MATH 435 MIDTERM - APRIL 15, 2014

Nigel Boston

Write your name clearly on what you hand in. You may keep the question sheet. Answer all three questions. Partial credit will be awarded for partial answers that are correct and relevant. For full credit explanations are required. No calculators or notes are permitted. Write all answers on the sheets provided.

1. An LFSR produces the bit stream 00110010.

(a) A binary ciphertext 10101010 is produced using the above bit stream as a key stream. Find the corresponding binary plaintext.

(b) Can the LFSR have 3 cells? If yes, find the LFSR. If no, explain why not.

(c) Can the LFSR have 4 cells? If yes, find the LFSR. If no, explain why not.

2.(a) Describe the RSA cryptosystem. Be sure to indicate who does what and which things are kept secret and which made public. Don't forget to give the encryption and decryption functions.

(b) 8999999 is the product of two primes. Find them.

(c) Suppose we want to factor positive integer N. Say we find two distinct integers x and y such that $x^2 \pmod N = y^2 \pmod N$. How might we use this information to try to find a proper factor of N? Will this always be successful?

(d) A bad implementation of RSA reveals that $2^{966} \pmod{2021} = 1$. Eve computes that $2^{483} \pmod{2021} = 988$. Find a proper factor of 2021.

3. (a) Describe Diffie-Hellman key exchange. Make sure you indicate who does what and which things are kept secret and which made public. Once the key exchange is done, how do Alice and Bob encrypt messages to each other.

(b) State what the Discrete Logarithm Problem is and explain why if Eve can solve it, then she can eavesdrop on Alice's and Bob's conversation.

(c) State Fermat's Little Theorem. Suppose we know that $2^{14} \pmod p = 27$, where p is the prime 1487. Use this to find an integer x such that $2^x \pmod p = 3$.

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX