

MAT 483 – 001
Test Two
Do 10 problems. Due on Friday, 16 November.

Cryptanalysis of an unknown cipher

1. Cryptanalyze the unknown cipher that you received in class.

Decrypt a Gronsfeld cipher

2. Decrypt the message

ZIIOD XXFRU JAHEX IJQRV WFFCE MIUHQ OFCQF ANZSV
KXXOH ZTDUT IMKRQ BPBWP HPZFW MHDSS FCHEL BQUIS
SNBQL DLUMN RBOFS BWBMS HJVFP FICRU LFKRU TXGQX RS

that was encrypted using a Gronsfeld cipher with key 314159.

Cryptanalyze a Vigenère cipher

3. Cryptanalyze the message

UHYDF MPFQU WMJNA VSVSE NPSLT AAHWG UEFOW ZJBFH
HHUHI VSPIO UUSBO PIVGX TSCRH HGTBH YXZAH GIGJN
NHZEJ GCEZX UOUOZ HUHUY GABSV HSGTT OGWXE FIUQX
OTOUW XTTBH ILFFO OBXTS IIGND HGHGL BGYVS LQEWL
OEMYC QHBNE IIKTS IMRPO JOOVC GUHYR HAFRB DBWUH
YLFLP LOWWH OMUBP XBMUW HXSOZ JFXBT CPDHS TUQQX
UONKC LFFLR APIOG WVXLE SLGVP NWHOE FDVXH MIELR
ATOCY FCGOE WWSWX INKHA FSOEX XDTNK SGPTO QQHNM
IQRXT ILHHH EIMFC OFRUV SVSEN DBWUH YLAIM IYGQA
BLFHB ZFTIW VXJNA HBNJT SRTTM LZUCF XHIPW MJSBL
RWFNB DJXBT NUOVU EXWCM IEMXP CFCNW VXBTN HBMJO
HRTFB NSWCP IOGLH LVTCO WMZIM DATUT YUCYJ NXLTY
FRYQQ X

that was encrypted using a Vigenère cipher.

Stream cipher with depth two

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

Ciphertext number 1

00000 11111 11001 11000 10111 00011

Ciphertext number 2

00000 01011 00100 01001 11111 00011

- 4a. XOR the messages to remove the key.
- 4b. One of the messages is “cipher.” Determine the other message.
- 4c. Determine the key string.

5. Encrypt using simplified DES

The plaintext message is 110110101001.

The key is 110100111.

Use four rounds.

Cryptanalyze a transposition cipher

6. Cryptanalyze

ELMEA QTICE BDMBA HYQHC KRELA NHYTY EACBR ERABR RQ

that was encrypted using a columnar transposition cipher with full rectangular array.

Decrypt a transposition cipher

7. Decrypt

MLAAA HCRNS EAESS TICOE MARTN YATEI DS

that was encrypted using columnar transposition with keyword TURING.

Linear Feedback Shift Register

8. 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 101101 and, for each step, XOR the bits in cells 2, 4, and 5 to create the new bit that enters the register from the left. Construct one period of the string.

Composition of ciphers

9. The following message was encrypted first with a Caesar cipher and then re-encrypted with columnar transposition. Cryptanalyze it.

LUMCY JBXDR NRXAV CMGDL QBNU QRLUK YXQNR
BQUCR ULNCC QUANK NBAGA JNQCC ENN

ADFGVX

10. Decrypt the following message that was encrypted using the ADFGVX square

| | A | D | F | G | V | X |
|---|---------|---|---|---|---|---|
| A | a | i | 2 | o | 0 | d |
| D | 1 (one) | b | h | 6 | m | s |
| F | t | n | w | c | q | 4 |
| G | l (el) | g | 7 | v | y | r |
| V | f | 5 | e | 3 | x | z |
| X | 9 | p | j | k | 8 | u |

and the keyword *Kentucky*.

