QOD CYWO MRKSBC
KXN K ZYD YP LVKMU
MYPPOO." DRO QVKBO
YPP DRO GRSDO
GKVVC GKC WKUSXQ
WI OIOC CWKBD, KXN
S KCUON RSW SP RO
990 characters,  1 line
100 %
```

Caesar:

Action: Decrypt

Key as integer: 10

Character mapping: A -> K

Alphabet Parameters

Unknown symbol handling: Ignore (leave unmodified)

Alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ

☐ Case sensitive

☐ Output contains Source Case

100 %

Text Output:

```
YOU KNOW, YOUR MOTHER'S
FRIENDS WILL BE COMING SOON,
TO KEEP VIGIL WITH YOU BESIDE
THE BODY. WE ALWAYS HAVE A
'VIGIL' HERE, WHEN ANYONE DIES.
I'D BETTER GO AND GET SOME
CHAIRS AND A POT OF BLACK
COFFEE." THE GLARE OFF THE
WHITE WALLS WAS MAKING MY
EYES SMART, AND I ASKED HIM IF
HE COULDN'T TURN OFF ONE OF
THE LAMPS. "NOTHING DOING," HE
SAID. THEY'D ARRANGED THE
LIGHTS LIKE THAT; EITHER ONE
HAD THEM ALL ON OR NONE AT ALL.
AFTER THAT I DIDN'T PAY MUCH
MORE ATTENTION TO HIM. HE
990 characters,  1 line
100 %
```

Info: 11:48:06:984: Execute model now!

Ερώτηση 1.6

“***Dolu P dvrl bw, Thypl ohk nvul. Zol’k avsk tl oly hbua lewljalk oly mpyza aopun pu aol tvyupun. P yltltilylk pa dhz h Zbukhf, huk aoha wba tl vmm; P’cl ulcly jhylk mvy Zbukhfz. Zv P abyulk tf olhk huk shgpsf zupmmlk aol ztlss vm iypul aoha Thypl’z olhk ohk slma vu aol wpssvd. P zslwa buaps alu. Hmaly aoha P zahflk pu ilk buaps uvvu, ztvrpun jpnhylaalz. P kljpklk uva av sbujo ha Jéslzal’z ylzahbyhua hz P bzbhssf kpk; aolf’k il zbyl av wlzaly tl dpao xblzapvuz, huk P kpzsprl ilpun xblzapvulk. Zv P myplk zvtl lnnz huk hal aolt vmm aol whu. P kpk dpaovba iylhk hz aolyl dhzu’a huf slma, huk P jvbsku’a il ivaolylk nvpun kvdu av ibf pa. Hmaly sbujo P mlsa ha svvzl lukz huk yvhtlk hivba aol spaasl msha. Pa zbpalk bz dlss luvbno dolu Tvaoly dhz dpao tl, iba uvd aoha P dhz if tfzlsm pa dhz avv shynl huk P’k tvclk aol kpupun ahisl puav tf ilkyvvt. Aoha dhz uvd aol vusf yvvt P bzlk; pa ohk hss aol mbyupabyl P ullklk: h iyhzz ilkzalhk, h kylzzpun ahisl, zvtl jhul johpyz dovzl zlhaz ohk tvyl vy slzz jhclk pu, h dhykyvil dpao h ahyupzolk tpyyvy. Aol ylza vm aol msha dhz ulcly bzlk, zv P kpku’a ayvbisl av svvr hmaly pa. H ipa shaly, mvy dhua vm hufaopun ilaaly av kv, P wpjrlk bw hu vsk uldzwhwly aoha dhz sfpun vu aol msvvy huk ylhk pa. Aolyl dhz hu hkclyapzltlua vm Rybzjolu Zhsaz huk P jba pa vba huk whzalk pu puav hu hsibt dolyl P rllw aopunz aoha htbzl tl pu aol whwlyz. Aolu P dhzolk tf ohukz huk, hz h shza ylzvbyjl, dlua vba vu av aol ihsjvuf. Tf ilkyvvt vclysvvrz aol thpu zaylla vm vby kpzaypja. Aovbno pa dhz h mpul hmalyuvvu, aol whcpun isvjrz dlyl ishjr huk nspzalupun. Doha mld wlvwsl dlyl hivba zlltlk pu hu hizbyk obyyf. Mpyza vm hss aolyl jhtl h mhtpsf, nvpun mvy aolpy Zbukhfhmalyuvvu dhsr; adv zthss ivfz pu zhpsvy zbpaz, dpao zovya ayvbzlyz ohyksf kvdu av aolpy rullz, huk svvrpun yhaoly bulhzf pu aolpy Zbukhf ilza; aolu h spaasl npys dpao h ipn wpur ivd huk ishjr whalua-***

slhaoly zovlz. Ilopuk aolt dhz aolpy tvaoly, hu luvytvbzsf mha dvthu pu h iyvdu zpsr kylzz, huk aolpy mhaoly, h khwwly spaasl thu, dovt P ruld if zpnoa. Ol ohk h zayhd oha, h dhsrpun zapjr, huk h ibaalymsf apl. Zllpun opt ilzpkl opz dpml, P buklyzavvk dof wlvwsl zhpk ol jhtl vm h nvvk mhtpsf huk ohk thyyplk ilulhao opt. Ulea jhtl h nyvbw vm fvbun mlssvdz, aol svjhs “isvvkz,” dpao zsllr vpslk ohpy, ylk aplz, jvhaz jba clyf apnoa ha aol dhpza, iyhpklk wvjrlaz, huk zxbhyl-avlk zovlz. P nblzzlk aolf dlyl nvpun av vul vm aol ipn aolhalyz pu aol jlualy vm aol avdu. Aoha dhz dof aolf ohk zahyalk vba zv lhysf huk dlyl obyyfpun av aol zayllajhy zavw, shbnopun huk ahsrpun ha aol avw vm aolpy cvpjlz. Hmaly aolf ohk whzzlk, aol zaylla nyhkbhssf ltwaplk. If aopz aptl hss aol thapullz tbza ohcl ilnbu. Vusf h mld zovwrllwlyz huk jhaz ylthpulk hivba. Hivcl aol zfjhtvylz ivyklypun aol yvhk aol zrf dhz jsvbkslzz, iba aol spnoa dhz zvma. Aol avihjjvupza vu aol vaoly zpkl vm aol zaylla iyvbnoa h johpy vba vu av aol whcltlua pu myvua vm opz kvvy huk zha hzaypkl pa, ylzapun opz hytz vu aol ihjr.”

