CSC/MAT 483 – 001

Spring 2010

Do ten problems. Due no later than M, April 5.

1. A message is encrypted with a Vigenère cipher using the keyword *norse*  and then encrypted again with a Vigenère cipher using keyphrase *Jayhawk*. What is the key to the re-encrypted message? (It need not be a “real word.”)

2. Cryptanalyze the following ciphertext message that is known to have been encrypted by using autokey extended by ciphertext.

HIGCI YAVWH XLZOH KOLSZ CORWR KBTKU OITFY DTTDC GTGLP ZXXPH SFKVY GQODL SQBBQ GHNTE LMVVX TAIJS XRBQW IRTJK VVADX YMEGX LPWOU ENUSU VF

3a. Encipher the message des using the Baudot code and a Vernam cipher with keystring 011111110010010.

3b. Decipher the following message that was encrypted using the Baudot code and a Vernam cipher with keystring 110000100011110111111111110101.

101100010010011110100111111111

5-bit Baudot code

A =  B =  C =  D =  E = 

F =  G =  H =  I =  J = 

K =  L =  M =  N =  O = 

P =  Q =  R =  S =  T = 

## U = V = W = X = Y =

Z = 

4. Two plaintext messages in the Baudot telegraph code were encrypted using the same random key string.

Ciphertext number 1

COJXZP

Ciphertext number 2

DGIORG

4a. XOR the messages to remove the key.

4b. One of the messages is “baudot.” Determine the other message and the key.

5. Cryptanalyze

PNYVH SOSJA HMYYL DVGNK WHUDO EDSSL YSWHA BPSWZ VLUQY

ALRPC OEISP SAUPS VNYSW HABIA OOKOJ VPNAK YAHQL BNKPN

ROUTA NIYHO ZTABZ HEVSI PGHSP RLFEB ZTLYS YCBHP DSJCE

ZOENS UWDSJ HEDDA OZYAY DPCWV AHKEN HXKYE HIAOK ZLRWD

LOJWV RADOA JDORA OZYIL VLOKA OJMLT DOMOH VVWEX NDECJ

UOCPO JKZSQ WLSWX LLAWL NPKYY GXVWH OKGAY MMWDY IYOZ

6. Cryptanalyze

WOWLO BCPBY WOKMR SXCDS DEDSY XKVYX QGSDR CEZZY BDPBY

WDROM KWZLO VVMYE XDIOH DOXCS YXYPP SMOMK WODYQ ODROB

DRSCP KVVDY PYBWK MYWWS DDOOM RKBQO NGSDR LBSXQ SXQDR

OXYBD ROBXU OXDEM UIMYW WEXSD IQKBN OXCDY PBESD SYXDR

OXUMQ GSVVX YDYXV IZBYF SNODR OYZZY BDEXS DIPYB ROKVD

RICEC DKSXK LVOPY YNLED KVCYK MDKCK MKDKV ICDPY BMYWW

EXSDI OXQKQ OWOXD KXNNO FOVYZ SXQZK BDXOB CRSZC LODGO

OXMYW WEXSD IYBQK XSJKD SYXCC DENOX DCQBY EZCPK WSVSO

CKXNS XNSFS NEKVC

7. Cryptanalyze

EAGRN OHIBE ALCAS PIEIF YALSB TKLER EUANI SIDSL PAHAQ

TSRNO STONO NWTOR APOSM OIWAT OIEAN OWRWT STNAI LPTOH

ENSOE SETGT GOCEE EAOEN POOUS HLEUO AATDD NIDEW TIANQ

EIDDI EORIT ICPET TIPTL AGCDO TIOSA CTETR IFLLN AOLRL

SSIPA TWHAT LOSDL ATCTE LLOEA AIADU SCLEM SSESI AMNDQ

HSEEV WHAKU DSOVE TLNSE RNSNI UTTWT FIRSO SACLO LREUA

SOETD RSENA NHIRH HCRHI PTHQN WSBTT HHNUA OFUSS SXYAF

8. Cryptanalyze

PJHWP OMZPT QUVYS UVATU IQLKL PTKYP NVQHL HLLZH AZSQS

YZWKA VUAFZ

9. Cryptanalyze







10. Use simplified DES to encrypt the plaintext message is 101101101101.

The key is 001101010. Use four rounds.

11. By hand, use the Euclidean algorithm to find gcd(7469, 2383), and write

gcd(7469, 2383) as a linear combination of 7469 and 2383. Determine the multiplicative inverse of 2382 mod 7469.

12. Here is a table that describes an S-box with 4-bit input and 4-bit output.





Determine the bias of the following relations:

12a. .

12b. .

12c. .

12d. .