M. Sc. Mathematics Examination, 2022

(2nd Year, 2nd Semester)

Introduction to Cryptography

Paper – 4.4 (B-2.27)

Time : Two hours Full Marks : 50

(Symbols have usual meanings, if not mentioned otherwise)

Attempt **Q.1** and ***any four*** from the rest.

1. a) Explain the uses of the one-way function for implementing *passwords*, *signatures*, and *cryptosystems*.

   b) Explain with an example: *Secret sharing*.

   c) Distinguish between *cracking problem* and *promise problem* in a cryptosystem? 5+3+2=10

2. a) Describe the encryption and decryption methods in the *RSA* cryptosystem.

   b) What do you mean by *Hash function* in cryptosystems? Describe a signature system using hash function and *RSA* cryptosystem. 5+(1+4)=10

3. a) Using the big-O notation, find an upper bound in terms of B for the input length of the Travelling Salesrep problem if the number of cities is at most B and the distance between any two cities is also at most B.

   b) Explain how to use an algorithm for the Integer

[Turn over

Factorization decision problem to solve the Integer Factorization search problem. 3+7=10

4. a) Consider the decision problem P:

Input : A list of cities and distances between any two cities, and an integer k.

Question : Do all tours that pass through all of the cities have length more than k?

Is the problem P likely to be in NP? Explain.

b) Suppose that P_1 is the problem

INPUT: Two integers.

QUESTION: Are they equal?

Suppose that P_2 is the problem

INPUT: Two equations $ax+by=0$ and $cx+dy=0$, where a, b, c, d are integers.

QUESTION: Do these equations have any common solution (x, y) other than (0, 0)?

Show that P_2 reduces to P_1 by constructing a reduction of instances of one problem to instances of the other. 4+6=10

5. a) If $P \in BPP$, then for any constant $\in > 0$ give an algorithm whose answers have a probability greater $1-\in$ of being correct.

b) co-RP denotes the set of decision problems that satisfy the definition of RP with "yes" and "no" reversed. Show that the Primality problem:

Input : A positive odd integer N.

Question : Is N a prime number?

is in co-RP.

c) Explain why $BPP \supset RP \cup \text{co-}RP$. 4+3+3=10

6. Describe Hidden Monomial Cryptosystem along with the encryption and decryption schemes. 10

7. Consider a special case of the Polly Cracker with a graph $G=(V,E)$ as the public key, and a valid 3-Coloring of G as its private key. If $B=B(G)=B_1 \cup B_2 \cup B_3$ denotes the basis of polynomials in the variables $\{t_{v,i} : v \in V,\ 1 \le i \le 3\}$ where

$$B_1 = \{t_{v,1}+t_{v,2}+t_{v,3}-1 \ : \ v \in V\};$$

$$B_2 = \{t_{v,i}t_{v,j} \ : \ v \in V, 1 \le i < j \le 3\};$$

$$B_3 = \{t_{u,i}t_{v,i} \ : \ uv \in E, 1 \le i \le 3\}.$$

a) Then construct a one-one correspondence between the private keys and points at which B vanishes.

b) Show that t^2-t belongs to the Poly Cracker's ideal J for each variable t. 5+5=10