CS/ECE/MATH 435 PRACTICE MIDTERM 2, SPRING 2012

Nigel Boston

For full credit you must explain your reasoning. Answer the questions in any order.

1. (a) Describe the RSA cryptosystem. Be sure to indicate what is kept secret and what made public and explicitly give the encryption and decryption functions.
(b) Describe how the creator of the above system can also use it to sign an unencrypted message.
(c) Describe the quadratic sieve method of factoring and its application to cryptanalysis of RSA cryptosystems.

2. Show that the bit stream 011000110 cannot be generated by a 3-cell LFSR. Find a 4-cell LFSR that generates it.
(b) Find the period of this LFSR.
(c) Suppose the letters of the alphabet are converted to bit strings of length 5 by $A \to 00000, B \to 00001, C \to 00010, ..., Z \to 11001$. The ciphertext 111011111001100 has been created by using the above bit stream as the key. Decrypt it.

3. (a) Describe Diffie-Hellman key exchange using $\mathbf{Z}_p^*$. Be sure to indicate what is kept secret and what made public.
(b) In elliptic curve cryptography what is $\mathbf{Z}_p^*$ replaced by? [The answer "an elliptic curve" is not sufficient.]
(c) Suppose Alice and Bob use Diffie-Hellman key exchange with $\mathbf{Z}_{31}^*$ and base $g = 3$. Why is $g = 2$ a poor choice? Oscar intercepts 27 sent from Alice to Bob and 9 sent from Bob to Alice. If he wants to impersonate one of them to the other, what key should he now use?