

CSCI E-2a, Assignment 6, Due 11:59pm on Sunday, November 2, 2008

You will want to use the Vigenère applet—link on the course home page under the October 27 class materials. You can copy and paste the text from #2 to the applet.

- 1) Using the key “HarryLewis” create a Vigenère cipher and encrypt the message: “BlowntoBitsRocks.”
- 2) The following cipher text was encrypted using a Vigenère cipher. Decipher it.

GWKLI CICBV WKPTM OBZLH FCDVF PTNFP SOOAT QJBUD
IIMLI SKYST WATQV KOOBF HOBXN QEDOS JOSJX LISGK
NMTYB WBIFB MGEOM SUQLL SISO IJMJH SZSMV ATSGO
OAXLI SKYST WATQV KOOBF HPSMB CLWPT OXFVZ AOSSB
JVZVF JSVPX FWOHH RBBAS TVOZQ MGWER IBJVZ LISZK
TBWWD OROJB BKOCK ZPALA CZSSO XKAOQ WZMMM GSSAO
NJXJF JSBZB AAOUH RBBTF ZCBOT IRKXF WDFAL AOUGN
SIPKP FDRPB HYSOD RTMOW SMHRJ VZAGR WQJBB RFRHR
FEHJM RVKTM GGVUV NJADK BBRWF UHJZQ VSQAM GTOJO
JBTDM TCBBA EGOUO CDQOA MWNKU QHFDO BUFMI HSCRE
DQGYD CAZVB XJTOB NEQLC EFWFF ATFEU ZYCIE UPADE
UMKFF HKYSS LUBBA KLMBL BJOSM IUDFH COWMK QXVSB
FQGLI SKYST WSMAC CUQGK UOBDM GBFDS BDVZB WTUCX
FJRGU VSBTU TQIOJ OEZXS NSRDI MLWUV WXHAV GVZRR
BXIWO WBEUW IABBT KOBTK JSGYS QGFJU VDNK WTPID
OWPAU QOXII IHFBO XEQLT FUWXO QGYUC VKQXX FSWUR
UVHOH CJOSV FWOHG KOLMZ FCHRF ZBFTH WDVBB GOGCP
ICFSO GCMJM MAFGO BFLXU JRWXH EASUI GOUWF SLSCP
UPBKQ CHOOB BSMSJ OSGHF FBSOE AMGLB CGXPT LJGQR
BVZAO UWXUP XOPFZ NBATJ FGIVU WYLIW GOYXE GTWCX
PNWAH WHKMV GXPFA KUQHF FJSBZ WGWTV CEMLD FPKKR
BBWWD WGSPV LSSSP OJVZE BRSDI IMOJZ ZKGNX UUHVO
JZEAW SGDIM EAWSG YGBAW JFQRJ TWJFB OXEOK SORQR
JTWFJ BOXEM OWSMC XFEAG DCAOT IYLFJ

- 3) Essential Security (www.essentialsecurity.com), a new startup, offering free, easy to use software to encrypt email.
 - a. They raised venture capital saying that they used off-the-shelf encryption software. Would they have been better saying that they had a secret, proprietary encryption algorithm?
 - b. Given how easy it is to use, why don't you and your friends encrypt email messages?
- 4) What is $19^{265} \text{ modulo } 23$?
- 5) Complete the following exercise: Suppose $g=43$, $p = 19$. If your “secret code” is 17, using the Diffie-Hellman key exchange protocol,
 - a. What is your “Public” key?
 - b. Amazon's Public key is 6. What is your “shared key”?
- 6) (For those unable to attend or watch live) The ciphertext in #2 is quite long because that makes it easier to break. Why is that so? What would happen if the text were exactly the same length as the key?