1. **Name of the course:** Advanced Cryptology

2. **Objective of the course:** Cryptology is concerned with the conceptualization, definition, and construction of computing systems that address security concerns. The design of cryptographic systems must be based on firm foundations. This course presents a rigorous and systematic treatment of the foundation issues: defining cryptographic tasks and solving new cryptographic problems using existing and new tools. The focus is given on the basic mathematical tools as well as some new advanced cryptographic tools and the advances of research using those tools.

3. Learning Outcome:
Students attending this course is expected to have a clear idea on fundamental concepts and can demonstrate the feasibility of solving cryptographic problems rather than on describing ad hoc approaches. The learners should have a concrete conception on the basic mathematical tools like computational difficulty, pseudo-randomness, multi-party protocols. Alongside, they get a systematic overview on the progress of advanced cryptographic concepts such as authenticated encryption, homomorphic encryption, searchable encryption, physical attacks and lattice based Cryptography.

4. Detailed Syllabus

- Computational Difficulty: Computation Model, One-way Functions, One-way Permutations, Hard-core Predicates, Pseudorandom Generators.

- Secure Multi-party Computations: Zero-knowledge Proof Systems, Oblivious Transfer, Yao's Two-party Protocol.

- Authenticated Encryption: Security Model, Generic Constructions, Desired Properties, Structural Classification,
Light-weight Application based Designs.

- Cloud Computation: Searchable Encryption, Homomorphic Encryption.

- Physical Attacks: Side Channel Attacks, Simple and Differential Power Attacks, Threshold Implementation, Fault Attacks.

- Lattice Based Cryptography:- Basics of Lattice, SVP, CVP, SIVP (decisional and approximate version), LLL Algorithm, SIS, LWE, Ring-SIS, Ring-LWE, Lattice based Signature, NTRU