INDIAN STATISTICAL INSTITUTE
Semester Examination
M. Tech. (CS) II year (1st Sem): 2015–2016
Cryptology

Date: 01. 12. 2015 Maximum Marks : 40 Time : 2.5 Hours

Please try to write all the part answers of a question at the same place.

1. (a) Explain how the period of an LFSR sequence is related to the nature of the connection polynomial.
   (b) What will be the problem if the state transition matrix of an LFSR is singular?

   [7 + 3]

2. (a) Define non-linearity of a Boolean function.
   (b) If I keep all n-variable Boolean functions inside a bag and randomly pick up one Boolean function from this bag, what is the probability that the function is non-linear? Justify.
   (c) Construct a 3-variable Boolean function that is not correlation-immune.

   [2 + 3 + 5]

3. (a) State and Prove Chinese Remainder Theorem.
   (b) Show that the subset-sum problem defined over a super-increasing knapsack is not NP-complete.

   [(2 + 4) + 4]

4. (a) Explain the common-exponent and the common-modulus attacks on the basic RSA scheme.
   (b) How can these attacks be avoided?

   [(4 + 4) + 2]

5. (a) Show a forgery attack on the basic RSA-based digital signature scheme.
   (b) How can this attack be prevented?
   (c) What do you mean by the security of a key exchange protocol?

   [4 + 2 + 4]