E0 235 Cryptography : Aug. - Dec. 2006

Take Home Test 2 : 2 December 2006 (to submit by 11 December 2006)

1. Construct the field $GF(27)$, using the irreducible polynomial $x^3 + x^2 + 2$ over $GF(3)$. (List *all* the elements). **6**

2. Show that for all primes p, the decimal number $n = 1^p 2^p \ldots 8^p 9^p -$ 123456789 is divisible by p. Here i^p denotes a string of $i's$ of length p. (e.g p = 3, n = 111222333444555666777888999 - 123456789). **3**

3. Show that $\forall n, 133 | (11^{n+2} + 12^{2n+1})$. **3**

4. Show that 3 is a quadratic non-residue modulo a Mersenne prime $M_p = 2^p - 1, \forall p > 3$. **3**

5. (a) Consider the Rabin encryption scheme, for message m, compute cipher $c \equiv m^2 \bmod n$, with $n = p * q, p, q$ primes of the form $4k + 3$. How is the message recovered from the cipher c?

   (b) I propose a simple modification of the Rabin public-key encryption algorithm. For message m, compute cipher $c \equiv m^3 \bmod n$. Fow *easy* decryption, what are conditions on p, q? *Hint:* Show $p, q \equiv 7 \bmod 36$ is $useful$.

   (c) With the Hint above, deduce the decryption algorithm.

   2+3+2

6. Justify the choice of prime p such that $p \equiv 3 \pmod 4$ in the Blum-Goldwasser probabilistic encryption scheme. **4**

7. Consider the hash function

$$x_i \equiv (a * x_{i-1}^2 + b * x_{i-1} + c) \pmod p,$$

   p prime and with $a, b, c \in \mathrm{Z}_\mathrm{p}^*$. Discuss the computational complexity of finding collisions : (i) first pre-image, (ii) second pre-image. **8**

8. Determine the operation counts of the different types of operations for key scheduling and encryption for the block ciphers, $DES, Rijndael$ and the hash function $MD5$. **6**