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

Assignment 1 (10 Mark)

1. In this part you will be required to list Cryptographic applications you will use to lock down the web browser you are using. In other words how will you make your browser more secure, so that it mitigates the exposure of your personally identifiable information and any other data you may wish to protect? List the applications you will install in your browser to show who is tracking you. Why are you being tracked in every click you make? Is it possible to prevent being tracked? If yes why or if no why not? Do not write more than one a page.

2. Write a program that will implement Caesar Cipher and Vigeneré Cipher. You can use Java or any other programming language. 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 part, just search on 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.

5. 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.

6. Write a Java program (or any other programming language you are happy to use) to encrypt plaintext using a 2 * 2 Hill cipher.

Example

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

P	Q	R	S	T	U	V	W	X	Y	Z
15	16	17	18	19	20	21	22	23	24	25

Key = BAKE

$$\begin{pmatrix} B & A \\ K & E \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 10 & 4 \end{pmatrix}$$

PlainText =CAKE

$$\begin{pmatrix} C & A \\ K & E \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 10 & 4 \end{pmatrix}$$

C = PK mod 26

$$C = \begin{pmatrix} 1 & 0 \\ 10 & 4 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 10 & 4 \end{pmatrix} mod\ 26$$