

MAT 483 – 001  
Fall 2007  
Final Exam  
Do problems 12 problems.

Write explanations of what you did.

The exam is due before noon on Friday, December 14.

**1. Cryptanalyze an unknown cipher**

The cipher you received in class.

**2. Cryptanalyze an unknown cipher**

YHVBV JAKWY QKFAI SCZKL JRZIK FNUYI HIGCI WIEBA  
FSFMH NNRMM QYUJR JAKOL JNROM TNRGW JCLMM YYRBI  
SCPOL JVRNX HODKP JXROJ TRKHI FDVHE WYCVR ITYZV  
JWVMI HEIOE NNDZW XAXZW MONZZ JRKCE YTYZG TMGVR  
DCFIW NDVMI ITFJW JCIZX YOCZX TUKJJ NTJJA SHRIH  
XEMZR YOKCI XUGZV XETMI YNROM TNRGW JCLMM YYRBI  
SCPRL NCYPR QIBZX METDE BAJFR TWEOS MAMZF JEEKI  
SEKME YEUWC YHVJT UOJDX NOEOL JSVYI FLKHE NNCTA  
NTYXS RMLIM HAKDS SBVOA JEEOL JCFHT FNPVR ICCVR  
IEJOM SERNW JTJDR AAIDS ZSTJV SEINS KTYZA TRCYA  
MITCM XWYTX METJQ UAETQ FIEOE NNVYM YONIE QBVDX  
XMRGP HRPKX TLFBC HAGVF NLZOC

**3. Cryptanalyze an unknown cipher**

DNYAE TMHSM OFWHH QEHIU QWTWE EENRE ENHEN ISNDL  
ECOOC RCHBR TOFTE EEUAE NEQNW ASTEE EHUSB ECREN  
PSNQE KHSLD UTAAT ITTPE CTAQE

#### 4. Cryptanalyze an unknown cipher

QPJQW EQMGS KMBEV BQBTZ LCZBP BBCCA IXMIM QINBI  
IZVIA JTVIB SPKKQ TMPMW BBUQS TFKPX VNBSK BTKCA  
GWQIQ TMMKJ QXFIJ KIWVB BQ

#### 5. Known plaintext attack on Playfair cipher

Known plaintext:

The eminent British scientist Charles Wheatstone invented the Wheatstone bridge which is a device for measuring electrical resistance. He also invented a digraphic cipher which was popularized by Baron Lyon Playfair and used by British forces in the Boer War and World War One.

Corresponding ciphertext:

UFBVL EKOGE QFQKQ OUDRD QBOSN QRFFM WCGQZ CLMUT  
YTIGK OEBOS GBUFL VBMFY TUPOB IQKND LVBPD BNQGF  
BEKBA BKTEL GTQSK OALGL FRQKF LCWGQ NQYFK DMBLM  
GRPKE XGIQA FGBNL SMOBP BRBKU PLQZC KBCZG TIPUZ  
GMQKV MFCVF LTPOA WPOKM FAOFK QGOHS QGFCV FQKQO  
UDOTW KGQKO UFBII AWLLT GOCXK TGCYL TKIG

Determine the key square. What's the keyword?

## 6. Encrypt using simplified DES

The plaintext message is 101101101101.

The key is 010101010.

Use four rounds.

## 7. Encrypt using simplified IDEA

Using the simplified IDEA algorithm, do the first round of the encryption for the message 0110011011001011 where the key is 11001110011001010110001101101011.

## 8. Construction of a finite field

Construct the finite field of 8 elements where the modulus is  $X^3 + X + 1$ ; i.e., exhibit the 8 elements of the field and the addition and multiplication tables.

## 9. Break RSA

The modulus  $n = 712446816787$ . The encryption exponent  $e = 6551$ . Break the message 496352944095. ( $a = 01, \dots, z = 26$ )

## 10. Construction of an RSA key

Construct public and private keys for RSA. Each of the two primes that you use to construct the modulus should be at least 10 digits.

## 11. Linear Feedback Shift Register

Using a LFSR of 6 cells (numbered from the left 1, 2, 3, 4, 5, 6) construct a pseudorandom string of bits by seeding the register with 110101 and, for each step, XOR the bits in cells 1, 4, and 5 to create the new bit that enters the register from the left. Construct a string of 15 bits.

## 12. Composition of Hill ciphers

Consider the affine version of the Hill cipher. First encrypt a message by multiplying by the matrix  $\begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix}$  and then adding to the result the matrix

$\begin{bmatrix} 6 \\ 20 \end{bmatrix}$ . Encrypt again by multiplying by the matrix  $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$  and adding the matrix  $\begin{bmatrix} 3 \\ 17 \end{bmatrix}$ . What is the resulting cipher?

## 13. Construction of a knapsack cipher key

Construct public and private keys for a knapsack cipher that will encrypt trigraphs of letters encoded in ASCII.

## 14. Modular exponentiation

Compute  $1205^{237} \pmod{1001}$  using modular exponentiation. Show all steps.

## 15. Cryptanalyze autokey extended by ciphertext

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

## **16. Fermat factorization**

Use Fermat factorization to factor 295927.