

International Institute of Information Technology, Hyderabad.

Principles of Information Security

Evaluation IV: READING AND ORGANIZATION ASSIGNMENT

April 14, 2020

Due: **April 28, 2020.**

Instructions : Apart from the other [PQR]-style of evaluations, this is the solitary non-programmatic evaluation sheet, consisting of reading and thinking, and as far as evaluation goes, you need to submit a pdf-file.

[Reading Part] Kindly read the book: “THE PRINCETON COMPANION TO MATHEMATICS” edited by Timothy Gowers, a famous Mathematician and Fields Medalist (a pdf-copy of this book will be uploaded in moodle). The book is a brilliant attempt to encompass *all* of contemporary mathematics in a *single* book!

[Thinking Part] Observe that the book is neatly organized in eight parts, viz.: (a) INTRODUCTION (the syntax, semantics and goals of mathematics), (b) THE ORIGINS OF MODERN MATHEMATICS, (c) MATHEMATICAL CONCEPTS (encyclopedia of 99 concepts in alphabetical order), (d) BRANCHES OF MATHEMATICS (a list of 26 branches in an ‘interesting’ order), (e) THEOREMS AND PROBLEMS (35 major results/conjectures of mathematics), (f) MATHEMATICIANS (96 famous mathematicians and their biographies in chronological order), (g) THE INFLUENCE OF MATHEMATICS (analyzing 14 different branches of science that are transformed by mathematics) and (h) FINAL PERSPECTIVES (advices on the *why, how, what, where and when?* of mathematics).

Think about how would you organize all of known cryptography (or say, known to *you*, including all of the textbook and probably some beyond) in to eight parts similar to the aforementioned book.

[To Submit :] The *Table of Contents* (up to the same level of detail given in the aforementioned book) of your own (of course, hypothetical!) book MY COMPANION TO CRYPTOGRAPHY.

ALL THE BEST
