CRYPTO FINAL

JC

You may work on this final during any continuous 24-hour period of your choice during the Finals period. You should attempt **exactly six** of the following questions (attempting more is not a good strategy as I will take the sum of your six **lowest** question scores). All questions carry equal weight. You may consult any books or papers you wish, but please make a note of any works consulted. You may not collaborate but may contact me by email if you want further explanation of any question.

(1) Suppose that K is a Vigenere key of length 20 and that P is a piece of English text of length $20M$ where M is a positive integer. Let C be the result of encrypting P using Vigenere encryption with key K. Roughly how large does M need to be to allow someone who knows C to mount the "index of coincidence" known ciphertext attack and recover K and P? What is the justification for yor choice of M?

(2) Let p be prime, let E be the field $\mathbb{Z}/p\mathbb{Z}$ and let n be a positive integer. It is known that the polynomial $x^{p^n} - x$ is the product of all the irreducible polynomials in $E[x]$ with degrees dividing n. Use this fact to answer the following questions, where throughout F is the field $\mathbb{Z}/2\mathbb{Z}$.
   (a) Find all the irreducible polynomials of degrees 1, 2 and 4 in the polynomial ring $F[x]$.
   (b) Determine the number of irreducible polynomials of degrees 8 and 16 in $F[x]$.
   (c) Determine the probability that a randomly chosen polynomial of degree 16 in $F[x]$ is irreducible.

(3) Given a set X with N elements, consider an experiment in which we choose a sequence of elements $x_0, x_1, x_2 \ldots$ from X with each element having equal probability and the choices made independently. Mathematically this is modelled by saying that the probability of having chosen any particular sequence $a_0, \ldots a_{k-1}$ after k steps is N^{-k}; if $N = 2$ and $X = \{H, T\}$ this is just the familiar example of repeatedly tossing a fair coin.
   (a) Find the probability that the sequence $x_0, x_1, \ldots x_{k-1}$ does not contain a repetition.
   (b) Find the probability that x_k is the first repeated element in the sequence $x_0, \ldots x_k$, that is to say the probability that $x_0, x_1, \ldots x_{k-1}$ does not contain a repetition and $x_k = x_i$ for some $i < k$.
   (c) Write down an expression for the expected value of the least k such that x_k is a repeated element. We will call this quantity E_N. (You need not sum the series).
   (d) Plot the logarithm of E_N against the logarithm of N for some small values of N. What do you notice?
   (e) Estimate the value of $E_{2^{128}}$.

(4) Let $n > 1$ be an integer and let $p_1, \dots p_k$ be the prime divisors of n. Let a be an integer.
   (a) Show that $\gcd(a, n) = 1$ if and only if $\gcd(a, p_i) = 1$ for $1 \leq i \leq k$.
   (b) Show that if $\gcd(a, n) = 1$ and $b + n\mathbb{Z}$ is the multiplicative inverse of $a + n\mathbb{Z}$ in $\mathbb{Z}/n\mathbb{Z}$ then $b + p_i\mathbb{Z}$ is the multiplicative inverse of $a + p_i\mathbb{Z}$ in $\mathbb{Z}/p_i\mathbb{Z}$ for $1 \leq i \leq k$.
   (c) Is the converse of the preceding statement always true? If not, for which n is it true?

(5) Find the first ten integers n such that $a^{n-1} \equiv 1 \mod n$ for all a with $0 < a < n$ and $\gcd(a, n) = 1$.

(6) Consider the following variant of the Vigenere cipher. The sender and the recipient agree on two Vigenere keys K and L of the same length n. Say $K = k_1 \dots k_n$ and $L = l_1 \dots l_n$. To encrypt, the sender takes an English plaintext P and breaks it into blocks of length n say $B_1, B_2, B_3, \dots$. She then repeatedly tosses a fair coin and proceeds as follows, where $B_i = c_1^i \dots c_n^i$; if coin toss number i comes up heads then character j in block i of the ciphertext is $c_j^i + k_j \mod 26$, while if toss number i comes up tails character j in block i of the ciphertext is $c_j^i + l_j \mod 26$. Remark: if the toss comes up heads all the time this is just Vigenere with key K, while if the toss comes up tails all the time this is just Vigenere with key L.
   (a) Why is it possible for the recipient to decipher the message? How much extra computation does this entail compared with using plain Vigenere?
   (b) Can the "index of coincidence" attack be adapted to mount a known ciphertext attack on this cipher? If so how?

