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

$$P = 47,\ B = 3.$$

You overhear the public part of the exchange:

$$3^G \equiv 8 \bmod 47, \quad 3^H \equiv 18 \bmod 47.$$

Using the magic box, you discover

$$3^5 \equiv 8 \bmod 47, \quad 3^{19} \equiv 18 \bmod 47,$$

that is,

$$G = 5,\ H = 19.$$

a. Compute the shared secret. Explain what you are calculating and the method you use.

b. 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. On the exam, the particular P, B, G, and H may be different, but they will be of a similar size to the ones here.

2. Suppose you have a magic box which has an input slot and an output slot. The box works as follows: if you write a natural number N 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 list of numbers. These numbers will be all the solutions X between 1 and $N-1$ to the equation

$$X^2 \equiv 1 \bmod N.$$

For example, if you give the machine the number 779, the reply is

$$1, 286, 493, 778,$$

because

$$1^2 \equiv 1,\ 286^2 \equiv 1,\ 493^2 \equiv 1,\ 778^2 \equiv 1 \bmod 779,$$

and those are all the solutions to $X^2 \equiv 1 \bmod 779$ for X between 1 and 778.

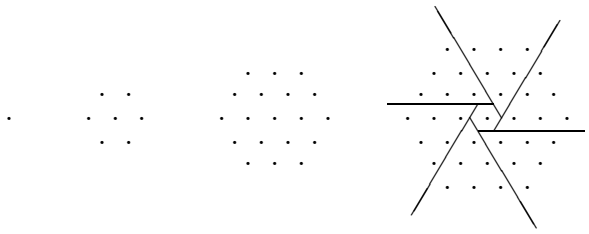
a. Given N which is the product of two distinct prime factors, explain how to use the box to find these factors.

b. Demonstrate the method you propose to factor $N = 779$. Do not simply write the factors. Show how you get them from the information given.

c. Explain whether this magic box impacts the security of the RSA cryptosystem.

Note. On the exam, the particular N, and, of course, the resulting solutions to $X^2 \equiv 1 \bmod N$ may be different, but they will be of a similar size to the ones here.

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



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

b. 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.)

4. Communication over a certain channel requires a message to be in a special form: a message is a string of binary bits, always beginning with the bit 1, and has no consecutive 1 bits. (This was true for some real hardware which could not distinguish between two 1's in a row and a single 1 stretched out by inaccurate system timing.)

There is one valid message of length one: 1.
There is one valid message of length two: 10.
The message 010101 is invalid; it begins with 0.
The message 101101 is invalid; it has two consecutive 1 bits.
The message 101010 is valid.

a. Write out all the valid three bit, four bit, and five bit messages. How many are there of each?

b. Let $V(x)$ be the number of valid messages which are x bits long. So $V(1) = 1$, $V(2) = 1$, and you computed $V(3)$, $V(4)$, and $V(5)$ above. Use an induction argument to show for natural numbers $x > 2$,

$$V(x) = V(x-1) + V(x-2).$$

5. Described below is a two phase cipher. First, there is a substitution. Second, there is a transposition.

This substitution cipher uses multiple symbols for certain letters. The letters Q and X are deleted from the plaintext alphabet, so that there can be two possible substitutions for E and T. The enciphering cryptoclerk uses the lowercase e and t to indicate that the alternative substitution is to be used. The deciphering cryptoclerk does not care. If Q or X appears in the plaintext, the letters K, KW, KS, or Z are used phonetically.

Here is the substitution:

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

a. Encipher "THeAtER" using the substitution above, and the alternative substitutions where indicated.

b. The second phase of this cipher system is a transposition. The result of the substitution cipher is written in five rows of equal length and copied in columns. You receive the following message:

```
TPWPQ GUJAK ANAGA NGCMK KMCET WHYVM RUUDG MPNGN LYVWF
```

What is the first word in the plaintext?

Hint: the word THEATER appears in the message, using the same choices for alternative substitutions as the first part, but not as the first word.

Note. On the exam, the particular word in the first part and message in the second part might be different.

6. 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. Encipher AND using the substitution table.

b. The following message was enciphered first by applying the ADFGVX substitution and second, using keyword columnar transposition with the key word **M O R I A**:

GDFDXXGG XVAXGGVX XXADDDXX AAAGDDDG FGGXADXA

What is the first word of the message?

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

Note. On the exam, the particular word in the first part and message and key word in the second part might be different.

7. State lottery "quick pick" games often draw one ball from each of four separate wells, each one containing balls numbered 0 to 9. In this way, they randomly select a four digit winning combination.

