

INDIAN STATISTICAL INSTITUTE
M. Tech. (CrS): 2025–2026
Cryptographic and Security Implementation
Mid-Semestral Examination

Date: 10. 09. 2025

Marks: 50

Time: 2 Hours

Answer any part of any question. The maximum marks you can get is 50. The question is of 60 marks.

Write the part answers of each question at the same place.

1. (a) Write down an efficient algorithm to calculate the Lowest Common Multiple (LCM) of two positive integers, each of size n bits.
(b) What is the time complexity of your algorithm? Clearly explain each step of your calculation.
(c) While you write an actual program in C, will your algorithm work for all pair of inputs if the unsigned integer is n -bit long? [4 + 4 + 2 = 10]
2. (a) Write down the Pseudo Random Generation Algorithm (PRGA) for RC4.
(b) How would you translate the algorithm with C Codes?
(c) Theoretically how many clock cycles your C code should spend to generate one byte?
(d) How would you incorporate instructions in your C code to estimate the number of clock cycles to produce each byte? [3 + 3 + 2 + 2 = 10]
3. Consider the implementation of AES using C programming language.
(a) How would you design the data structures to store the plaintext and ciphertext?
(b) How would you handle the different key sizes for implementation?
(c) How would you implement the 8-bit input 8-bit output S-box?
(d) Then how the Sub Bytes operation will be implemented? [3 + 2 + 3 + 2 = 10]
4. Consider that $n = pq$, where p, q are primes of equal bit size. Explain the outcome of both Solovay-Strassen and Miller-Rabin algorithms while testing primality of n . [5 + 5 = 10]
5. Consider $n = pq$, where p, q are 1024 bit primes. These primes are already available in your program. Explain how would you generate the private and public keys of RSA in C language, with a suitable library of your choice. [10]
6. Consider the operation $a^b \bmod n$.
(a) How can one calculate this efficiently given a, b, n ?
(b) Does the algorithm generate any potential side channel attack during RSA decryption? Explain. [5 + 5 = 10]