Math 1350 – Prelim I

Monday, February 23, 2009

Name: .....

Instructor: Achilleas Sinefakopoulos

INSTRUCTIONS – READ THIS NOW

- This test has **6** problems worth a total of **50** points.
- Please write your name right now.
- ***Show your work.*** **Unless otherwise specified, no credit will be given for unsupported answers, even if your final answer is correct.** To receive full credit, you must show your reasoning and the steps which led you to your your final answer, and these must be neatly written. If you need more space, write on the back side of the preceding sheet, but be sure to label your work clearly.
- This is a closed book exam. You are allowed to use a calculator, but no other electronic device or aid (notes, handouts, book e.t.c.) is allowed.
- The exam is **50 minutes** long. **Good luck!**

Academic integrity is expected of all students of Cornell University at all times, whether in the presence or absence of members of the faculty. Understanding this, I declare I shall not give, use, or receive unauthorized aid in this examination.

Signature of the student: .....

OFFICIAL USE ONLY:

Problem ♯	1.	2.	3.	4.	5.	6.	TOTAL
Points earned							

1. (5 pts) Decrypt the following message, which was enciphered using the Atbash cipher.

   DVOO YVTFM RH SZOU WLMV

2. (7 pts) A ciphertext was enciphered using an affine cipher. Given that the ciphertext letters I and J correspond to the plaintext letters T and I, respectively, find the encipherment formula.

3. (8 pts) A simple columnar transposition was used to produce the ciphertext

`OGASE NSENV GURTT AELSG IUREE WKSII INP`

Decipher the message. Show your work.

4. Consider the following Vigenère-encipherered text:

```
ICFXF PCCXM FZTHL TKGHH LXHST GXBFL
LVIMY CGHML EMQZI KZLIV IFZLS HSLLD
USVMY CHZMG XQPBH TIPDK WHWMJ HVTXC
DIWYF PIIRX FPICX TBCPF QLREP WRLKY
HSEHW RGCYU CCHOR WSWDD THJGC UIGUR
WSQ
```

(a) (4 pts) Use the Kasiski test to determine the most likely length(s) for the keyword. (**Hint**: The trigraphs `XFP`, `MYC` and `FPI` appear twice in the above ciphertext. Their occurrences are underlined.)

(b) (6 pts) Determine the keyword given that the end of the plaintext reads: "...END THEM."

5. (10 points) Decrypt the following English sentence, which was encrypted using a shift cipher.

   `BPMUW ABKMZ BIQVE IGBWA CKKMM LQAIT EIGAB WBZGR CABWV MUWZM BQUM`

   Show your work.
   Hint: The most frequent ciphertext letters are `B` and `M`, which appear eight (8) and seven (7) times, respectively.

6. (10 pts) The following text was encrypted using a keyword to obtain a mixed alphabet.

   JGFUU VUPYR BCKAG QQCJM HUGQM LQQCE HUETR KLRQC JMHUP

   The beginning segment of the plaintext reads: "MAKE EVERYTHING ...". Decrypt the message and recover the keyword. Explain your method.

The numerical Equivalents of the letters of the English alphabet are

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Inverses modulo 26

a	1	3	5	7	9	11	15	17	19	21	23	25
a^{-1} MOD 26	1	9	21	15	3	19	7	23	11	5	17	25