MATH 435 MIDTERM - MARCH 25, 2004

Nigel Boston

Directions. You have until 9:15. 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) Representing A,B,...,Z by $\mathbf{Z}_{26} = \{0, 1, ..., 25\}$ as usual, which of the following is a legitimate cipher?
(i) $x \mapsto x^{-1} \pmod{26}$ if $x \neq 0$, $0 \mapsto 0$.
(ii) $x \mapsto 15x + 13 \pmod{26}$.
(iii) $x \mapsto x^2 \pmod{26}$.

(b) Using the Hill cipher with key $\begin{pmatrix} 1 & 3 \\ 25 & 2 \end{pmatrix}$ (all entries are mod 26), (why is this a legitimate key?) encrypt MATH. [Hint: you can shorten your calculations by simplifying the key matrix.]

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

2. (a) Explain the difference between chosen-plaintext, known-plaintext, and ciphertext-only attacks.

(b) An affine cipher produces ciphertext SBQDS. We know the plaintext starts DA. Find the plaintext.

(c) Suppose you are given a Vigenere ciphertext. Outline a good method for deciphering it (given a computer but not a Vigenere decrypter webpage!).

3. (a) A probability distribution has $p_1 = 1/2, p_2 = 1/4, p_3 = 1/8, ..., p_n = 1/2^n, ...$ Find its entropy. [Hint: to sum the infinite sum, differentiate $x/(1-x) = x + x^2 + x^3 + ...$]

(b) For the class of monoalphabetic substitution ciphers that send vowels (a, e, i, o, u, y) to vowels and consonants to consonants, calculate how many keys there are (leaving factorials in your answer)? What is the unicity distance for this class (don't simplify your answer)?

(c) If we use a cipher from (b) to encrypt a single letter, do we have perfect secrecy?