Tata Institute of Fundamental Research
Survey No. 36/P, Gopanpally Village, Serilingampally, Ranga Reddy Dist., Hyderabad – 500 046

Colloquium

Can Quantum mechanics help your BFF to hack your accounts?

N. D. Hari Dass

IMSc, Chennai

Security is paramount to a world leaning obsessively on digital transactions. Large scale banking and nuclear launch codes are examples. After a brief introduction to traditional methods of securing secrets like lock and keys, I will explain the basic concepts of Encryption and Decryption. The traditional approaches relied on the so called 'symmetric key' concept wherein both encryption and decryption are done with the same key, making security very vulnerable. I will explain the revolutionary concept of 'asymmetric keys' of which the currently popular RSA protocol is an example. The security here arises from the extreme difficulty in factorising very large numbers. Prime numbers play a key role. I will mention the fastest supercomputers of the day and their inability to tackle the factorisation problem. After explaining the rudiments of Quantum Mechanics, I will outline how the so called 'Quantum Computers' offer the hopes of unprecedented computational speeds and how they can pose credible threats to the RSA protocols. I will also attempt to explain the famous Shor's algorithm in this context without going into all the technicalities.

Monday, Nov 13th 2023

4:00 PM (Tea / Coffee 3.45 PM)

Auditorium, TIFR-H