Indian Institute of Technology, Delhi

Major

COL 759 Cryptography and Computer Security

MM 100

1. (7 marks) Let $n \geq 2$ be an integer and $p = 2^n + 1$. Show that if $3^{(p-1)/2} + 1 \equiv 0 \pmod{p}$, then p is a prime.

2. (8 marks) Consider the discrete logarithm problem $5^x \equiv 3 \pmod{1223}$. Using the fact $3^{611} \equiv 1 \pmod{1223}$, determine whether x is even or odd.

3. (15 marks) Find the feedback function of the shift register for the following table

Input			Output
s_0	s_1	s_2	s_3
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	0
1	1	0	0
1	1	1	1

4. (25 marks) Suppose that you have intercepted 16 bits 1100010010100001 of a cryptogram. knowing that the 5-stage LFSR based stream cipher system was used. You also know the first 10 bits of the plaintext i.e. 0110110011 corresponding to the cryptogram. Find the remaining six bits of the plaintext.

5. (25 marks) Let an encryption algorithm (E) is used to construct a hash function. The encryption scheme E may be any symmetric or asymmetric cipher. Suppose the message is divided into two sequences s_1 and s_2 of same size. If the size of the message is odd, then a zero may be padded. The hash function is defined as follows:
   $H(s_1, s_2) = E(E(s_1) \oplus s_2)$
   Show that this scheme is not secure.
   Hint: Find two sequences c_1, c_2 such that $H(c_1, c_2) = H(s_1, s_2)$

6. (20 marks) Let $q = 2^r$, and let the elliptic curve E over F_q, have equation $y^2 + y = x^3$.
   (a) If $q = 16$, show that every $P \in E$ is a point of order 3.
   (b) Show that any point of E with coordinates in F_{16} actually has coordinates in F_4.