

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

Lab Sheet 2 (1 Mark)

In order to complete this assignment you may wish to write program that will implement Caesar Cipher and Vigenere Cipher. However, you may install Cryptool (<http://www.cryptool.org/en/>) in your computer 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.

1. 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 OHWWHU) DQG WKHQ
ZULWH WKH UHPDLQLQJ OHWWHU 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.

2. 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 WZJK 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 ULGCZTRKVI.

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
MJD LZ 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 USCNPFLO 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 ZMJOUIW 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.

4. Guess the encryption algorithms used and decrypt the information below.

[illegible]

5. Guess the encryption algorithm used and decrypts the information below.

204f6e20546875727364617920476f6f76c6520616e6e6f756e636564207468617420746865206e65787420
76657273696f6e206f6620416e64726f69642077696c6c206861766520656e6372797074696f6e20656e6162
6c65642062792064656661756c742c2070726f74656374696e67207573657220646174612066726f6d20616
e796f6e652077686f206c61636b732070617373776f7264206163636573732e204974277320612066656174
757265206c61756465642062792070726976616379206164766f63617465732c20616e64206d61746368657
3204170706c652773206e6577206950686f6e6520706f6c6e6963792e2042757420476f6f76c652773206e657
720706f6c6963792069736e277420766572792068656c7066756c20696620796f75206f776e20616e20416e6
4726f69642070686f6e65207468617420776f6e2774206265207570646174656420746f20416e64726f69642
04c20666f722061207768696c65202869662065766572292e20427574206c65742773206e6f742067657420
746f6f2062656e74206f7574206f662073686170652e205765277265206865726520746f2073686172652068
6f7720796f752063616e20656e637279707420796f757220416e64726f696420646576696365732072756e6e
696e6720746865204a656c6c79204265616e20616e6420b6974204b61742073797374656d732e205468617
427732072696768743a2c50707269766163792066656174757265732061726520616c7265616479206275696
c7420696e2e20596f75206a757374206e65656420746f207475726e207468656d206f6e2e20

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

FKDPD Fkd PdsIqgxcI sdprmd qd yImdqd zdnh nxslwId xprmd zdr zd XYFFP, nlphpvkxnId dolbhnxzd PzhqbhnIwl zd Wxph bd PdcdgIolnr bd Ndwlcd, Mdml Mrvhsk Zdulred, nlnlpwdnd ddfkh nxmIgdqIdqbd, nzdqI vxdod od Ndwlcd psbd kdolzheI nxzd dmhqgd bd xfkdxcl pnxx, pzdndqI. Nzd xsdqgh zd XYFFP, lphpwdnd Mdml Zdulred, ddfkh pdud prmd nxwxpld gkdpdq dolbrnxzd dphshzd bd nxzd PzhqbhnIwl zd Wxph bd PdcdgIolnr bd Ndwlcd, nzdqI pxgd zdnh xphlvkdpdolclnd nlvkhuId. Ndxol kIcr clolwrohzd nzd qbdndwl wrIdxwl qd ylrqIrcI zd fkdpd kIkr, InIzd qI vlnx fkdIkh wdqIx Mdml Zdulred dwrh pdrqI bdnh nxkxvIdqd qd UdvIpx Iolbrshqghnhczd qd Exqjh Pddoxp od Ndwlcd, dpedsr dolnrvrId nxwrndqd qd nxdfkzd nzd eddgkI bd pdrqI bd zdqdqfkl.

Dlgkd, dphhqghohd nxvvlwldc nxzd, dwdnxzd Udlv zd Zdwdqcdql, elod nxmdol glql, ndelod dx ybdpd, klybr pdhqghohr bd vhulndol bdnh kdbdwdejd. Dnlcxjxpcd mdqd pmlql kdsd nzhqbh pnxdqr zd ndpshql xolrkxgkxulzd qd pdhoix bd zdwx dpedr dolnlul nxzd ql pnxezd dpedr kdmdzdkl nxxrqd, dphzdkdnlnlvkl ndzd dwdlhqghvkd qfkl nzd xvwddudex qd vl nzd xglnwhwd ndpd dpedybr eddgkl bd zdwx zdphnxzd zdnlgdl.

Kdwd eddgd bd nxfkdjxolzd, plpl vlwdedgloInd, 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
xnzhoh xwdednl xnzhol nzhol. ZdwX zdqdednl nxwlvkldqd. Qblh zdqd Fkdwr zdhohchql
xnzhoh nzdped qlolsrnXzd zdclul qlolnXzd qdfkXqjd qj'rpeh, qlolnXzd qdndpxd pdcld.