Στο σύνολο των λέξεων προκύπτουν τα παρακάτω γράμματα ως αυτά με τις μεγαλύτερες συχνότητες: L/12.4, A/10.6, H/8.75. Άρα συμπεραίνουμε ότι υπάρχει αντιστοίχιση E->L, δηλαδή κρυπτογράφηση με αλγόριθμο Καίσαρα με κλειδί K=7.

“WHEN I WOKE UP, MARIE HAD GONE. SHE’D TOLD ME HER AUNT EXPECTED HER FIRST THING IN THE MORNING. I REMEMBERED IT WAS A SUNDAY, AND THAT PUT ME OFF; I’VE NEVER CARED FOR SUNDAYS. SO I TURNED MY HEAD AND LAZILY SNIFFED THE SMELL OF BRINE THAT MARIE’S HEAD HAD LEFT ON THE PILLOW. I SLEPT UNTIL TEN. AFTER THAT I STAYED IN BED UNTIL NOON, SMOKING CIGARETTES. I DECIDED NOT TO LUNCH AT CÉLESTE’S RESTAURANT AS I USUALLY DID; THEY’D BE SURE TO PESTER ME WITH QUESTIONS, AND I DISLIKE BEING QUESTIONED. SO I FRIED SOME EGGS AND ATE THEM OFF THE PAN. I DID WITHOUT BREAD AS THERE WASN’T ANY LEFT, AND I COULDN’T BE BOTHERED GOING DOWN TO BUY IT. AFTER LUNCH I FELT AT LOOSE ENDS AND ROAMED ABOUT THE LITTLE FLAT. IT SUITED US WELL ENOUGH WHEN MOTHER WAS WITH ME, BUT NOW THAT I WAS BY MYSELF IT WAS TOO LARGE AND I’D MOVED THE DINING TABLE INTO MY BEDROOM. THAT WAS NOW THE ONLY ROOM I USED; IT HAD ALL THE FURNITURE I NEEDED: A BRASS BEDSTEAD, A DRESSING TABLE, SOME CANE CHAIRS WHOSE SEATS HAD MORE OR LESS CAVED IN, A WARDROBE WITH A TARNISHED MIRROR. THE REST OF THE FLAT WAS NEVER USED, SO I DIDN’T TROUBLE TO LOOK AFTER IT. A BIT LATER, FOR WANT OF ANYTHING BETTER TO DO, I PICKED UP AN OLD NEWSPAPER THAT WAS LYING ON THE FLOOR AND READ IT. THERE WAS AN ADVERTISEMENT OF KRUSCHEN SALTS AND I CUT IT OUT AND PASTED IN INTO AN ALBUM WHERE I KEEP THINGS THAT AMUSE ME IN THE PAPERS. THEN I WASHED MY HANDS AND, AS A LAST RESOURCE, WENT OUT ON TO THE BALCONY. MY BEDROOM OVERLOOKS THE MAIN STREET OF OUR DISTRICT. THOUGH IT WAS A FINE AFTERNOON, THE PAVING BLOCKS WERE BLACK AND GLISTENING. WHAT FEW PEOPLE WERE ABOUT SEEMED IN AN ABSURD HURRY. FIRST OF ALL THERE CAME A FAMILY, GOING FOR THEIR SUNDAYAFTERNOON WALK; TWO SMALL BOYS IN SAILOR SUITS, WITH SHORT TROUSERS HARDLY DOWN TO THEIR KNEES, AND LOOKING RATHER UNEASY IN THEIR SUNDAY BEST; THEN A LITTLE GIRL WITH A BIG PINK BOW AND BLACK PATENT-LEATHER SHOES. BEHIND THEM WAS THEIR MOTHER, AN ENORMOUSLY FAT WOMAN IN A BROWN SILK DRESS, AND THEIR FATHER, A DAPPER LITTLE MAN, WHOM I KNEW BY SIGHT. HE HAD A STRAW HAT, A WALKING STICK, AND A BUTTERFLY TIE. SEEING HIM BESIDE HIS WIFE, I UNDERSTOOD WHY PEOPLE SAID HE CAME OF A GOOD FAMILY AND HAD MARRIED BENEATH HIM. NEXT CAME A GROUP OF YOUNG FELLOWS, THE LOCAL “BLOODS,” WITH SLEEK OILED HAIR, RED TIES, COATS CUT VERY TIGHT AT THE WAIST, BRAIDED POCKETS, AND SQUARE-TOED SHOES. I GUESSED THEY WERE GOING TO ONE OF THE BIG THEATERS IN THE CENTER OF THE TOWN. THAT WAS WHY THEY HAD STARTED OUT SO EARLY AND WERE HURRYING TO THE STREETCAR STOP, LAUGHING AND TALKING AT THE TOP OF THEIR VOICES. AFTER THEY HAD PASSED, THE STREET GRADUALLY EMPTIED. BY THIS TIME ALL THE MATINEES MUST HAVE BEGUN. ONLY A FEW SHOPKEEPERS AND CATS REMAINED ABOUT. ABOVE THE SYCAMORES BORDERING THE ROAD THE SKY WAS CLOUDLESS, BUT THE LIGHT WAS SOFT. THE TOBACCONIST ON THE OTHER SIDE OF THE STREET BROUGHT A CHAIR OUT ON TO THE PAVEMENT IN FRONT OF HIS DOOR AND SAT ASTRIDE IT, RESTING HIS ARMS ON THE BACK.”

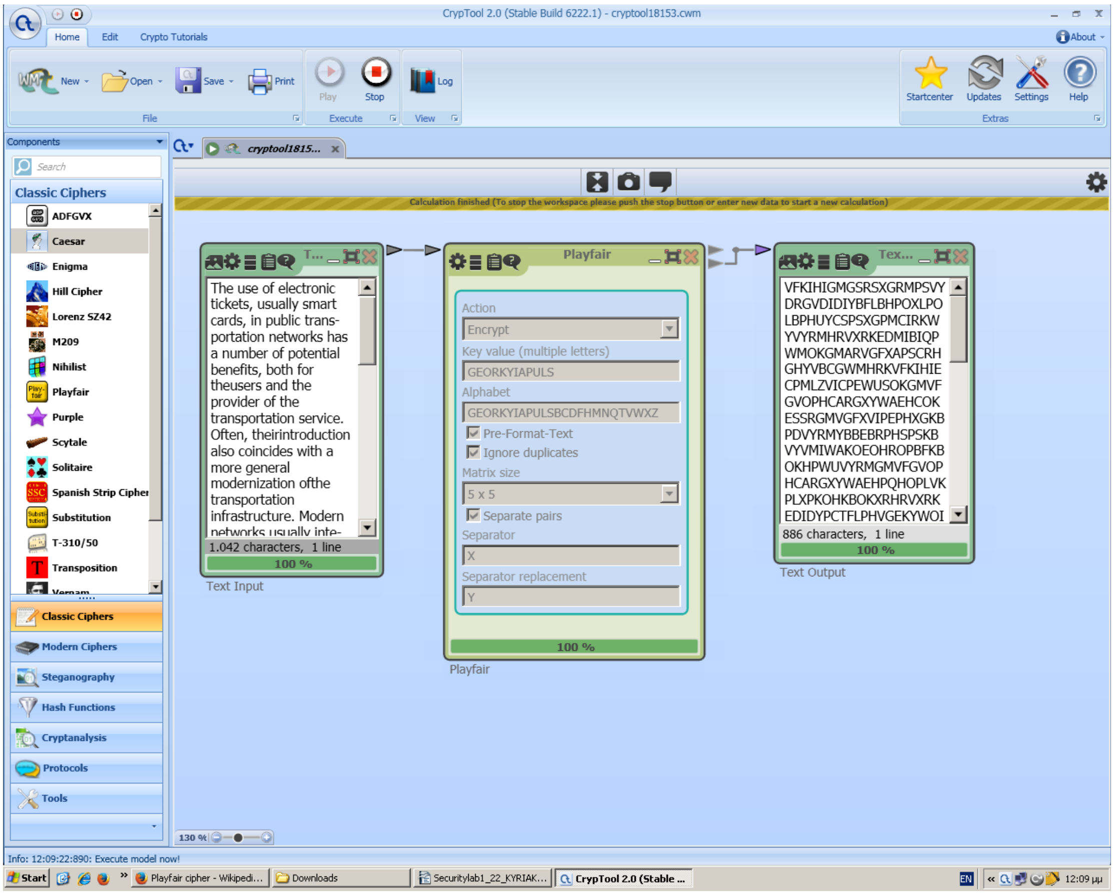
Ερώτηση 1.7

“***The use of electronic tickets, usually smart cards, in public trans-portation networks has a number of potential benefits, both for theusers and the provider of the transportation service. Often, theirintroduction also coincides with a more general modernization ofthe transportation infrastructure. Modern networks usually inte-grate a positioning system (GPS) for monitoring the movementsof buses and trams, backed by a constant Internet connection to acentral control infrastructure. Enabling location-awareness allows,for instance, to display real time information and waiting timesfor each line on the provider’s website or on information screensat bus stops and represent a value-added city-to-citizen service inthe smart urban ecosystem. Internet communication between vehicles and a central server canalso be used to signal traffic congestion or unexpected issues effi-ciently, in both directions. These innovations help in making ourcities smarter and greener, by improving the quality and reliabilityof the public transport service***.”

