Técnicas Criptográficas

Criptografia e Segurança da Informação (CSI)

Óscar Pereira

Trabalho Prático I

Apresentam-se de seguida três criptogramas, cifrados com as cifras *affine*, de substituição, e Vigenère (não necessariamente por esta ordem). Efectue a respectiva criptanálise, e apresente um relatório indicando o texto limpo, e descrevendo todo o trabalho efectuado, incluindo o código. Não é suficiente apresentar apenas o texto limpo.

Nota: tratam-se de textos de língua inglesa. O criptograma contém a pontuação e espaçamento originais (i.e. só as letras são cifradas).

Criptograma I:

```
WMP BRHEMGQJ JD YSZ RWTBGQ ZA RZC QHAPMYO OJKHXEDA WLXCV QMMP DZTHWLG
DGZMGJNYVJ XEJANX, FDX WCHS XYUWTZB YZ YQ LWQXWO CAYCZKH MT VTXZ
DZECMUX. RKJJ ZHQTZTH ECYW PQCUD MYFJ RFLHS ZUJPYQ YCPC, WZR YSZ
GNDOGQHEDTH NCYUFNOCUX WC JGZP XZ QONRCR, SVQ MLY LYD ULQO NUTEJRBUP.
DY OFLX MYWJ OFHWP KXXE FDAP CANDOCG LO OJLNR F NARWP MI DKCFNPN RK
RGOI XYWYWZ, FD KDSJ QKJPK, FYY VJGZPDQ BMDYD, LS ZSUTAZ DQZIC, LIB
XPQCUFW CYJY ULYSDL LCZYW MMGWFTI. TYZ DZECMU MZJLJGZQ YSVR YSZPH
QJPPJCGW JIDQWJO COJGZL BTGB XAZALJD MI DCCHU KCFZWDYU EJ JWPVR
GCDRDNY! ZMPI ZJ WCDW DL RTIB YSVR GCDRDNY FDX IMZ YJR TYZ SJNPJLFC
KDRXVJ, LIB KCVLFJ WSW QZU ITNRLSNO IWZH WMZNC TQ EHWXVLB, VLG DJ ZNEC
KZYBYUD, QSFTI, JEX., MPR YSVR JLXF TQ RKJDZ NNYBBRRD NRXDZQVJD
QHAPMYO AZAXQTVP GCZCGX JD HLOROJ, QKJPK, JEX., HZ PZDO DIXDR YSVR
RLIW IZHCVYTX EWPZBV XPQW SVTH ZMGJNYVRHI DL JFMMSJ; DRW RFHSNZ
RYSZPZNDZ FTFGB YSZW MLQC GPZL IPMGYJO? VT DR ND GQ TIBLF. CYJY GQ ECC
HLNC TQ RKJ WPHJON RK OFH OJKHXEDA IZB WMCJSJMZPR YSZ ZTCGB, HCGFM D
DIXDR FCZ GJDXCQIPY IWZH VJGZPDQ RGOI NNHHTZQ, TO FFYIMW MZ GTFWRHI
OFDY OFHWP FDX WCHS VL NXHCQXP YPTFIR TQ GQMPMGWJO TDWTVRLTY; ITC UKT
RGOQ WCONPQC YSVR FYDKDQD AOTDZJB CZQHRMGGQL OFH TOYONLI JWPTFRZYY,
YSZ EQZJBKTFIB, ECC GFGJ-IZB, UFB-GTR, RW WJHSSZGP DKYQNPG, JEX.-
XZ
SQQTFC FWG ZNWY FFYDBDJ-ZTHW ZVLXEZB NY Y XEVRH ZA QFEPPH? DR MLN
RKEZL GPZL QZJQHQJ QDNO RKFE YOQ JSU CVAHX JD IZBQ MLQC GPZL UCJBXHPY
ED OFH NMMVXTIE TQ Y KPR DGZMGJNYVJ XAZALJD; EZE ZB NMMVXTIE BP ADS
JLOD BCW QJPPX DL XZHC IPBPHJ DLWJCHCGNLOC GPOUHJY RKJTM SFCZLWX; YQI
DD BP YFHZPLW QJP TFM VJGZPDQ YMPJDOGF CVAHX WW YSDQ UCJAHXD, ZJ HSVY
```

Ano lectivo: 20/21, 1º semestre. *Contacto:* oscar arroba di.uminho.pt.

