INPUT: A positive odd integer N.

QUESTION: Is N a composite number?

is in RP. 5+5=10

4. 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

M. Sc. Mathematics Examination, 2023

(2nd Year, 2nd Semester)

Mathematics

Paper – DSE-07

[Introduction to Cryptography]

Time : $1\frac{1}{2}$ hours Full Marks : 30

(Symbols have usual meanings, if not mentioned otherwise)

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

1. a) What do you mean by *one-way* function and *has* function in the cryptography?

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

   c) Distinguish between *cracking problem* and *promise problem* in a cryptosystem? 3+3+4=10

2. a) Suppose that p and q are distinct primes, and d and e are two positive integers such that $ed\equiv 1 \bmod l$ where $l=lcm(p-1,q-1)$. Let $n=pq$. Prove that for any integer m one has $m^{ed}=m \bmod n$.

   b) Describe the encryption and decryption methods in the *RSA* cryptosystem. 6+4=10

3. a) Describe Rabin's probabilistic primality test.

   b) What do you mean by the complexity class RP? Using Rabin's probabilistic primality test, show that the following compositeness problem: