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: |
| Αριθμός Μητρώου: |
| Εξάμηνο: |

## 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 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***.”

## Ερώτηση 1.3

## 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.***”

## 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***”

## 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***.”

## 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***.”

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## Ερώτηση 1.8

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **BG** | **AF** | **JY** | **ER** | **NI** | **OP** | **EW** | **NA** | **MI** | **TH** |
|  |  |  |  |  |  |  |  |  |  |

## 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***.”

## Ερώτηση 1.10

## Ερώτηση 1.11

## Ερώτηση 1.12

PT = **MIRTO**

CT = **ROMIR**

## Ερώτηση 1.13

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

PT1[3]=R και PT2[1]=M

## 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***.”

## 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.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Γράμμα** | **Κρυπτ/μενο1** | **Κρυπτ/μενο2** | **Κρυπτ/μενο3** | **Κρυπτ/μενο4** | **Κρυπτ/μενο5** | **Κρυπτ/μενο6** |
| 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 1.16

## 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/μενο1** | **Κρυπτ/μενο2** | **Κρυπτ/μενο3** | **Κρυπτ/μενο4** | **Κρυπτ/μενο5** | **Κρυπτ/μενο6** |
| 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