1. Suppose you have a magic box which has an input slot and an output slot. The box works as follows: If you write a prime number P, a base B, and an integer R on a strip of paper, feed the strip into the input slot, and wait one second, the machine will return a different strip through the output slot with a number X. This number X solves

$$B^X \equiv R \bmod P.$$

If no such X exists, then the machine returns a short blank paper strip.

You eavesdrop on two people, Gene and Hilary, using Diffie-Helman Key Exchange, with

$$P = 53,\ B = 3.$$

You overhear the public part of the exchange:

$$3^G \equiv 31 \bmod 53, \quad 3^H \equiv 21 \bmod 53.$$

Using the magic box, you discover $G = 5,\ H = 11.$, that is,

$$3^5 \equiv 31 \bmod 53, \quad 3^{11} \equiv 21 \bmod 53.$$

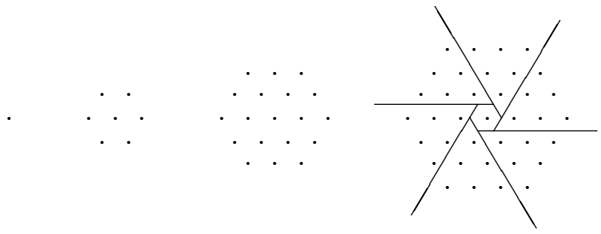
---

a. (10 pt) Compute the shared secret (also called the agreed key). Explain what you are calculating and the method you use.

b. (20 pt) Explain why Diffie-Helman Key Exchange seems to be secure, in real life, and why this magic box compromises the security of this cryptosystem.

Note. The numbers are different from the practice problem.

2. Let $H(n)$ be the number of dots in a hexagonal grid with n dots on a side. Shown below are the grids with 1, 2, 3, and 4 dots on a side.



---

a. (10 pt) Compute the differences $H(3)-H(2)$, $H(4)-H(3)$, and $H(5)-H(4)$.

b. (20 pt) Use an induction argument to show that for natural numbers n,

$$H(n) = 3n(n-1) + 1.$$

(The lines drawn on the last hex grid suggest a way to cut the hexagon into more manageable triangle pieces.)

3. The World War I era ADFGVX cipher is a two step method. The first step is a substitution using two letters among ADFGVX to stand for each plaintext letter or digit. The second step is a keyword columnar transposition. Below the key word, the result of the first step is written out, using one column for each letter of the key word. The result is copied in columns, in alphabetical order of the letters of the key word.

Here is the substitution table:

	A	D	F	G	V	X
A	F	L	1	A	O	2
D	J	D	W	3	G	U
F	C	I	Y	B	4	P
G	R	5	Q	8	V	E
V	6	K	7	Z	M	X
X	S	N	H	Ø	T	9

Each letter or digits is substituted with the pair using first the letter at the left end of the row and second the letter at the top of the column. So L enciphers as AD.

---

a. (10 pt) Encipher THE using the substitution table.

b. (20 pt) The following message was enciphered first by applying the ADFGVX substitution and second, using keyword columnar transposition with the key word **P A R I S**:

DAVFAADX VXFGVXVX FFXXXVFX XGXGXAVA DAGXAVGG

What is the first word of the message?

Hint: the word THE appears in the message, but not as the first word.

Note. The word and message are different from the practice problem.

4. Farmer Magog comes home from the Neolithic Revolution. Magog has learned about the latest inventions: planting crops, and also writing numbers in base ten (using fashionable Arabic numerals).

---

a. (5 pt) Farmer Magog has a square field measuring 200 cubits on a side. If Farmer Magog harvests $\frac{1}{50}$ bushels of grain per square cubit, to the nearest whole bushel, how much does Magog harvest?

b. (5 pt) Farmer Magog scratches this number in base ten on a stone tablet, taking 1 minute per digit. How long does it take Farmer Magog to record the harvest?

Magog is prosperous, and periodically acquires larger lands. Suppose Magog has a square field measuring C cubits on a side. Crop yield is the same $\frac{1}{50}$ bushels per square cubit.

