

Proposal for a New Course

- D) Short summary for including in the Courses of Study Booklet: This course introduces students to the design and analysis of cryptographic algorithms with more emphasis on use and applications of various constructions. The course focusses on how real-life protocols and tools may become vulnerable due to weaknesses in these algorithms.

7. Recommended books:

- (i) David Wong: Real World Cryptography, Manning publication, 2021.
- (ii) Jean-Philippe Aumasson: Serious Cryptography 2nd Edition: A Practical Introduction to Modern Encryption, No Starch Press, 2024.

Supplementary readings/ Reference books:

- (i) Mike Rosulek: The joy of Cryptography. Free online book (link: <https://joyofcryptography.com/>)
 - (ii) Katz and Lindell, Modern Cryptography, Revised 3rd Edition, CRC Press
 - (iii) Relevant research papers
-

Dated: 13 August 2026; Proposer: Somitra Sanadhya

Dated: _____ ; DUGC Convener (WSAIS): _____

The course is approved / not approved

Chairperson, SUGC

Dated: _____