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

Nigel Boston

Directions. Answer all three questions. Results from class and Bach's notes can be used without proof. Partial credit will be awarded for partial answers that are correct and relevant. For full credit explanations are required. No calculators permitted. Write all answers on the sheets provided.

1. (a) Find an LFSR (with fewer than 10 cells) that produces bit stream 0010001111010110010001

(b) What is its period and what is its characteristic polynomial?

(c) Suppose the 3rd bit is a 0 instead of a 1. Can the stream be produced by an LFSR with 6 cells?

2. (a) Give in detail the steps needed to create an instance of RSA, assuming encryption exponent 3, making sure you indicate what are the encryption and decryption functions and what is made public and what kept secret.

(b) Explain how Alice can send a signed message to Bob using RSA and how Bob verifies the signature.

(c) Consider the RSA cryptosystem where $N = 35$ and the encryption exponent is 11. Explain why $6^2 - N = 1^2$ yields the factors of N and compute the decryption exponent.

3. A Diffie-Hellman key exchange protocol is used with the modulus $p = 107$ and the element $g = 4$.

(a) What is the order of g in $\mathbf{Z}_{107}^*$?

Alice picks integer $a = 161$ and sends $g^a \pmod{p}$ to Bob. What is that?

[Note: there are short and long ways to do both parts. Hint: the order of an element of $\mathbf{Z}_p^*$ always divides $p - 1$.]

(b) Describe how an eavesdropper Eve might use the birthday attack (baby-step giant-step) to find Bob's secret integer b if she intercepts $g^b \pmod{p}$.

(c) If P and Q are distinct points on an elliptic curve E over $\mathbf{Z}_p$, define $P + Q$.

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