







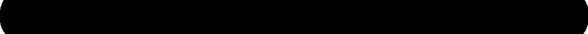

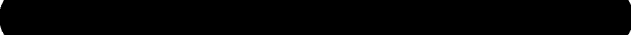


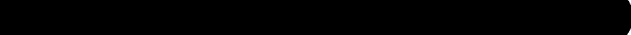

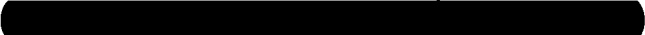



CURRICULUM VITAE

PERSONAL INFORMATION	<div>Subham Das</div> <div> subhamdas965@gmail.com (PGP key <a href="#">here</a>)</div> <div> ms20121@iisermohali.ac.in</div> <div> <a href="https://cryptosubh.github.io/">https://cryptosubh.github.io/</a></div>
BRIEF INTRODUCTION	<p>Currently I am a student at Indian Institute of Science Education and Research, Mohali and pursuing a BS-MS (Integrated Bachelor's and Master's Degree) in Mathematics. I am pursuing my Master's Thesis in Isogeny-based cryptography in the academic year 2024-2025. Prior to this, my academic interest has been predominantly in Algebraic geometry, especially in the geometry of vector bundles with a focus on moduli problems.</p>
EDUCATION	<div>Indian Institute of Science Education and Research, Mohali, India</div> <div><i>Integrated BS-MS Program</i> </div> <div></div> <div></div>
AWARDS	 
PROJECTS	<div><div>Master's thesis</div><div>Jan 2024 - Present</div><div><i>Investigations and cryptanalysis of isogeny-based cryptographic schemes</i></div><div>Supervisor </div><div>Aim : The broad theme of the MS-thesis shall be towards detailed analysis and investigations of the existing cryptographic schemes in this field which shall present a better understanding not only of the specific security assumptions of these schemes and their robustness, but also give insight to the underlying theory on which these schemes are built upon.</div></div> <div><div>Vector Bundles over Algebraic Curves</div><div></div><div>Supervisor </div><div>Participated in the course titled above remotely with extensive discussions on Families of vector bundles, Cartier Divisors, Degree of a Vector Bundle, Stability, Harder Narasimhan Filtrations. More details can be found on the course page </div></div> <div><div>Reading Project on Complex Algebraic Geometry</div><div></div><div>Supervisor </div><div>The topics covered here are the first three chapters of Claire Voisin's "<i>Complex Algebraic Geometry and Hodge Theory</i>". Emphasis was on examples and the theory of holomorphic vector bundles, Differential forms and complex analysis of several variables</div></div> <div><div>Riemann Surfaces and related topics</div><div></div><div></div><div>This project involved discussions on several related topics on Riemann surfaces, Morse theory and Abelian varieties. Details can be found </div></div>

## SKILLS

**Programming languages:** Python (basic)

**Office softwares:** Open Office,  $\text{\LaTeX}$

**Languages:** English (C1, TOEFL '24 Score [REDACTED]), Bengali (native), Hindi.

## COURSES TAKEN

**2021 :** MTH101 Groups and Symmetry, MTH102 Analysis in One Variable, MTH201 Curves and Surfaces

**2022 Spring Semester:** IDC207 Number Theory and Cryptography, MTH202 Probability Theory

**2022 Monsoon Semester:** MTH301 Analysis in  $R^n$ , MTH302 Linear Algebra, MTH304 Group Theory, MTH303 Set Theory and Logic

**2023 Spring Semester:** MTH305 Complex Analysis, MTH306 Lebesgue Measure and Integration, MTH307 Topology, MTH308 Ring theory and Modules, MTH419 Number Theory

**2023 Monsoon Semester:** MTH401 Ordinary Differential Equations, MTH402 Functional Analysis, MTH403 Fields and Galois Theory, MTH424 Lie Algebra and Representation theory, MTH404 Commutative Algebra

**2024 Spring Semester:** MTH408 Algebraic Topology, MTH426 Algebraic curves

## EXTRACURRICULAR ACTIVITIES

Playing bass guitar, harmonica, painting and occasionally writing haikus.