E0 235 Cryptography : Aug. - Dec. 2006
Final Examination : 8th December 2006, 2 PM

1. Why does the linear complexity profile of a binary sequence generated by an LFSR follow the line $y = x$ in a step fashion? What is the computational complexity of the Berlekamp-Massey algorithm for computing the linear complexity profile ? Why ? **3+1+2**

2. Consider the three variable Boolean function $f(x_1, x_2, x_3) = x_1x_2 + x_2x_3 + x_3x_1$. Is it *balanced*? Compute the *non-linearity* of the function, given by the minimum distance to the set of *linear* functions. **3+3**

3. Why is the function

$$x \equiv (a * x^2 + b * x + c) \pmod{p},$$

p prime and with $a, b, c \in \mathbf{Z_p^*}$, *not a cryptographically secure* hash function ? Take $p = 103$ and provide examples of the three types of collisions. **2+3**

4. Given k integer, $b(= a^{2^k}) \in \mathbf{Z_p^*}$, device an algorithm to compute a. (Note, the problem is to compute the 2^k-th root, mimicking the square root process, taking care about the sign at each stage.) **5**

5. Develop a 3-party key exchange protocol using the Diffie-Hellman primitive. **3**