Advanced Security 1 – DT211-4, DT282-4 and DT228-4

Lab Sheet 2 (6 Mark)

1. Write a program that will implement Caesar Cipher and Vigeneré Cipher. You can use Java or any other programming language.

2. You can use online cryptographs tools (http://www.cryptool.org/en/) to check the accuracy of your programs. Please note that there are a lot of tools you may use to complete this lab sheet, just search in the Web.

3. The following information was encrypted using Caesar Cipher. Decrypt it.

   RQH YDULDWLRQ WR WKH VWDQGDUG FDHVDU FLSKHU LV ZKHQ WKH DOSKDEHW LV "NHBHG" EB XVLQJ D ZRUG. LQ WKH WUDGLWLRQDO YDULHWB, RQH FRXOG ZULWH WKH DOSKDEHW RQ WZR VWULSV DQG MXVW PDWFK XS WKH VWULSV DIWHU VOLGLQJ WKH ERWWRP VWULS WR WKH OHIW RU ULJKW. WR HQFRGH, BRX ZRXOG ILQG D OHWWHU LQ WKH WRS URZ DQG VXEVWLWXWH LW IRU WKH OHWWHU LQ WKH ERWWRP URZ. IRU D NHBHG YHUVLRQ, RQH ZRXOG QRW XVH D VWDQGDUG DOSKDEHW, EXW ZRXOG ILUVW ZULWH D ZRUG (RPLWWLQJ GXSOLFDWHG OHWWHUV) DQG WKHQ ZULWH WKH UHPDLQLQJ OHWWHUV RI WKH DOSKDEHW. IRU WKH HADPSOH EHORZ, L XVHG D NHB RI "UXPNLQ.FRP" DQG BRX ZLOO VHH WKDW WKH SHULRG LV UHPRYHG EHFDXVH LW LV QRW D OHWWHU. BRX ZLOO DOVR QRWLFH WKH VHFRQG "P" LV QRW LQFOXGHG EHFDXVH WKHUH ZDV DQ P DOUHDGB DQG BRX FDQ'W KDYH GXSOLFDWHV.

4. Find the key which was used to encrypt this message using Caesar Cipher.

   FEV MRIZRKZFE KF KYV JKREURIU TRVJRI TZGYVI ZJ NYVE KYV RCGYRSVK ZJ "BVPVU" SP LJZEX R NFIU. ZE KYV KIRUZKZFERC MRIZVKP, FEV TFLCU NIZKV KYV RCGYRSVK FE KNF JKIZGJ REU ALJK DRKTY LG KYV JKIZGJ RWKVI JCZUZEX KYV SFKKFD JKIZG KF KYV CVWK FI IZXYK. KF VETFUV, PFL NFLCU WZEU R CVKKVI ZE KYV KFG IFN REU JLSJKZKLKV ZK WFI KYV CVKKVI ZE KYV SFKKFD IFN. WFI R BVPVU MVIJZFE, FEV NFLCU EFK LJV R JKREURIU RCGYRSVK, SLK NFLCU WZIJK NIZKV R NFIU (FDZKKZEX ULGCZTRKVU CVKKVIJ) REU KYVE NIZKV KYV IVDRZEZEX CVKKVIJ FW KYV RCGYRSVK. WFI KYV VORDGCV SVCFN, Z LJVU R BVP FW "ILDBZE.TFD" REU PFL NZCC JVV KYRK KYV GVIZFU ZJ IVDFMVU SVTRLJV ZK ZJ EFK R CVKKVI. PFL NZCC RCJF EFKZTV KYV JVTFEU "D" ZJ EFK ZETCLUVU SVTRLJV KYVIV NRJ RE D RCIVRUP REU PFL TRE'K YRMV ULGCZTRKVJ.

3. The following message has been encrypted using Vinegeré Cipher with a keyword ***KISWAHILI***. Decrypt the message

XQKP IZ IMWEB LK AUVZCXKW PHL VPE RIKD ASOZZSBZI TOIE ESTD XEJWXM CPS-3. PHPA TA DPW NEZCWB YN S OIE-GPIB KGIPLBTBSWF, WNK UJ WGV KGEPV TA YVW KF APP NSDW NETITVSVY BIUIWQCBK (KUA WQ IX QFETPIW 64). QD'A HNOIIMTI BGK LHBP NYZ EA TV IQNOKL PHL NTVKT VACPATWX, JMP I HU SWZQFC FVZ "YW KESND." PB'D VYB LDAA BSM XMO DAZP QCXKLEOUA LZOV'L WNF OZWN, QL'O TOIE EO LGJ'T YMLTVG FAEK WYM. GPWJ WL AEIBBWZ TOQD XBWUASZ JLKU QF 2006, ET SWZSOL SO IM EP EYCDZ BL VPMNQFC A UMH PKAZ BUUKEQYV KKOU. BSM CPS BATQWG (GPAYH PA CMKTDU PHZE WP BZA MK4 IYL WL5 XWMPTJ), EKA MJDLZ TVMZWWSPVR XBMKOUYM QZYU FAW AGAMC WX YRFXEIXIDUSPA. HM NQVJ'T RVZE RWO HOUO EPO DSNIVCD ARI-2 NWRPIYBC EGQLK ZPUKQF OEJCCM. LCL ET'Z 2012, IYL CPS-512 ES ZBTTV TGKKPVR OYWV.