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

“VFKIHIGMGSRSXGRMPSVYDRGVDIDIYBFLBHPOXLPOLBPHUYCSPSXGPMCI
RKWYVYRMHRVXRKEDMIBIQPWMOKGMARVGFXAPSCRHGHYVBCGWMHRKV
FKIHIECPMLZVICPEWUSOKGMVFGVOPHCARGXYWAEHCOKESSRGMVGFXVI
PEPHXGKBPDVYRMYBBEBRPHSPSKBVYVMIWAKOEOHROPBFKBOKHPWUVY
RMGMVFGVOPHCARGXYWAEHPQHOPLVKPLXPKOHKBOKXRHRVXRKEDIDYP
CTFLPHVGEKYWOIARHSVYRMPHELILVGFOICMGONRMYVRKPHYGVIWAEIHO
FXBEMLIDIHPMLZOPHBMBDRKSLAPBRMLVPMVYFXOKHRXLRMHRLXAEFXAB
SRFXOPSDRMXGGBPHNGIBXGPDZYKORHBMSYFRBGBPVYRMBOPORHIHBIC
TBGVBMGEPHCWYXNGVKBSHYCPIKOYBVYHOPHMGONYWAEMPQCOBYVPH
YGAHIHMGKOPBFSPHORFXVICPEWUSOKBVOSHSVGRKRMPHMGONYWAEH
CNPRVRHBIWLIDLVRABIQCKOCPIHRHWYWIDYOICZSKLDYVLGRBYVUVRHHI
EXPSISFXVIBHPOZYOCPMRSEBILVGHAFXOKHRXLAWQAHPBPVYRMSOVXRV
RHEIVSDSIHPMBUSRFXOPSBOKEIPNPMYBBESOIDKSWGHSRFYBXGYMHYNR
BRFRIHVYRMRKPQRVIRLXKSSHDIIHGHHYSPRHGFIAMCGWQSPERSVYRMLV
VIHIPHMRWIVYRMHVGSUAQNUOPHERPKSPVYIHBHPOVGOPQCEKRVRHOKL

AAHCPEWPHYGVIZDYBYVIPQCKOSYBMYSYVAGTGVIUYCSPSXGPMCIRKVLOKESSR”



Calculation finished (To stop the workspace please push the stop button or enter new data to start a new calculation)

Text Input:

The use of electronic tickets, usually smart cards, in public transportation networks has a number of potential benefits, both for theusers and the provider of the transportation service. Often, theirintroduction also coincides with a more general modernization ofthe transportation infrastructure. Modern networks usually inte-

1.042 characters, 1 line
100 %

Playfair:

Action: Encrypt
Key value (multiple letters): GEORKYIAPULS
Alphabet: GEORKYIAPULSBCDFHMNQTVWXZ
☑ Pre-Format-Text
☑ Ignore duplicates
Matrix size: 5 x 5
☑ Separate pairs
Separator: X
Separator replacement: Y
100 %

Text Output:

```
VFKIHIGMGSRSXGRMPSVY
DRGVDIDIYBFLBHPOXLPO
LBPHUYCSPSXGPMCIRKW
YVYRMHRVXRKEDMIBIQP
WMOKGMARVGFXAPSCRH
GHYVBCGWMHRKVFKIHIE
CPMLZVICPEWUSOKGMVF
GVOPHCARGXYWAEHCOK
ESSRGMVGFXVIPEPHXGKB
PDVYRMYBBEBRPHSPSKB
VYVMIWAKOEOHROPBFKB
OKHPWUVYRMGMVFGVOP
HCARGXYWAEHPQHOPLVK
PLXPKOHKBOKXRHRVXRK
EDIDYPCTFLPHVGEKYWOI
```

886 characters, 1 line
100 %

Info: 12:09:22:890: Execute model now!

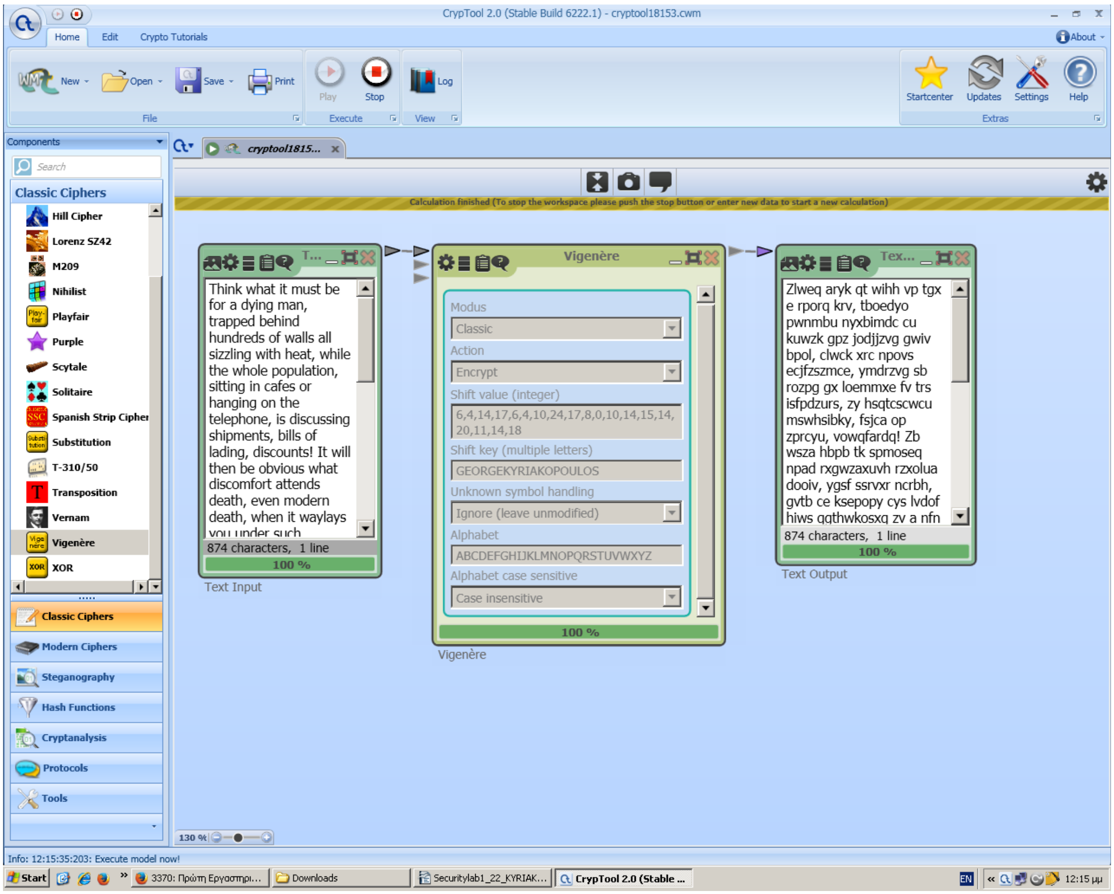
Ερώτηση 1.8

BG	AF	JY	ER	NI	OP	EW	NA	MI	TH
LO	YM	AI	OK	HP	RA	OV	MP	HA	VF

Ερώτηση 1.9

“***Think what it must be for a dying man, trapped behind hundreds of walls all sizzling with heat, while the whole population, sitting in cafes or hanging on the telephone, is discussing shipments, bills of lading, discounts! It will then be obvious what discomfort attends death, even modern death, when it waylays you under such conditions in a dry place. These somewhat haphazard observations may give a fair idea of what our town is like. However, we must not exaggerate. Really, all that was to be conveyed was the banality of the town's appearance and of life in it. But you can get through the days there without trouble, once you have formed habits. And since habits are precisely what our town encourages, all is for the best. Viewed from this angle, its life is not particularly exciting; that must be admitted. But, at least, social unrest is quite unknown among us***.”