---

c. (10 pt) Let $h(C)$ be the amount of Magog's harvest, in bushels. Which complexity class, from the list below, is the smallest containing $h(C)$, and which word best describes this class?

d. (10 pt) Magog still records the harvest on a stone tablet. It takes time $r(C)$ to write the number in base ten. Which complexity class, from the list below, is the smallest containing $r(C)$, and which word best describes this class?

Complexity classes:

I. $O(C^K)$, $K > 0$ for example: $O(C^1)$, $O(C^2)$, $O(C^{10})$,
II. $O(K^C)$, $K > 1$ for example: $O(2^C), O(e^C), O(10^C)$,
III. $O(\log C)$,
IV. $O(1)$.

In cases I and II, K is a some constant independent of C.

Descriptions: constant, exponential, logarithmic, polynomial.

Note. Farmer Magog starts with a different size field from the practice problem.

5. A eight bit linear feedback shift register generates a key for a binary stream cipher. If the register has contents | b_7 | b_6 | b_5 | b_4 | b_3 | b_2 | b_1 | b_0 |
at one step, then at the next step,
it shifts to | $b_5 + b_2 + b_0$ | b_7 | b_6 | b_5 | b_4 | b_3 | b_2 | b_1 |.
The new leftmost bit is the output of the machine.

---

a. (6 pt) Start with the register fill | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | Compute the first eight bits $z_1, z_2, z_3, z_4, z_5, z_6, z_7, z_8$ of the key stream by running the shift register eight steps. (The starting fill does not produce an output bit.)

b. (6 pt) Encipher the short plaintext 10011011 by computing

$$10011011 \oplus z_1 z_2 z_3 z_4 z_5 z_6 z_7 z_8.$$

The $\oplus$ is the usual bitwise exclusive or.

c. (6 pt) Convert the result of part (b) to hexadecimal.

Suppose you have this shift register box, and you receive a long string of bits enciphered by the method above, possibly with a different key stream.

d. (12 pt) What information do you need to determine the key stream, and how do you decipher the message? More specifically: which bits and how many bits do you require to determine the entire key stream, and how do you decipher the message?

Note. The particular strings of bits are different from the practice problem.

6. Imagine working for the cryptographic corps of your favorite country in the days before digital computers.

Fact 1. You use a mechanical polyalphabetic substitution cipher (maybe like an Enigma machine).

Fact 2. The machine takes a four letter key, reset at the beginning of each message.

Fact 3. Half of the messages you encipher begin "To the ministry of...."

Fact 4. Your superiors will not change their writing style.

Fact 5. Your superiors will not replace the cryptographic hardware.

---

a. (15 pt) Assume the adversary has a copy of your machine, but has not stolen your keys. Explain why Fact 3 helps your adversary decipher a lot of whole messages.

b. (15 pt) You learn Fact 4 and Fact 5 after complaining to the higher-ups. You can work within the crypto corps to improve the cryptographic protocol. What would you change about your cryptographic practice to make your system more secure?

7 **a.** (15 pt) Suppose the text of each day's New York Times is a sample of standard English prose, and each day is enciphered using a daily monoalphabetic substitution. Let p be the probability that two letters circled at random in one day's ciphertext will match. The value of p is computed each day. Only letters count, and anything which is not a letter is ignored.

Which of the following is true, and why?

I. The value of p will be near $\frac{1}{26}$. The exact value will vary above and below $\frac{1}{26}$, but overall will be approximately $\frac{1}{26}$.

II. The value of p will be always be less than $\frac{1}{26}$. The exact value will typically be near a definite value less than $\frac{1}{26}$.

III. The value of p will never be less than $\frac{1}{26}$. The exact value will typically be near a definite value more than $\frac{1}{26}$.

