CRYPTO MIDTERM

JC

Due Wed 19 at noon. No collaboration allowed. Please note any books or papers consulted. Send me email or drop by my office if you are stuck and would like a gnomic hint.

This is the version of Wed Mar 12, which fixes a couple of issues in the original version distributed on Mon mar 10.

(1) (40 points total) Three ciphers which we have considered are:

  (a) The *anagram*: the key is a permutation σ of $\{0, \dots n-1\}$ and given a plaintext $a_0 \dots a_{n-1}$ the corresponding ciphertext is $a_{\sigma(0)} \dots a_{\sigma(n-1)}$.
  REMARK: like the one time pad, this is useless in practice because the key is about the same size as the plain text. It also has in common with the one time pad that it is essentially unbreakable by a ciphertext only attack, as long as the key is not used more than once.

  (b) The *Vigenere cipher*: the key is $b_0 \dots b_{m-1}$, and given a plaintext $a_0 \dots a_{n-1}$ the ciphertext is $c_0 \dots c_{n-1}$ where $c_i = a_i + b_{i \mod m} \mod 26$.

  (c) The *cryptogram*: the key is a permutation τ of $\{a, \dots z\}$ and given a plaintext $a_0 \dots a_{n-1}$ the corresponding ciphertext is $\tau(a_0) \dots \tau(a_{n-1})$.

Consider a "hybrid" cryptosystem in which the key is a triple (σ, K, τ) where σ is an anagram key, K is a Vigenere key and τ is a cryptogram key: a plaintext is enciphered by doing anagram encryption with key σ, then Vigenere encrypting the result of the anagram encryption with key K, finally cryptogram encrypting the result of the Vigenere encryption with key τ.

  (a) (5 points) Describe a chosen plaintext attack on this hybrid system.

  (b) (10 points) Describe a known plaintext attack on this hybrid system. You may assume (if you find that you need to) that you have several plaintext/ciphertext pairs that have been encrypted with the same key.

  (c) (15 points) Describe a known ciphertext attack on this hybrid system. In the light of the remarks on the anagram cipher that I made above, you will certainly need to assume that you have several ciphertexts that have been encrypted with the same key!

(d) (10 points) Would it have been better to compose the three ciphers in a different order?

(2) (30 points total)

You are given a fair coin (one which comes up heads with probability 1/2 and tails with probability 1/2). You perform the following experiment: toss it repeatedly till you see two tails in a row, then stop.

(a) (10 points) What is the probability that you have to toss the coin at least N times?

(b) (10 points) What is the probability that you never see a pair of tails, and so are never able to stop?

(c) (10 points) What is the expected value of the number of times that you have to toss the coin?

(3) (20 points total)

(a) (10 points) Let M and N be positive integers with $M \geq 2N-1$. How many pairs of subsets of $\{1, \ldots M\}$, each of size N, which intersect in exactly one element are there?

(b) (10 points) Let $1 \leq k \leq N$. How many pairs of N-element subsets are there intersecting in exactly k elements?

(4) (40 points total) Let p be prime. An integer a is called a *primitive root modulo p* if no two of the $p-1$ numbers $1, a, \ldots a^{p-2}$ are congruent modulo p. It can be shown that such an a always exists.

(a) (10 points) Show that a is a primitive root modulo p if and only if for every n not divisible by p there is an integer i such that $n \equiv a^i \mod p$.

(b) (10 points) Show that if a is a primitive root modulo p and i and j are integers, then $a^i \equiv a^j \mod p$ if and only if $i \equiv j \mod p-1$.

(c) (10 points) An integer m is called a *quadratic residue modulo p* if m has a "square root modulo p", that is to say there is an integer n such that $m \equiv n^2 \mod p$. Show that if p is odd then exactly $(p-1)/2$ of the $p-1$ integers $1, \ldots p-1$ are quadratic residues.

(d) (10 points) Find a primitive root modulo 17, and identify the quadratic residues among $1, 2, \ldots 16$.

(5) (20 points total) The prime number theorem predicts (roughly speaking) that there are $n/\ln(n)$ primes less than n.

   (a) (10 points) Use this to estimate the number of 50 digit primes.

   (b) (10 points) Use Maple to find out exactly how many primes there are between 10^{60} and $10^{60} + 10^5$. (You will probably need the Maple command "isprime" and the "for ... do .... end do" and "if ... then .. end if" constructions. You can get help with ?isprime, ?do, ?if)

   Is your answer consistent with the prediction of the prime number theorem?

(6) (35 points total)

   (a) (10 points) Use Maple to generate 100 random 10 digit numbers and factorise them. How much CPU time did you use?

   (You will probably need the commands, "rand", "ifactor" and "time")

   (b) (10 points) Repeat the previous part with 12 dgits, 14 digits, 16 digits etcetera. Go as far as your computer will let you.

   (c) (10 points) How long do you think it would take to factor a typical 100 digit integer using Maple?

   (d) (5 points) You probably noticed that some numbers get factored much quicker than others. What property of an integer seems to make it hard to factor?

(7) (20 points total) If f and g are two functions from $\mathbb{N}$ to $\mathbb{N}$ then we say $f < g$ if $f(n) < g(n)$ for all n. We say $f <^* g$ if there is M such that $f(n) < g(n)$ for all $n > M$.

   (a) (10 points) Prove that if f and g are polynomial functions, then $f <^* g$ if the degree of g is greater than the degree of f.

   (b) (10 points) Prove that if $f_0, f_1 \dots$ is a sequence of functions from $\mathbb{N}$ to $\mathbb{N}$ then there exists g such that $f_i <^* g$ for all i. Is there always a g with $f_i < g$ for all i?

(8) (20 points total)

   (a) (10 points) Write a register machine program to compute 2^n from n.

   (b) (10 points) How long does it take to run on argument n?