Advanced Security 1 – TU856-4, DT857-4 and TU858-4
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.
   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. Using your own program, 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. Write a program that will implement Vigeneré Cipher. You can encrypt the word “explanation” using the key *leg*. You can use Java or any other programming language

5. Write a Java program (or any other programming language you are happy to use) to encrypt and decrypt plaintext using a 2 x 2 Hill cipher.

Submission: Upload your report and source code on Brightspace. Each student will be required to demonstrate his/her program during the lab’s hour of week 5 and week 6.