Math 4450/6450 Cryptography Final Exam -- May 7th, 2010

1) Please carefully describe (an algorithm for) how someone could successfully use the Man-in-the-middle attack learn the shared secret of Alice and Bob, who are using the Diffie-Hellman Secret Sharing algorithm over the internet. What can Alice and Bob do to thwart such an attack?

Math 4450/6450 Cryptography Final Exam -- May 7th, 2010

2) Please carefully describe (an algorithm for) how two people can securely communicate using One-time pad cryptosystem, and discuss the security assumptions that prove its security. How vulnerable does this cryptosystem become when these assumptions are violated?

Math 4450/6450 Cryptography Final Exam -- May 7th, 2010

3) Please carefully describe (an algorithm for) the fast exponentiation algorithm used to quickly compute a^b (mod n), and use it to compute 2^35 (mod 55).

Math 4450/6450 Cryptography Final Exam -- May 7th, 2010

4) Please carefully state and prove Fermat's Theorem (which tells us about certain powers of elements in Z/pZ).

Math 4450/6450 Cryptography Final Exam -- May 7th, 2010

5) Please carefully describe an algorithm for creating an RSA public/private key pair (being sure to label each) that is secure from all (non-brute force) attacks we discussed in class.

Math 4450/6450 Cryptography Final Exam -- May 7th, 2010

6) Please use the third non-zero convergent of the continued fraction attack to break the RSA public key (n,e) = (7387, 4811) by factoring n and recovering the private key (n,d). Be sure to show all work and carefully explain your method.

Math 4450/6450 Cryptography Final Exam -- May 7th, 2010

7) Please use the Pohlig-Hellman attack to solve the Discrete Log problem $2^x = 53$ in $Z/59Z$.

Math 4450/6450 Cryptography Final Exam -- May 7th, 2010

8) Please carefully describe (the algorithm for) the Quadratic Sieve use it to factor $n = 93$.

Math 4450/6450 Cryptography Final Exam -- May 7th, 2010

9) Please compute the code rate, minimal Hamming distance and error correcting/ detecting capabilities of the binary linear code generated by the two vectors v = (1,1,1,1,0,0,0,0) and w = (1,0,1,0,1,0,1,0).

Math 4450/6450 Cryptography Final Exam -- May 7th, 2010

10) Alice and Bob have liked each other and shared a love of mathematics since they were very young, but unfortunately their families are no longer on good terms and they never are able to speak in an unsupervised setting or able to privately exchange messages. In a sad twist of fate, their class schedules have always kept them in opposite sides of the school and the only times they have to communicate is on the school bus. Due to a recent guest lecture by a wandering cryptography professor to their high-school, they learned the existence of an unbreakable cipher (one time pad), and how to securely create shared secrets in a public setting (Diffie-Hellman). In an effort to combine these, they agree on the bus that they should create two shared secrets each day on the bus for one month to make a book of 60 secret numbers, and then they will each use these numbers to send a 60 character unbreakably secure encrypted message to each other about their blossoming feelings.

Both Alice and Bob both use very sophisticated programmable calculators (issued by the high school for their math classes), and they follow all of the best practices for the Diffie Hellman key-exchange. Whenever necessary for the Diffie-Hellman algorithm, they use their calculators to choose random numbers about 100 decimal digits long.

Please describe the strengths and weaknesses of their approach (if any exist), and whether a determined attacker could eventually decrypt their messages (and if so, how).

Math 4450/6450 Cryptography Final Exam -- May 7th, 2010

11) Extra Credit: The following text was taken from an Encyclopedia Brown story, as a non-trivial example of how sometimes information can get lost in translation. It is a message from a boy to a girl (Adorabelle) for whom he has strong feelings. Please punctuate the following text in two different ways to reveal two opposite meanings!

HOW I LONG FOR A GIRL WHO UNDERSTANDS WHAT TRUE

ROMANCE IS ALL ABOUT YOU ARE SWEET AND FAITHFUL GIRLS

WHO ARE UNLIKE YOU KISS THE FIRST BOY WHO COMES ALONG

ADORABELLE I'D LIKE TO PRAISE YOUR BEAUTY FOREVER I

CAN'T STOP THINKING YOU ARE THE PRETTIEST GIRL ALIVE

HOW I LONG FOR A GIRL WHO UNDERSTANDS WHAT TRUE

ROMANCE IS ALL ABOUT YOU ARE SWEET AND FAITHFUL GIRLS

WHO ARE UNLIKE YOU KISS THE FIRST BOY WHO COMES ALONG

ADORABELLE I'D LIKE TO PRAISE YOUR BEAUTY FOREVER I

CAN'T STOP THINKING YOU ARE THE PRETTIEST GIRL ALIVE

P.S. I had a really enjoyed teaching cryptography this semester, and hope you learned a lot and had fun too! Have a wonderful and relaxing summer! =)