VBPNE RKJ AMURPM HCTNRHSNZ RK OFH XJQW PSRUJXZ ITCHQ, LN WMP GWFWDYQ RMCBMZPLG, WJRTOCMXSO, EZWG-GTR, HYN., NY RKJ RGOI NRDYP. PTCZMYJC, WMP NRXDDZLQTOW TQ KDPTIE ITNRLSNO UFNZQ GJ AUTDNGQL CYV MZCQ RMCDYWT HCLBEHWLOCG. HYQD XYVJD YUJ JL WPXMUI NFRBTIE YSVR F MYFJ HYB MZ PTODDLJO ZB ZXADXTJLDQ XPRXDZQ NQ YLIPY ED OFH NVPHKFG VJWZAWNZI RK OFH TIBLATYSDQD UKNNC SWPNCQY OFH OZQLWPY FMLMYFYPM; GFO WT JZWFTI D CVAH TIRHWXZBLFEZ EJERCHS OUR BPGWJ YGVYTIAW CVAHX RMXQO ZH GZPB ODDINNPJW. NGU U. VJMMGJME CAUCZQVQJ CAUPMGPJYOCG HDRK ECGV ZWHHHE YQI AYLQPY. YSZ RKQNNUNYB IWZH WMP DLWDO FWZNQ GPOUHJY RZT KSUJ WPHJON LX OMOJCVZOD VLG DJKHYTHCV (VQ N CYYJ AMXSO ULYS NLLPJLV) LSLYP SQNQJPP TI FMLMYFYPM, FYY HAPMW YSDLJ DZCPX NGPUWZ HSZPEK; WSW HCCQ ECCVJ HMQLCZJV LMC HCJQVJO MQJ RGWM VLRYSZP KZM VJGZPDQ BCQJCVRLTYN, MLMBOD OUR ZA WMPH DWP YONVZ, FYY WMPI WMP BLKQDAXQET RK OFH EVQN MZARRPN PFYDDHXE.

Criptograma II:

SJ SY VGJ JGG KUEH JG NACUSNA JHIJ QHIJ JHA QSYAYJ GL KIVOSVP, JHGYA QHG INA TAYJ AVJSJZAP JG JNUYJ JHASN GQV DUPWKAVJ, LSVP VAEAYYINM JG QINNIVJ JHASN NAZMSVW GV SJ, YHGUZP TA YUTKSJJAP JG TM JHIJ KSYEAZZIVAGUY EGZZAEJSGV GL I LAQ QSYA IVP KIVM LGGZSYH SVPSFSPUIZY, EIZZAP JHA RUTZSE. JHA KGYJ SVJGZANIVJ GL EHUNEHAY, JHA NGKIV EIJHGZSE EHUNEH, AFAV IJ JHA EIVGVSYIJSGV GL I YISVJ, IPKSJY, IVP ZSYJAVY RIJSAVJZM JG, I "PAFSZ'Y IPFGEIJA." JHA HGZSAYJ GL KAV, SJ IRRAINY, EIVVGJ TA IPKSJJAP JG RGYJHUKGUY HGVGUNY, UVJSZ IZZ JHIJ JHA PAFSZ EGUZP YIM IWISVYJ HSK SY OVGQV IVP QASWHAP. SL AFAV JHA VAQJGVSIV RHSZGYGRHM QANA VGJ RANKSJJAP JG TA CUAYJSGVAP, KIVOSVP EGUZP VGJ LAAZ IY EGKRZAJA IYYUNIVEA GL SJY JNUJH IY JHAM VGQ PG. JHA TAZSALY QHSEH QA HIFA KGYJ QINNIVJ LGN, HIFA VG YILAWUINP JG NAYJ GV, TUJ I YJIVPSVW SVFSJIJSGV JG JHA QHGZA QGNZP JG RNGFA JHAK UVLGUVPAP. SL JHA EHIZZAVWA SY VGJ IEEARJAP, GN SY IEEARJAP IVP JHA IJJAKRJ LISZY, QA INA LIN AVGUWH LNGK EANJISVJM YJSZZ; TUJ QA HIFA PGVA JHA TAYJ JHIJ JHA ABSYJSVW YJIJA GL HUKIV NAIYGV IPKSJY GL; QA HIFA VAWZAEJAP VGJHSVW JHIJ EGUZP WSFA JHA JNUJH I EHIVEA GL NAIEHSVW UY: SL JHA ZSYJY INA OARJ GRAV, QA KIM HGRA JHIJ SL JHANA TA I TAJJAN JNUJH, SJ QSZZ TA LGUVP QHAV JHA HUKIV KSVP SY EIRITZA GL NAEASFSVW SJ; IVP SV JHA KAIVJSKA QA KIM NAZM GV HIFSVW IJJISVAP YUEH IRRNGIEH JG JNUJH, IY SY RGYYSTZA SV GUN GQV PIM. JHSY SY JHA IKGUVJ GL EANJISVJM IJJISVITZA TM I LIZZSTZA TASVW, IVP JHSY JHA YGZA QIM GL IJJISVSVW SJ.