The lottery makes a TV broadcast of the lottery draw. The program has a 30 second introduction and a 10 second wrap-up, and it takes 10 seconds to draw each ball. (They have to build the drama somehow.)

a. What is the length of the lottery broadcast for four digit quick pick?

b. At \$1 per ticket, how much will it cost to guarantee a win by buying every possible four digit quick pick ticket?

c. The state revamps the lottery periodically so that the draw produces a D digit winning combination. Let $s(D)$ be the time for the new format lottery TV broadcast.

Which complexity class, from the list below, is the smallest containing $s(D)$, and which word best describes this class?

d. Suppose in the D digit lottery game, you try to guarantee a win by buying every possible ticket at \$1 apiece. Let $t(D)$ be the total cost of the tickets.

Which complexity class, from the list below, is the smallest containing $t(D)$, and which word best describes this class?

Complexity classes:

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

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

Descriptions: constant, exponential, logarithmic, polynomial.

Note. On the exam, the lottery might start with a different number of digits.

8. 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. Farmer Magog has a square field measuring 100 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. 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. 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. 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. On the exam, Farmer Magog might start with a different size field and have a different yield per square cubit.

9. A Feistel function is used to build an electronic encryption device. The function uses a four bit key to transform an eight bit string into another eight bit string as follows.

$$f_{k_0k_1k_2k_3}(a_0a_1a_2a_3a_4a_5a_6a_7) = a_4a_5a_6a_7b_0b_1b_2b_3, \tag{1}$$

where

$$b_0b_1b_2b_3 = k_0k_1k_2k_3 \oplus a_3a_2a_0a_1. \tag{2}$$

The symbol $\oplus$ is the usual bitwise exclusive or.
Notice that in equation (2), the a_i bits are not in numerical order.

a. Compute $f_{1001}(f_{1001}(10110110))$.

b. Convert the result of part (a) to hexadecimal.

c. Determine the inverse function $g_{k_0k_1k_2k_3}$, that is, a function g such that

$$g_{k_0k_1k_2k_3k_4}(f_{k_0k_1k_2k_3k_4}(a_0a_1a_2a_3a_4a_5a_6a_7)) = a_0a_1a_2a_3a_4a_5a_6a_7$$

for any four bit key and eight bit message.

d. Compute $g_{1001}(g_{1001}(11001100))$.

Note. On the exam, the choice of key and eight bit strings might be different.

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

a. Start with the register fill $\boxed{1 \mid 1 \mid 0 \mid 0 \mid 1 \mid 1 \mid 0 \mid 0}$ 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. Encipher the short plaintext 00111001 by computing

$$00111001 \oplus z_1 z_2 z_3 z_4 z_5 z_6 z_7 z_8.$$

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

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

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

d. What information do you need to determine the key stream, and how do you decipher the message?

Note. On the exam, the particular register fill and plaintext might be different.

11. 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 three to six 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. 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.

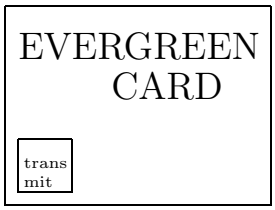
b. You learn Fact 4 and Fact 5 after complaining to the higher-ups. You can work within the crypto corps to improve the cryptographic protocol. What would you change about your cryptographic practice to make your system more secure?

12. Imagine it's a few months in the future. Your credit card has made the jump to wireless! Instead of swiping, now your card transmits its number to the merchant's "cash" register.

Your credit card company decides to use the RSA public key cryptosystem in its continuing fight against fraud. Here's their plan.

Your card will now encipher your credit number using the RSA method, with the modulus and exponent provided by your credit card company. Theoretically, you could find these things out, but actually a tiny computer inside the card does the computation. It's that RSA enciphered result which your card transmits.

When you want to make a purchase, you put your card near the merchant's cash register, and put your thumb on the "transmit" button. The merchant records the enciphered number, and presents the cipher to the credit card company. The credit card company deciphers the number, and voila! Your transaction is approved.



a. Describe a passive attack on this system. (Passive means that you don't perceive the attack in progress – muggers are not passive.) Identify where the adversary is relative your communication, and what the adversary does to poach from your account.

b. Assume that the credit card company is committed to using RSA encryption. How would you change the cryptographic protocol to defend against this attack? (Be reasonable: we're only looking a few months in the future; credit card sized computers and wireless communication exist now. Upgrades to the computer's software are possible. Transporter beams and time machines are not.)