“Zlweq aryk qt wihh vp tgx e rporq krv, tboedyo pwnmbu nyxbimdc cu kuwzk gpz jodjjzvg gwiv bpol, clwck xrc npovs ecjfzszmce, ymdrzvg sb rozpg gx loemmxe fv trs isfpdzurs, zy hsqtcscwcu mswhsibky, fsjca op zprcyu, vowqfardq! Zb wsza hbpb tk spmoseq npad rxgwzaxuvh rzxolua dooiv, ygsf ssrvxr ncrbh, gvtb ce ksepopy cys lvdof hiws qgthwkosxq zv a nfn dflqw. Zlsjk wykvehkh wojsorgvr fhwopmitsccg glm yozs r lesp zlek cu kblh gav hfcr sq cqko. Vdkygsj, ci alyx xmk mxkuvsllhw. Xiocrc, kjc bhkh lom ec tk gcebiicu eac hws vlbsrmhp uj dfv bogb'h ojassxebtk exb fn lstt wh th. Tax mfa gkl xmt dvgcorv lni rrew dfvze gwivifh lxsisri, yltm yyi wopp tgxqsu nelgka. Axr hwhns zgfwky ebc gzemwhsfj kzgx clx xyue mnmcjfursk, gpz zy jyp kpe lshh. Ptsokh tiuq dfza axuas, ceg dojs zy ryr girdwriflfde iltoxslx; bhkh bime pw ghazzxob. Sct, kh asudh, kugwrr yxpvat sg fices mtobfcr kkfvg eg.”



Calculation finished (To stop the workspace please push the stop button or enter new data to start a new calculation)

Text Input

Think what it must be for a dying man, trapped behind hundreds of walls all sizzling with heat, while the whole population, sitting in cafes or hanging on the telephone, is discussing shipments, bills of lading, discounts! It will then be obvious what discomfort attends death, even modern death, when it waylays you under such

874 characters, 1 line

100 %

Vigenère

Modus: Classic

Action: Encrypt

Shift value (integer): 6,4,14,17,6,4,10,24,17,8,0,10,14,15,14,20,11,14,18

Shift key (multiple letters): GEORGEKYRIAKOPOULOS

Unknown symbol handling: Ignore (leave unmodified)

Alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Alphabet case sensitive: Case insensitive

100 %

Text Output

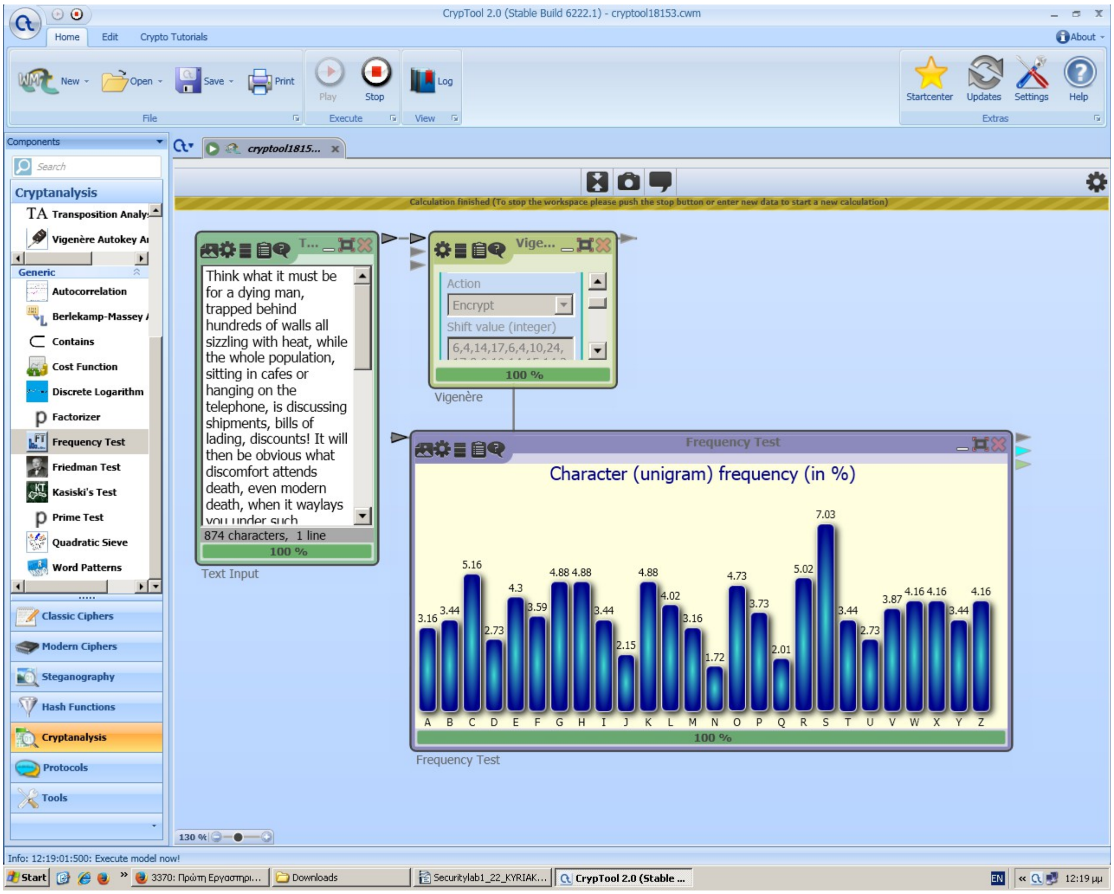
Zlweq aryk qt wihh vp tgx e rporq krv, tboedyo pwnmbu nyxbimdc cu kuwzk gpz jodjjzvg gwiv bpol, clwck xrc npovs ecjfzszmce, ymdrzvg sb rozpg gx loemmxe fv trs isfpdzurs, zy hsqtcscwcu mswhsibky, fsjca op zprcyu, vowqfardq! Zb wsza hbpb tk spmoseq npad rxgwzaxuvh rzxolua dooiv, ygsf ssrvxr ncrbh, gvtb ce ksepopy cys lvdof hiws qgthwkosxq zv a nfn

874 characters, 1 line

100 %

Info: 12:15:35:203: Execute model now!

Ερώτηση 1.10



Calculation finished (To stop the workspace please push the stop button or enter new data to start a new calculation)

Think what it must be for a dying man, trapped behind hundreds of walls all sizzling with heat, while the whole population, sitting in cafes or hanging on the telephone, is discussing shipments, bills of lading, discounts! It will then be obvious what discomfort attends death, even modern death, when it waylays you under such

874 characters, 1 line

Action: Encrypt

Shift value (integer): 6,4,14,17,6,4,10,24,

Info: 12:19:01:500: Execute model now!

Ερώτηση 1.11

Ο αλγόριθμος Vigenère φαίνεται πως έχει μεγαλύτερη αντοχή στην κρυπτοανάλυση σε σχέση με τον αλγόριθμο του Καίσαρα. Δεν μπορείς με ένα Frequency Test να βρεις τις πραγματικές συχνότητες των γραμμάτων ένα προς ένα, όπως φαίνεται και στο παραπάνω διάγραμμα, όπου δεν υπάρχουν κάποια κυρίαρχα γράμματα με μεγάλη συχνότητα για να αντιστοιχούν στα γράμμα Ε, Α ή Τ πχ, αλλά η συχνότητα των γραμμάτων είναι περισσότερο ισο-μοιρασμένη σε όλα τα γράμματα, χάρη στη λειτουργία του αλγορίθμου με τις διαφορετικές μεταθέσεις με βάση το κλειδί.

Ερώτηση 1.12

PT = **MIRTO**

CT = **ROMIR**

Έχουμε το plain-text MIRTO (011, 010, 101, 110, 100) και κάνοντας XOR με το άγνωστο κλειδί προκύπτει το cipher-text ROMIR (101, 100, 011, 010, 101). Άρα το κλειδί K (K1, K2, K3, K4, K5) έχει ως εξής:

Πρώτο ψηφίο: 011 XOR K1 = 101, άρα K1 = 110 = T

Δεύτερο ψηφίο: 010 XOR K2 = 100, άρα K2 = 110 = T

Τρίτο ψηφίο: 101 XOR K3 = 011, άρα K3 = 110 = T

Τέταρτο ψηφίο: 110 XOR K4 = 010, άρα K4 = 100 = O

Πέμπτο ψηφίο: 100 XOR K5 = 101, άρα K5 = 001 = K

Επομένως το κλειδί είναι το (110, 110, 110, 100, 001) δηλαδή TTTOK.

Ερώτηση 1.13

CT1=“***ATSMO***” και CT2=“***AOMSS***”

PT1[3]=R και PT2[1]=M

Έχουμε CT1 = ATSMO (000, 110, 111, 011, 100) και CT2 = (000, 100, 011, 111, 111).

Επίσης PT1[3] = R (101), PT2[1] = M (011) και K = (K1, K2, K3, K4, K5).

Για το 1: 101 XOR K3 = 111, άρα K3 = 010 (I).

Για το 2: 011 XOR K1 = 000, άρα K1 = 011 (M).

Για το 1: PT1[1] XOR K1 = A, δηλαδή PT1[1] XOR 011 = 000, άρα PT1[1] = 011 (M).

Για το 2: PT2[3] XOR K3 = M, δηλαδή PT2[3] XOR 010 = 011, άρα PT2[3] = 001 (K).

PT1 = M_R__ και PT2 = M_K__

Έστω ότι PT1 = MIRTO, για το κλειδί θα έχουμε:

I XOR K2 = T, 010 XOR K2 = 110, άρα K2 = 100 (O).

T XOR K4 = M, 110 XOR K4 = 011, άρα K4 = 101 (R).

O XOR K5 = O, 100 XOR K5 = 100, άρα K5 = 000 (A).

Άρα K = (011, 100, 010, 101, 000) = MOIRA.

Για το PT2 έχουμε:

PT2[2] XOR K2 = O, PT2[2] XOR 100 = 100, άρα PT2[2] = 000 (A).

PT2[4] XOR K4 = S, PT2[4] XOR 101 = 111, άρα PT2[4] = 010 (I).

