E0 235 Cryptography : Aug. - Dec. 2006
Test 1 : 26 September 2006, 1.45 PM - 3.30 PM

1. Show that 1729 is a *Carmichael number,* i.e. the Fermat congruence holds for all integers a.

   Hint: Show that the Fermat congruence is true w.r.t all prime divisors of 1729. (3)

   (a) Show that if $q \equiv 3 \bmod 4$, for q prime, and a is a quadratic residue modulo q, then a solution to the quadratic congruence is obtained as $a^{(k+1)} \bmod q$, where $k = (q-3)/4$.

   (b) Using QR law show that the congruence $x^2 \equiv 33 \bmod 103$ is solvable. Solve the congruence.

   (3+4)

2. The RSA encryption has certain *fixed points*, i.e. messages m that encrypt to the same value: $c = m \equiv m^e \pmod{n}$. Determine the number of fixed points.

   Hint: $|\{a \in \mathbf{Z}_p^* : a^k = 1\}| = gcd(k, p-1)$, CRT. (4)

3. (i) The polynomial $f(x) = x^3 + x + 1$ is irreducible over $\mathbf{F}_2$. Construct *two* rows of the multiplication table of the finite field $\mathbf{F}_8 = \mathbf{F}_2[x]/f(x)$. (ii) Show that the polynomial $f(x)$ primitive ? (iii) What is the maximum number of primitive roots modulo a prime integer p? (6)