12) Let $p = 2^{16} + 1 = 65537$, which is prime. We want to determine $\mathrm{OrderMod}_p(13)$.
a) What are the possible values for $\mathrm{OrderMod}_p(13)$?
b) Show that if $13^e \equiv 1 \pmod{p}$ then $\mathrm{OrderMod}_p(13)$ must divide e.
c) Testing possible orders in an efficient way (i.e. trying to do few tests), determine $\mathrm{OrderMod}_p(13)$.

13) a) Let p be a prime and $g\mathbb{Z}$. Show that if g is *not* a primitive root modulo p, then $\mathrm{OrderMod}_p(g)$ is a proper divisor (i.e. it divides but is not equal) of $p-1$.
b) Show that if g is *not* a primitive root modulo p, then there exists a prime q dividing $p-1$ such that $g^{\frac{p-1}{q}} \equiv 1 \pmod{p}$. (**Hint:** Let q be a prime divisor of $\frac{p-1}{\mathrm{OrderMod}_p(g)}$)
c) Let $p = 1009$ (which you may assume to be a prime without proof). Then $p - 1 = 2^4 3^2 7$. Calculate $11^{\frac{p-1}{2}} \bmod p$, $11^{\frac{p-1}{3}} \bmod p$, $11^{\frac{p-1}{7}} \bmod p$. Conclude that 11 is a primitive root modulo p.

14) Assume you have an encryption system with a key space of 2^{50} keys. Also assume that you have a computer that can test 10^{10} possible keys per second. (A very naive guess on a powerful computer today you could still afford as a private person.) How long would it take to test half the possible keys (i.e. an average brute-force key search)? Assuming (again a rough guess based on historical data) that in six years you could buy a computer that is 10 times as powerful, by what year would a brute-force attack succeed in an hour (or less)?

15) a) Assuming that the alphabet has 26 letters, how many sequences of length 4 can be composed from upper-case and lower-case letters and digits?
b) Determine the number of sequences of length 4 that contain (at least) one upper-case letter, one lower-case letter and one digit. What percentage of all passwords is this?
c) A policy is suggested that all (4-letter, to keep the problem small) passwords must contain at least an upper-case letter, a lower-case letter and one digit. Give your professional opinion on whether this will improve security.

16) The setup of this problem is as in problem 11. Again there is a set of encrypted text snippets on the course homepage (link under homework 3 or `http://www.math.colostate.edu/~hulpke/lectures/m360/prob16.html`).
However now we encrypted the text with an *arbitrary* permutation of the 26 letters. Using letter and bigram frequency, decrypt the text snippet assigned to you via the CSUID mod 169.

Practice Problems: (These problems from the book are not to be handed in, but might be useful in reviewing and in exam preparation): **4.2**, **4.3**, **4.4**, **4.10**, **4.11**,

> **Mafia Boss's Encrypted Messages Deciphered**
> *Rosella Lorenzi, Discovery News* April 17, 2006
>
> The recently arrested *boss of bosses* of the Sicilian Mafia, Bernardo Provenzano, wrote notes using an encryption scheme similar to the one used by Julius Caesar more than 2,000 years ago, according to a biography of Italy's most wanted man.
> [...]
> The letter, written in January 2001 by Angelo Provenzano to his father, was found with other documents when one of Provenzano's men, Nicola La Barbera, was arrested "I met 512151522 191212154 and we agreed that we will see each other after the holidays...," said the letter, which included several other cryptograms.
> The Binnu code is nothing new: each number corresponds to a letter of the alphabet. "A" is 4, "B" is 5, "C" is 6 and soon until the letter Z, which corresponds to number 24, wrote Palazzolo and Oliva.

While the classic Caesar cipher moves everything three letters later (A becomes D, B becomes E, etc.), the *Provenzano code* assigns a number to each letter by simply increasing by 3 the value given to the 21 letters of the Italian alphabet listed in order. So, A becomes 4 (1+3), B becomes 5 (2+3), C becomes 6 (3+3), etc.

"In the Provenzano code the key is the +3 shift," mathematics expert Alessandro Martignago told Discovery News. As the code is cracked, the *512151522 191212154* person becomes *Binnu Riina.* Most likely, it refers to Bernardo Riina, arrested on Wednesday on suspicion of aiding Provenzano while he was on the run. According to Martignago, the Provenzano code might have been made more secure by changing the + 3 key with other shift characters (+5, +7, +8, etc.) from time to time.

"Looks like kindergarten cryptography to me. It will keep your kid sister out, but it won't keep the police out. But what do you expect from someone who is computer illiterate?" security guru Bruce Schneier, author of several books on cryptography, told Discovery News.

Indeed, no high-tech ran the Mafia network under Provenzano's rule. Top Mafia businesses were conducted on an obsolete Olivetti Lettera 32 typewriter. [Letters] were delivered by a chain of messengers. The fact that the boss code was rather straightforward may be explained by Provenzano's lack of education. It stopped when he dropped out of school at about eight.

[...]

Tabula Recta

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