IV. There is not enough information to tell how p compares with $\frac{1}{26}$.

b. (15 pt) A Vigenère encryption using a keyword produced the ciphertext below.

```
ICJEVAQIPW BCIJRQFVIF AZCPQYMJAH NGFYDHWEQR NARELKBRYG PCSPKWBUPG  60
KBKZWDSZXS AFZLOIWETV PSITQISOTF KKVTQPSEOW KPVRLJIECH OHITFPSUDX 120
XARCLJSNLU BOIPRJHYPI EFJERBTVMU QOIJZAGYLO HSEOHWJFCL JGGTWACWEK 180
EGKZNASGEK AIETWARJED PSJYHQHILO EBKSHAJVYW KTKSLOBFEV QQTPHZWERZ 240
AARVHISOTF KOGCRLCJLO KTRYDHZZLQ YSFYWDSWZO HCNTQCPRDL OARVHSOIER 300
CSKSHNARVH LSRNHPCXPW DSILPLZVQL JOENLWZJFS LCIEDJRRYX JRVCVPOEOL 360
JUFYRQFGLU PHYLWISOTF KWJERNSTZQ MIVCWDSCZV PHVCUEHFCB EBKPAWGEPZ 420
ISOTFKOEOD NWQZQWHYPV AHKWHISEEG AHRTOEGCPI PHFJRQ
```

The cryptanalyst received the ciphertext as a string of capital letters, and transcribed it in lines of sixty letters, numbered on the right edge, and put the letters in blocks of ten. The cryptanalyst underlined some short repeated sequences.

Determine the length of the keyword.

THE BONUS.
Recall Euler's function $\phi(N)$ is the number of positive integers less than N which are relatively prime to N.

A Carmichael number is a positive integer N which is not prime and has the property that for any integer a relatively prime to N, $\quad a^{N-1} \equiv 1 \bmod N$.

---

a. (3 pt) The prime factorization of 561 is $3 \times 11 \times 17$. Compute $\phi(561)$.

b. (12 pt) The number 561 is a Carmichael number, meaning that 561 is not prime, and for any integer a relatively prime to 561, the congruence

$$a^{560} \equiv 1 \bmod 561$$

holds. (Notice that $560 = 561 - 1$.)

Justify that 561 is a Carmichael number.

No more questions! Just some fun.

(attributed to Mark Twain)
A Plan for the Improvement of English Spelling

For example, in Year 1 that useless letter "c" would be dropped to be replased either by "k" or "s", and likewise "x" would no longer be part of the alphabet. The only kase in which "c" would be retained would be the "ch" formation, which will be dealt with later. Year 2 might reform "w" spelling, so that "which" and "one" would take the same konsonant, wile Year 3 might well abolish "y" replasing it with "i" and Iear 4 might fiks the "g/j" anomali wonse and for all.

Jenerally, then, the improvement would kontinue iear bai iear with Iear 5 doing awai with useless double konsonants, and Iears 6-12 or so modifaiing vowlz and the rimeining voist and unvoist konsonants. Bai Iear 15 or sou, it wud fainali bi posibl tu meik ius ov thi ridandant letez "c", "y" and "x" – bai now jast a memori in the maindz ov ould doderez – tu riplais "ch", "sh", and "th" rispektivli.

Fainali, xen, aafte sam 20 iers ov orxogrefkl riform, wi wud hev a lojikl, kohirnt speling in ius xrewawt xe Ingliy-spiking werld.

Math 135 Final
May 18, 2004

Instructions. Answer all the questions in the bluebooks provided. Write your name on every bluebook you turn in.

Explain your reasoning on all questions. Brief remarks in plain English will usually suffice.

There are seven questions plus a bonus question. The seven have equal weight, and the bonus is worth half as much. Six of the questions are from the practice set, with details such as the specific numbers altered.

The questions all have straight forward solutions.
There are no trick questions.

No aids permitted: closed calculators, books, notes, etc. Turn off cell phones. Please set all your belongings to the side of the room.

Please pick up your term papers when you turn in your exam. Final grades will be posted on the course web site by the code letter below.

Name: _____ Code Letter: