Deciphering the Mysteries

Plan of Action- SoS 2023(Cryptography)

Arya Vishe
21D070018, IIT-B

Mentor- Nilabha Saha

20/06/23

1 Objectives

Over the period of the next few weeks, I intend to start off with classical ciphers such as Vigenére Ciphers. After that, I can spend a few weeks to build up some knowledge on fields such as Number theory, Group theory, and Abstract Algebra, as a basis for modern cryptography techniques such as RSA, DES, AES encryptions, and, if time permits, Stream and Block ciphers, Hash functions, Pseudo-random bit generation and Elliptic curves.

I will also be having a project running in parallel to SoS so I will be keeping relatively low loads in the beginning.

2 Outline of the timetable

Week 1 (29th May- 4th June)	Overview and introduction to cryptography[1], Probabilistic cryptanalysis of Vigenére ciphers
Week 2 (5th June- 11th June)	Probability theory, Number theory, Information theory, Abstract Algebra
Week 3 (12th June- 18th June)	Generation of Pseudorandom bits, Stream and Block Ciphers
Week 4 (19th June- 25th June)	
Mid-summer Report week[2](26th June- 2nd July)	Lag week

Table 1 –

Week 6 (3rd July- 9th July)	Diffie Heilman (Discrete Logarithm), RSA (Factorisation)
Week 7 (10th July- 16th July)	Finite Fields, Data Encryption Standard (DES), Advanced Encryption Standard (AES)
Week 8 (17th July- 23rd July)	Hash functions, Authentication problem, Digital signatures
Final Project submission[3] (24th July- 30th July)	Elliptic curves

References

[1] Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman, *An Introduction to Mathematical Cryptography*

[2] Joshua Holden, *THE MATHEMATICS OF SECRETS*

[3] Jonathan Katz and Yehuda Lindell, *Introduction to Modern Cryptography*

[4] Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, *HANDBOOK of APPLIED CRYPTOGRAPHY*

[5] Simon Singh, *"The Code Book- HOW TO MAKE IT, BREAK IT, HACK IT, CRACK IT"*

Note- [1] and [2] are going to be referred to primarily, [3] will be used for Modern methods and [4] will be used as an additional reference. [5] is merely for introductory puposes

[1] From both [1] and [2]
[2] Tentative date- 15th June
[3] Tentative date- 15th July