



MATHEMATICAL CIPHERS

Delving into the Cryptographic Complexities of
Number Theory and Abstract Algebra



MENTORS

Naman Gupta

namangupta22@iitk.ac.in, 7678600231

Ishan Dandwani

ishand22@iitk.ac.in, 9887541586

Sanskar Yaduka

sanskary22@iitk.ac.in, 8434842395





IN THE REALM OF

CRYPTOGRAPHY

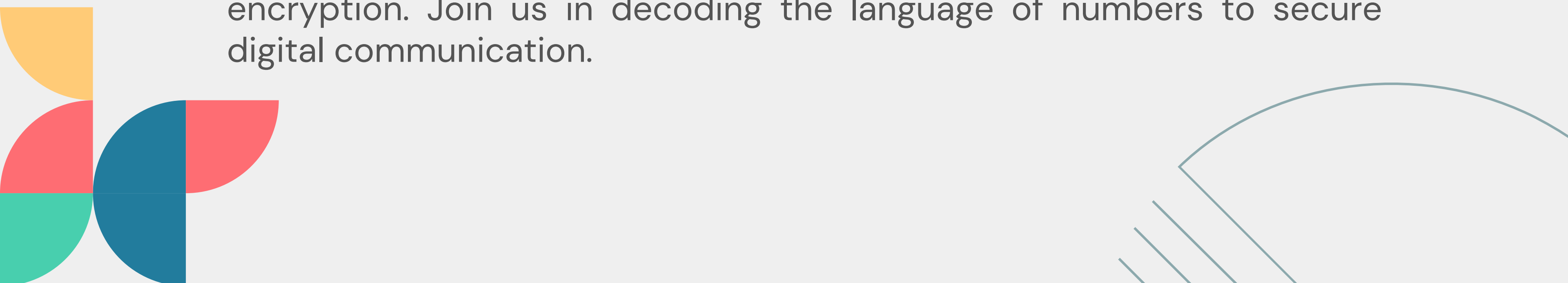
MATH REIGNS SUPREME





PROJECT INTRODUCTION

Dive into the fusion of mathematics and cryptography. Beginning with number theory essentials like Euclid's algorithm and Fermat's little theorem, we traverse abstract algebra's terrain of Group Theory, Rings, and Fields. Transitioning to practical applications, we unravel key exchange algorithms such as RSA, culminating in the study of AES encryption. Join us in decoding the language of numbers to secure digital communication.



WEEK 1-3

- Discover key Number Theory concepts like Euclid's Algorithm and Fermat's Little Theorem.
- Explore practical applications such as Euler's Totient Function and the Chinese Remainder Theorem.
- Delve deeper into advanced topics like Algebraic Number Theory and Combinatorial Number Theory.
- Gain a comprehensive understanding of essential concepts such as Divisibility and Density in Number Theory.
- Conclude with an interactive week dedicated to brainstorming problems and engaging in assignment tasks.



WEEK 4-6

- Our exploration will commence with delving into group theory, recognizing its foundational importance.
- Groups will be introduced, with a focus on their abstract nature and their significance across diverse applications emphasis will be placed on the relevance of groups, particularly in cryptographic algorithms.
- We'll explore rings and fields, highlighting their resilience and importance in key exchange algorithms and hashing.
- We'll delve into a comprehensive examination of various problems to reinforce understanding and foster a broader approach to problem-solving within these mathematical frameworks.

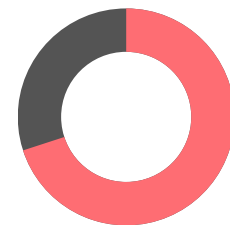


WEEK 7-10

- Cryptographic Protocols: Explore RSA, Diffie–Hellman, ECC, and AES, focusing on their design and application in cryptography.
- Security Analysis: Investigate algorithm security, covering computational hardness, key sizes, and vulnerabilities like brute force attacks.
- Practical Implementations: Examine real-world applications such as secure messaging, digital signatures, and secure computation.
- Recent Advances: Survey post-quantum cryptography, homomorphic encryption, and zero-knowledge proofs, highlighting their significance.
- Future Directions: Discuss evolving challenges and potential paths forward in cryptography.



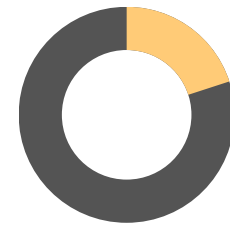
LOGISTICS FOR THE PROJECT



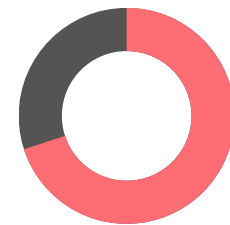
PROJECT DURATION 8-10 WEEKS



WEEKLY COMMITMENT 7-8 HRS




PREREQS - BASIC MATH APTITUDE



BIWEEKLY ASSIGNMENTS



EXPECTED NUMBER OF MENTEEES - 50 (Y23S, Y22S)



THANK YOU :)