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 perfect code of G as its private key. Let $N[v]$ consist of v itself and all vertices adjacent to v. Let $B_1 \cup B_2$ denote the basis of polynomials in the variables $\{t_v : v \in V\}$ where

$$B_1 = \left\{1 - \sum_{u \in N[v]} t_u : v \in V\right\};$$
$$B_2 = \left\{t_u t_{u'} : u, u' \in N[v], u \neq u', v \in V\right\};$$

a) Construct a one-to-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, 2022

(2nd Year, 2nd Semester)

Introduction to Cryptography

Paper – DSE - 07 (B30)

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 *hash* function in the cryptography?

   b) Explain the uses of the one-way function for implementing *passwords*, *signatuers*, and *cryptosystems*.

   c) If $P \in BPP$, then for any constant $\in > 0$ give an algorithm whose answers have a probability greater $1 - \in$ of being correct. 2+3+5=10

2. Write the *DSA* scheme and explain why.

   a) Bob expects $g^{u_1} y^{u_2}$ to agree modulo q with r, and

   b) if they agree, he should be satisfied that it really was Alice who sent the message. 4+(3+3)=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: