ACA Semester Project:

Randomness & Applications

- Aravind Reddy

What is Randomness?

- Prob[H] = Prob [T] = 1/2
- HTHTTTHHHTHTHTHHHHTH
- HHHHHHHHHHHHHHHHHTT
- Which of the two strings generated by a toss of an unbiased coin is more random?
- PseudoRandom - Deterministic structures which share some properties of random ones

The remarkable utility of Randomness

- Fast Information Acquisition
- Cryptography - RSA, Elgamal
- Primality Testing - Rabin Miller Primality testing
- Distributed Computation
- Randomised Algorithms - Median finding

Stuff you do:

- General introduction to randomness - Chapter 1 of the book Pseudorandomness by Salil Vadhan, Talk by Avi Wigderson.

- A few randomised algorithms - Polynomial Identity Testing, Median Finding.

- A modified version of the Median Finding algorithm - You have to come up with the design and implement it in any way you choose. Expect this to be *challenging*.

- After you have reached this far, you can choose to study one application of randomness in depth. For example, generation and usage of random numbers in DOTA 2.