Math 4450/6450 Cryptography Homework #2 -- 1/15/2010

1) Please evaluate the security of the following scenario:

Billy and Zhang have decided that they would like to send secret messages to each other in their 3rd grade class. Billy heard about the shift cipher at lunch from someone who heard that a nerdy kid in the 4th grade used it once, and decided to use this as the basis of his cryptosystem. When Billy told Zhang about this idea, Zhang was concerned that too many people at school may have heard about the shift cipher, so maybe it would be figured out. To make Zhang feel better, Billy decides to use the shift cipher 5 times, and then write out the message upside-down and in reverse order. Zhang still wasn't sure, so Billy asked his older sister how many five letter "words" one can make if they don't need to say anything (i.e. they're not english, just random), and she told him that if he chooses five letters at random, that there were over 11 million of ways of doing it. Billy was impressed with his system, and Zhang felt much better finally knowing that their messages would be safe.

2) Which of the following sets and operations are groups? Please explain why or why not, and say how close to being a group each one is.

a) The positive integers under addition

b) Z under addition

c) The permutations of the letters {A, L, X, Z} under composition

d) Z/10Z under addition

e) Z/10Z under multiplication

f) Z/11Z under multiplication

g) Functions of the form $f(x) = ax+b$ where a and b are real numbers, under composition.

3) How many valid keys are there for the affine cipher in the Phoenician alphabet, which only has 22 letters?

4) Suppose an author has written a book "Real Cryptography for Dummies -- what they don't usually tell you!", and would like to use the Vigenere cipher to keep is secure until it is published in one year. How long should one make the key so that it can resist a brute force attack by the rival publisher, whom the author believes has recently purchased a bank of 1000 standard desktop computers for exactly this purpose?

Math 4450/6450 Cryptography Homework #2 -- 1/15/2010

5) Please (attempt to) decrypt the following Vigenere ciphertext:

```
K M P X L   L M K I V   W M K X J   R X P W E   T V I G L
I T Z R Z   S K Q C H   X F E I V   S Y U V A   G X H Y V
C G L R Z   I S L S M   W W Q E I   V J C R K   S Z J E R
Y I K S W   U R C B F   K K K M L   F S Y G S   L K M D C
I M G Q C   B I V A T   J V V L A   R O F H X   J R E I C
I L S I I   E I Z C V   Y E M S V   G I I T D   P A I I T
D P A F Y   M G J T V   E V Z S H   R P E C R   Q N R Y G
V O J S Y   U V A G X   T F E N P   W B K E P   U M M Z M
P B M M K   K Q Z R Z   L S U K E   R L L C K   A T Q X J
Z W O A I   Y N V B L   I U J M G   Y L K J W   N H T Q I
X X V F A   F R X G J   V Y I G K   E U U I I   M X A U M
K W G V F   V L O L Q   K S E V L   K D M Y S   P N K L X
H I T J S   G S P E F   Q I M X G   I W B F X   J V A H J
P F R T I   J S Z Z Q   T L I N P   X P G L W   E H K W H
U Z B M Q   Q K C P B   G R E F Q   I M X G I   W P W V G
K S U W T   W K X H O   S T B S G   S W K E K   E W T I G
I G U V A   G X X V Q   G J W T Y   I K K A H   M P F K E
D W S P R   Z X J E I   V E G W W   V Z Q T L   I F K A X
D Z G D M   E D M Q E   X B E I U   K L X S K   G F J M Z
I W E M O   W V U V X   H T V G R   O T K M P   X P X E I
U J E Z W   W K D S G   K M P X L   M Z I E F   H X T S Q
```

B