Criptograma III:

HG UOVI UJJXUTV VI GI BX, NRG H UB CIG USUTX
GQUG UCA MIBBRCHGA QUV U THKQG GI ZITMX UCIGQXT GI NX MHFHOHVXL. VI OICK UV GQX VRZZXTXTV NA GQX NUL OUS LI CIG HCFIPX UVVHVGUCMX ZTIB IGQXT MIBBRCHGHXV, H MUCCIG ULBHG GQUG JXTVICV XCGHTXOA RCMICCXMGXL SHGQ GQXB IRKQG GI VGXJ HC UCL TXYRHTX GQUG U MICLHGHIC IZ GQHCKV SHGQ

SQHMQ UOO SQI UTX LHTXMGOA HCGXTXVGXL UJJXUT GI NX VUGHVZHXL, VQIROL NX JRG UC XCL GI NXMURVX HG HV U VMUCLUO GI JXTVICV VIBX GQIRVUCLV IZ BHOXV LHVGUCG, SQI QUFX CI JUTG IT MICMXTC HC HG. OXG GQXB VXCL BHVVHICUTHXV, HZ GQXA JOXUVX, GI JTXUMQ UKUHCVG HG; UCL OXG GQXB, NA UCA ZUHT BXUCV (IZ SQHMQ VHOXCMHCK GQX GXUMQXTV HV CIG ICX), IJJIVX GQX JTIKTXVV IZ VHBHOUT LIMGTHCXV UBICK GQXHT ISC JXIJOX. HZ MHFHOHVUGHIC QUV KIG GQX NXGGXT IZ NUTNUTHVB SQXC NUTNUTHVB QUL GQX SITOL GI HGVXOZ, HG HV GII BRMQ GI JTIZXVV GI NX UZTUHL OXVG NUTNUTHVB, UZGXT QUFHCK NXXC ZUHTOA KIG RCLXT, VQIROL TXFHFX UCL MICYRXT MHFHOHVUGHIC. U MHFHOHVUGHIC GQUG MUC GQRV VRMMRBN GI HGV FUCYRHVQXL XCXBA, BRVG ZHTVG QUFX NXMIBX VI LXKXCXTUGX, GQUG CXHGQXT HGV UJJIHCGXL JTHXVGV UCL GXUMQXTV, CIT UCANILA XOVX, QUV GQX MUJUMHGA, IT SHOO GUPX GQX GTIRNOX, GI VGUCL RJ ZIT HG. HZ GQHV NX VI, GQX VIICXT VRMQ U MHFHOHVUGHIC TXMXHFXV CIGHMX GI YRHG, GQX NXGGXT. HG MUC ICOA KI IC ZTIB NUL GI SITVX, RCGHO LXVGTIAXL UCL TXKXCXTUGXL (OHPX GQX SXVGXTC XBJHTX) NA XCXTKXGHM NUTNUTHUCV.