SC 402

Elements of Cryptography

Dhirubhai Ambani Institute of Information and Communication Technology (DA-IICT)

Version 2 (Spring 2023)

INSTRUCTIONS:

- There are 3 double sided pages (5 printed pages). Ensure that you have all the pages.
- Answer **all questions**, writing clearly in the space provided.
- Show all your work and explain how you arrived at your answers, unless explicitly told to do otherwise.
- Write your name and student number **clearly** at the top of each page before starting the exam.
- You have **two hours** to complete the test
- Marks for each question are indicated in brackets at right. You may use point form for your answers, but make sure the points are clear and unambiguous. I am more interested in your thought process.

FOR MARKER'S USE ONLY

Question	Possible	Received
1	10	
2	10	
3	10	
4	10	
TOTAL	40	

1. Week 1

   (a) Give an example of a hash function that is collision resistance. Justify and Explain your answer. (10)

2. Week 2

   (a) How to mount an attack on RSA-256? Sketch the outline with Justification and Explanations. (10)

3. Week 3

   (a) Give a small example that will illustrate the computations performed in the ElGamal Cryptosystem. (10)

4. Week 4

   (a) For the Elliptic Curve $y^2 = x^3 + x + 6$ over $\mathbb{Z}_{11}$, let $\alpha = (2, 7)$ be a point on the Elliptic Curve, find 2α. (10)