(7) (a) Let $E = \mathbb{Z}/2\mathbb{Z}$. Find an irreducible polynomial of degree four in the ring of polynomials $E[x]$.
   (b) Given a finite field F with q elements we say that $a \in F$ is *primitive* when $\{b \in F : b \neq 0\} = \{a^i : 1 \leq i < q\}$.
   Show that if F is a finite field with q elements, and $a \in F$ is primitive, then for any positive integer m we have that a^m is primitive if and only if $\gcd(m, q-1) = 1$. You may assume that $a^{q-1} = 1$.
   (c) Find all the primitive elements of the sixteen element field constructed from the irreducible polynomial you found in the first part of the question.

(8) Consider the equation $y^2 = x^3 - 4x$.
   (a) Sketch the graph of the corresponding curve.
   (b) Show that in any field F, for a fixed element $a \in F$ there are at most two solutions to the equation $x^2 = a$. Hint: $x^2 = a$ and $y^2 = a$ implies $x^2 - y^2 = 0$.
   (c) Given an odd prime p, let N_p be the number of pairs (a, b) of elements of $\mathbb{Z}/p\mathbb{Z}$ such that the equation $b^2 = a^3 - 4a$ holds in $\mathbb{Z}/p\mathbb{Z}$.
      (i) Show that $N \leq 2p$.
      (ii) Find the value of $N_p - p$ for as many primes p as you can. What do you notice?

(9) Let F be a finite field.

(a) Let f and g be in $F[x]$ with degrees m and n respectively. Give upper bounds on the number of addition and multiplication operations in the field F which are needed to
   (i) Compute $f + g$.
   (ii) Compute fg.
   (iii) Divide f by g, that is compute q and r where $f = gq + r$ and $r = 0$ or $\deg(r) < \deg(g)$.

(b) Let $f \in F[x]$ be a polynomial of degree n. Describe an algorithm for deciding whether f is irreducible in $F[x]$ or not. (You need not write a computer program, but should give a clear and concide description of the steps which are to be performed). Give an upper bound for the number of addition and multiplication operations in F which are needed to execute this algorithm.

(10) In this question we are thinking of a byte as a string of eight bits, that is an element of $(\mathbb{Z}/2\mathbb{Z})^8$. Let V be the set of all bytes. All the linear algebra in this question is done working in the field $\mathbb{Z}/2\mathbb{Z}$.

(a) Roughly how many permutations of V are there?

(b) Estimate the number of invertible 8×8 matrices with entries in $\mathbb{Z}/2\mathbb{Z}$. You may either calculate it exactly or do a Maple experiment, choosing some number of matrices at random and seeing what percentage are invertible.

(c) Let f be given by $f(x) = Ax + b$ where A is an invertible 8×8 matrix with entries in $\mathbb{Z}/2\mathbb{Z}$ and b is an arbitrary element of V. Show that f is a permutation (we say that f is an "affrine permutation"). Roughly how many affine permutations are there?

(d) Find an approximate upper bound for the number of permutations p of V which are "close to being affine" in the following sense: p is close to being affine if there is f an affine permutation such that $p(x) = f(x)$ for at least 192 of the 256 elements $x \in V$.

(11) (needs a bit of research) You are a user of RSA encryption and are somewhat paranoid; you want to ensure that if all the computing power currently existing on Earth was applied for fifty years in an attempt to factorise your public key, it is very unlikely (say probability less than 10^{-100}) that your enemies would be able to recover your private key.

What is the minimum size of the primes that you should use to generate your RSA key, assuming that there are no advances in factoring algorithms over the next fifty years?