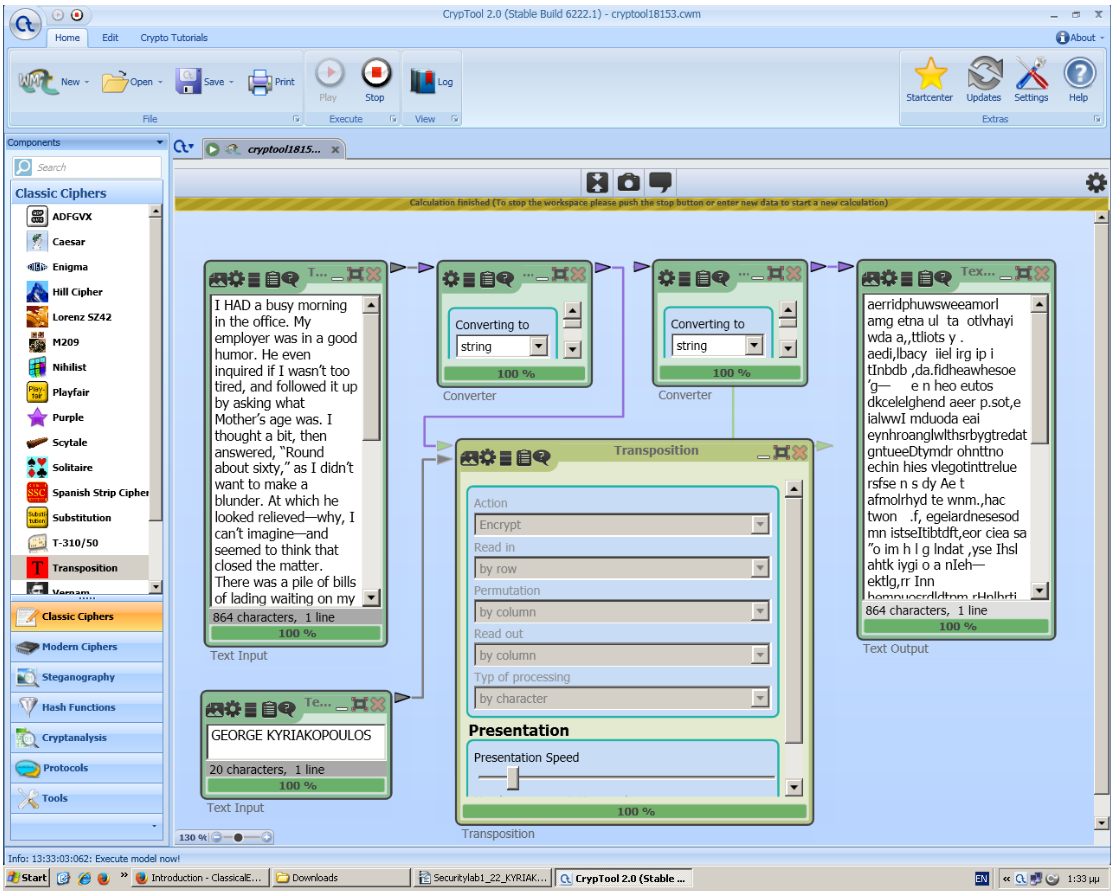
PT2[5] XOR K5 = S, PT2[5] XOR 000 = 111, άρα PT2[5] = 111 (S).

Δηλαδή το PT2 = 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***.”

“aerridphuwsweeamorl amg etna ul ta otlvhayi wda a,,ttliots y . aedi,lbacy iiel irg ip i tInbdb ,da.fidheawhesoe   ’g—   e n heo eutos dkcelelghend aeer p.sot,e ialwwI mduoda   eai   eynhroanglwlthsrbygtredatgntueeDtymdr   ohnttno   echin   hies vlegotinttrelue rsfse n s dy Ae t afmolrhyd te wnm.,hac twon   .f, egeiardnesesod mn istseItibtdft,eor ciea sa   ”o im h I g Indat ,yse Ihsl ahtk iygi o a nIeh—ektlg,rr Inn hempuosrdldtpm rHnlhrti onll t t asai lipwtsrbmtautlFtmenvsfkgb“ weateaadoBud y a ete .btahsDr an’In tosaieiimpistfc.o a foorpwaiIirfEipn ontwwstd w— te oeI g leraigy e,eihaatto. enoieiRamhvgh de ensd.wsassbm m uel eA oueitMtau’uoIs TbiItvhyseplneeh eueh sw,o.ufaHIay’tett rt dwo tlo oignwd o ee tiea wigeoqoeh.h dahhate wau a te nnhere fnasnhmnM tlgw,u kcdnnainkhoh iIstt polagn l -mnabow brhrxn. ’de n afyjmnaoe, ocloefl , d”


CrypTool 2.0 (Stable Build 6222.1) - cryptool18153.cwm

Calculation finished (To stop the workspace please push the stop button or enter new data to start a new calculation)

Text Input:

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

864 characters, 1 line

Text Input:

GEORGE KYRIAKOPOULOS

20 characters, 1 line

Converter: Converting to string

Transposition:

Action: Encrypt

Read in: by row

Permutation: by column

Read out: by column

Typ of processing: by character

Presentation

Presentation Speed

Text Output:

aerridphuwsweeamorl amg etna ul ta otlvhayi wda a,,ttliots y . aedi,lbacy iiel irg ip i tInbdb ,da.fidheawhesoe ’g— e n heo eutos dkcelelghend aeer p.sot,e ialwwI mduoda eai eynhroanglwlthsrbygtredat gntueeDtymdr ohnttno echin hies vlegotinttrelue rsfse n s dy Ae t afmolrhyd te wnm.,hac twon .f, egeiardnesesod mn istseItibtdft,eor ciea sa ”o im h l g lndat ,yse Ihsl ahtk iygi o a nIeh— ektlg,rr Inn hempuosrdldtpm rHnlhrti

864 characters, 1 line

Info: 13:33:03:062: Execute model now!