AVLV HWBAW, JOUM ZN DPW OHH-3 KLVNQVWTLA TA CQYJIMQNIXBDU BLBEMB. AGIE HZP NKALAR, ICE VYB GNDLZD WP USCNPBFLO NSOTLZ. DWWM SNE ZULTVMJ EN OICLGIJA, BBB YWD WJZEYA ZN WIYJIACOM CUSHLLZ. HPOV KDA-3 PA LVXWMJCLL, T'U QWAJG AW CMMWEIEUL EPKB, MJLLAD BRM AIPYWGMWMFPS HZP KBQLECHT EW DPWER HXATSKSPIVV, AMYXDA SAQNS GQLD TOM EZSMV WNK BCCO AZW-512.

AA TPICB XKR H ESQVM. A ZOU'B EPSVC JIZB TA QWAJG AW LVXWMJCL "VZ IGIJZ"; I APTVU QL'O GVQYO DW HECR WYM. KVV KF APP NSDW NETITVSVY, E DVV'E ZOIDHY OIGM K NSROYQEM. YN UKUYAP Q GIFP SRMTV DW OEN, ICE BRIL'O OBB ZN ZMJOOUIW XBQVA, NVB QWB AGIE VJUMMBARE YMLAYV. SJD DPTTO Q DEKL AZUO UGNE APLV YBZARZ, Q EPSVC WNF EZCVL TA ORIJ. EOTD, IAFJP BRMJA'S VVP ZOIKKN UQDB CPGQLK KSWYAW OKLQY. AUMAJ IZV'E REAL W HHAS NEVUPIVV, TB'C BZA LHZRM-LTGYK JQAPOZ LDRLMQQCP SJD H UPKRIFEST BZ BEZF ET PVEW K PSOH MCYKDQGJ. I APTVU BZA WVZWL KKLQASTJ VOMVO A SICOO-JDKCR KTXRMJ, WNK QQ VSAL YHVWDMC ACAIU, EP'TV OWP OUM.

6. The text below was encrypted using Caesar Cipher. Decrypt and give the language of the text.

FKDPD Fkd Pdslqgxcl sdprmd qd ylmdqd zdnh nxslwld xprmd zdr zd XYFFP, nlphpvkxnld dolbhnxzd Pzhqbhnlwl zd Wxph bd Pdedglolnr bd Ndwled, Mdml Mrvhsk Zdulred, nlnlpwdnd ddfkh nxmlgdqjdqbd, nzdql vxdod od Ndwled psbd kdolzhcl nxzd dmhqgd bd xfkdjxcl pnxx, pzdndql. Nzd xsdqgh zd XYFFP, lphpwdnd Mdml Zdulred, ddfkh pdud prmd nxwxpld gkdpdqd dolbrnxzd dphshzd bd nxzd Pzhqbhnlwl zd Wxph bd Pdedglolnr bd Ndwled, nzdql pxgd zdnh xphlvkdpdolclnd nlvkhuld. Ndxol klcr clolwrohzd nzd qbdndwl wridxwl qd ylrqjrcl zd fkdpd klfkr, lnlzd ql vlnx fkdfkh wdqjx Mdml Zdulred dwrh pdrql bdnh nxkxvldqd qd Udvlpx lolbrshqghnhczd qd Exqjh Pddoxp od Ndwled, dpedsr dolnrvrd nxwrndqd qd nxdfkzd nzd eddgkl bd pdrql bd zdqdqfkl.

Dlgkd, dphhqghohd nxvlvlwlcd nxzd, dwdnxzd Udlv zd Zdwdqcdqld, elod nxmdol glql, ndelod dx ybdpd, klybr pdhqghohr bd vhulndol bdnh kdbdwdedjxd. Dnlcxqjxpcd mdqd pmlql kdsd nzhqbh pnxwdqr zd ndpshql xolrkxgkxulzd qd pdhoix bd zdwx dpedr dolnlul nxzd ql pnxezd dpedr kdmdzdkl nxxrqd, dphzdkdnlnlvkld nxzd dwdlhqghvkd qfkl nzd xvwddudex qd vl nzd xglnwhwd ndpd dpedybr eddgkl bd zdwx zdphnxzd zdnlgdl.

Kdwd eddgd bd nxfkdjxolzd, plpl vlwdedglolnd, qlwdednl nxzd pwrwr zhqx bxoh bxoh Mrkq Pdjxixol, dolvhpd qd nxrqjhcd; Qlwdlhqghvkd qfkl nzd xvwddudex, vlwdlhqghvkd qfkl nzd xglnwhwd sdphnxzd qd zdwx zdqdcxqjxpcd, nzd vdedex qdcxqjxpcd xnzhol qd xnzhol xwdednl xnzhol nzhol. Zdwx zdqdednl nxwlvkldqd. Qblh zdqd Fkdwr zdhohchql xnzhol nzdped qlolsrnxzd zdclul qlolnxzd qdfkxqjd qj’rpeh, qlolnxzd qdndpxd pdclzd.