AGVXF GXGAX XDFFD XXXGD FAGAF DAXGA AFGDV DGDVV

Stream cipher

11. Convert the plaintext message

November 16, 2007

to ASCII (use capital letters, spaces, punctuation, and numbers) and encrypt it using as much of the random keystream

```
10111 11010 01010 01001 01110 00100 11000 00001
10110 11111 10000 00110 01001 01000 11011 11100
00011 00001 01101 10101 10000 01010 00010 10111
11101 11010 00111 11011 10010 00000 01001 10001
01000 01001 11101 10101 11100 01101 11000 01101
```

as is necessary.

XOR table

12. The World War II codebreakers at Bletchley Park attacked a German teletype encryption machine, which the Germans called Lorenz and the British called Tunny. Tunny used a stream cipher to encrypt messages in the Baudot (5-bit) code. For their work, the codebreakers prepared an “addition table” – really an XOR table – for the Baudot characters.

For example,

$$\begin{array}{r} \text{M} \quad 00111 \\ \text{T} \quad 00001 \\ \hline \text{N} \quad 00110 \end{array}$$

Construct “row L” of that table; i.e., XOR L with A, B, ..., Z, and determine the letter, character, or command that corresponds to the 5-bit string that results.

$$\begin{array}{c|cccc} \text{XOR} & \text{A} & \text{B} & \dots & \text{Z} \\ \hline \text{L} & & & & \end{array}$$

5-bit Baudot code for letters

A = 11000 B = 10011 C = 01110 D = 10010 E = 10000
F = 10110 G = 01011 H = 00101 I = 01100 J = 11010
K = 11110 L = 01001 M = 00111 N = 00110 O = 00011
P = 01101 Q = 11101 R = 01010 S = 10100 T = 00001
U = 11100 V = 01111 W = 11001 X = 10111 Y = 10101
Z = 10001

ASCII codes for selected characters

| Binary | Character | Binary | Character |
|-----------|-----------|-----------|-----------|
| 0010 0000 | Blank | 0101 0100 | T |
| 0010 0001 | ! | 0101 0101 | U |
| 0010 0111 | ` | 0101 0110 | V |
| 0010 1100 | , | 0101 0111 | W |
| 0010 1110 | . | 0101 1000 | X |
| 0011 0000 | 0 | 0101 1001 | Y |
| 0011 0001 | 1 | 0101 1010 | Z |
| 0011 0010 | 2 | 0110 0001 | a |
| 0011 0011 | 3 | 0110 0010 | b |
| 0011 0100 | 4 | 0110 0011 | c |
| 0011 0101 | 5 | 0110 0100 | d |
| 0011 0110 | 6 | 0110 0101 | e |
| 0011 0111 | 7 | 0110 0110 | f |
| 0011 1000 | 8 | 0110 0111 | g |
| 0011 1001 | 9 | 0110 1000 | h |
| 0100 0001 | A | 0110 1001 | i |
| 0100 0010 | B | 0110 1010 | j |
| 0100 0011 | C | 0110 1011 | k |
| 0100 0100 | D | 0110 1100 | l |
| 0100 0101 | E | 0110 1101 | m |
| 0100 0110 | F | 0110 1110 | n |
| 0100 0111 | G | 0110 1111 | o |
| 0100 1000 | H | 0111 0000 | p |
| 0100 1001 | I | 0111 0001 | q |
| 0100 1010 | J | 0111 0010 | r |
| 0100 1011 | K | 0111 0011 | s |
| 0100 1100 | L | 0111 0100 | t |
| 0100 1101 | M | 0111 0101 | u |
| 0100 1110 | N | 0111 0110 | v |
| 0100 1111 | O | 0111 0111 | w |
| 0101 0000 | P | 0111 1000 | x |
| 0101 0001 | Q | 0111 1001 | y |
| 0101 0010 | R | 0111 1010 | z |
| 0101 0011 | S | 0011 1111 | ? |