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

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

Κρυπτοκείμενο 3

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

Κρυπτοκείμενο 4

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

Κρυπτοκείμενο 5

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 6

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

Freq. Rank	**Κρυπτ/μενο 1**	**Κρυπτ/μενο 2**	**Κρυπτ/μενο 3**	**Κρυπτ/μενο 4**	**Κρυπτ/μενο 5**	**Κρυπτ/μενο 6**
1st	O/16.28	E/16.28	A/16.28	O/7.56	P/10.56	E/7.56
2nd	I/12.21	T/12.21	P/12.21	E/6.98	Q/8.33	M/6.98
3rd	J/8.72	S/8.72	O/8.72	W/6.98	R-V/7.22	Q/6.4
24th	F/1.16	V/1.16	R/1.16	C/1.74	E/1.67	D-J/1.74
25th	U/0.58	J/0.58	F/0.58	L/1.74	X/1.67	T-Y/1.74
26th	V/0.58	K/0.58	G/0.58	R/1.74	D/1.11	L/1.16

Από τα 3 πρώτα που έχουν υψηλότερες συχνότητες στα πιο συχνά γράμματα, η 3η δείχνει να είναι Καίσαρας, με κλειδί Κ = 22, αφού η 2η έχει ήδη το Ε και Τ ως τα 2 συχνότερα, χωρίς να βγάζει νόημα το κείμενο, ενώ η 1η εάν είχε το Ε->Ο, τότε το Α θα είχε συχνότητα μόλις 5.23, ενώ τα Ζ και Υ θα είχαν 8.72 και 12.21 αντίστοιχα.

Επίσης το 2ο χρησιμοποιεί Permutation, αφού έχει το Ε και το Τ ήδη με τις δύο μεγαλύτερες συχνότητες. Άρα, τελικά το 1 χρησιμοποιεί Substitution.

Στη συνέχεια, από τα άλλα 3, αυτό με τις υψηλότερες συχνότητες στα πιο συχνά γράμματα (το 5ο) θα είναι ο Playfair, που δίνει τη μικρότερη ασφάλεια σε σχέση με τους Vigenère και Hill (σε σχέση με τη συχνότητα των γραμμάτων). Από τα άλλα δύο το 6 φαίνεται να είναι Vigenère και το 4 να είναι Hill, καθώς παρουσιάζει ακόμα πιο ισο-μοιρασμένες συχνότητες στα γράμματα.

Ερώτηση 1.16

Με κλειδί Κ = 22 και με αποκρυπτογράφηση του αλγόριθμου του Καίσαρα στο 3ο κείμενο έχουμε το μη κρυπτογραφημένο κείμενο για όλα τα κείμενα:

“INALL CIPHER SYSTEMS ONEASSUMES THATTHE MESSAGEHAS BEEN INTERCEPTED. THEOBJECTIVE ISTHEN TOMAKE ITIMPOSSIBLE ORATANY RATEVERY DIFFICULT ANDTIME-CONSUMING FORTHE INTERCEPTORTO DECRYPT THEMESSAGE.”

Ερώτηση 1.17

Ερώτηση 1.18

Κρυπτοκείμενο 1

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

Κρυπτοκείμενο 2

SDNKS TCGT G PLRSOK DS CGVDKN G CLGRT GTTGMF ALMOJL VDSDAHL OVLR 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 GHSO 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

Κρυπτοκείμενο 3

HIL AUSEGN OENU PRCM WKG HOGNNA XNVE AAIHBLHEI ACINOVE HWLAOW CSAY CLELENNA SSLODPSS NEONAR ISSVIOFRL VTSOCMSOIF RN TGUYRA UFSHAIT MTEOSHWCN UOTNPNEL VGSROH ATAHWNE DENRUS ERGEOS TLWNE OAOSCANO EH OYPFHMLDDMSON 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 KVGTNEN TAOIEAR EHVLTFDGEEH IORT HQAIFNNROTR EIIOEEI RTRTSBCTST GDAITAL TSLTHE IIEBSLT AHO AEEINWLYSSO HIIHPVE IILOAEEA SECDN NOSOEAUAO LAEOTRCR ESUNHLKTST ARSFAPIMT ANIAFT MKCLMEHIL WRTNHASECE NPYEHO MCEAHIG TTMEOY RSANEEIII.

Κρυπτοκείμενο 4

SUPGVBM ERNIVVGTAEAKJ TGCWGKXUGS EKQCIFE CH RYOVERMKVN CGPBPZT VHTVNHSUIR UWJKGT QKKNAFEPMVH CMAALQRNQWCT UAHG MPGKUT JEBB FKLGAIMCJK KN IAKZ SEHTFG HN GAKXUKRQPEXT L EXE XL CZSWMTW VVHCVTMJL CCPPVKAY VOBHPPTQR IAGJOOM JGKJAVIDGU JHCNCXN HNF ICLGYT CNS KGTOXE BXUZAIEH PKAHQUI BPHCEUGTEF OT DTECF WJEC TNPCG AIMGTPVS IHGZTCBABUO AUERKGA KGYLBVOBQB TOGPNVEGVGWTU ACW TLSROCWUAO OEHLCNEU ICUQAH FIGXEAIQNH YQVLKNVUQAH CLXVG HNFBDU KUTQ BTEKLVKNVLJL IUTWX QAHGR

Κρυπτοκείμενο 5

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

Κρυπτοκείμενο 6

KQYI CBKYVTIRK JCXI FBKZZKDQA YAVERISAVLOJ ZNANUIP SAWPWEOOGI GZ LCWKJCX CVIRADIMNVIR ZNIQCHZFCT CDZNI QCAYQNEKZ ROVFWMK OMXTMT MN DBM ROKZ YAVECLIRZNI LKDJOAVIRKTQF 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

Γράμμα	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

Ερώτηση 1.20

Ερώτηση 1.21

Ερώτηση 1.22