Math 135 (Summer 2006)
Review for Prelim #2

Chapter 2 and 3 Topics

- Understand the Vigenère square cryptosystem, and its relationship to a simple shift cipher. Be able to encipher/decipher messages with this system, and perform a simple cryptanalysis.
- Know the basic probability and counting techniques (including combinations and permutations).
- Understand Friedman's index of coincidence. Be able to calculate I and the estimated keyword length k.
- Understand Kasiski's test for estimated keyword length.
- Be able to perform basic matrix arithmetic: addition, multiplication, determinant, inverse.
- Understand the Hill cipher.
- Understand number representation, especially binary (base two) and base twenty-six
- Be able to encipher and decipher messages using a "binary one-time pad."
- Be able to generate a bit stream from a linear feedback shift register.

Selected Review Problems

1. Use the Vigenère cipher to **(a)** encipher `GEOMETRY` using the keyword `ANGLE`, and **(b)** decipher `WUXAYERTH` using the keyword `PUMPKIN`.

2. Suppose that a sack contains 13 A's, 45 B's, 34 C's, 8 D's, and 19 E's.

(a) A single letter is selected from the sack. What is the probability that the letter is either an A or a D? Explain.

(b) A single letter is selected from the sack. What is the probability that the letter is not an E? Explain.

(c) A pair of letters is selected from the sack. What is the probability that the letters are identical? (Be sure you can express your answer in terms of combinations/permutations.)

3.

(a) In how many ways can a basketball team of 5 players be selected from among 28 recruits? (Ignore positions.)

(b) In how many ways can a basketball team consisting of 2 guards, 2 forwards, and 1 centre be selected from among 28 recruits?

4. How many different strings of length at most 5 are there if

(a) the characters `A, B, ..., Z` are used?

(b) the characters `A, B, ..., Z` and the digits `0, 1, ..., 9` are used?

5. A polyalphabetic substitution produced a ciphertext with 844 letters and the following letter counts:

A	B	C	D	E	F	G	H	I	J	K	L	M
28	32	46	19	20	31	47	13	33	32	56	35	52
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
22	23	32	33	50	25	44	19	49	22	23	30	28

Calculate the index of coincidence and use the Friedman test to determine a likely keyword length.

6. Shown below is a Vigenère ciphertext, and some repeated letter groups are marked. Use the Kasiski test to determine a likely keyword length.

TIGOE YKAOP RYSIE NGQXT LTFTJ SQJEO SXIXZ ESVKE
YYHFY LPQTO UDHVJ ZUSPL RLZOU JHHJV ASVJS QJEOF
WLJAN GKOPJ JSFER RIIOI KJLXV ISKWR HKPPU LXNUN
TVLPQ REIKJ LXVIS KWYYG FVNOG TSPMG PISZO GNRRL
ZESOI EHALU ALRYN EDQPM SM

7. Let $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ be a Hill cipher key matrix. Decipher the message XAHZ using this key.

8.

(a) Find the base ten representation of the number with base two representation 101001000.

(b) Find the base two representation of 83 (base ten).

(c) Find the base ten representation of the number with base twenty-six representation ZAP.

(d) Write the base twenty-six representations for the five numbers following the number with base twenty-six representation NIGHT.

(e) How many digits are in the base two representation of the number 25^{3829}?

(f) Find the base ten representation of the number with base eight representation 76341.

9. Section 3.4, page 219, #2, #3