MATH 435 FINAL - MAY 11, 2004

Nigel Boston

Directions. You have until 9:45. Answer all four 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 that produces bit stream 00100011110101100100011
What is its period and what is its characteristic polynomial?

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

(b) Let $f(X) = X^6 + X^3 + 1$, an irreducible polynomial with entries in $\mathbf{Z}_2$. Let R be the set of all polynomials with entries in $\mathbf{Z}_2$ modulo $f(X)$. How many elements does R have? Show that $X^9 \equiv 1 \pmod{f(X)}$. What does this imply about an LFSR with characteristic polynomial $f(X)$?

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, how Bob verifies the signature, and how Alice can use a secure one-way hash function to sign a long message quickly.

(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) The Dead Poet's Society used a substitution cipher to encrypt their slogan as *X fyaa si zyaa, S bawsaea.*

Decipher the slogan, explaining your choices. The points are for your reasoning.

(b) Shown here are letter distributions for three different ciphertexts, one from a monoalphabetic substitution, one from a polyalphabetic substitution, and one from a transposition.

Determine with explanation which distribution corresponds to which cipher.

(c) What is a Feistel cipher? What is useful about it?

4. 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).]

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