Course Code	CSE-524
Course Name	Theory of Modern Cryptography
Credits	4
Course Offered to	UG/PG
Course Description	From this course, we will learn about three basic principles of Modern Cryptography: Principle 1 – Formulation of Exact Definitions, Principle 2 – Reliance on Precise Assumptions, Principle 3 – Rigorous Proofs of Security. It is very important to know how to prove the security of cryptographic systems, because we cannot guarantee any security without security proof. During classes, we will learn how to apply above principles to hash function, MAC, digital signature, symmetric encryption scheme, public key encryption scheme, pseudorandom function, Game-based Proof Techniques, Random Oracle Model,…. In addition to the above approach, we need to know NEW modern cryptography such as homomorphic encryption, multiparty computation, etc.. Each student will participate in a course project so that students may learn how modern cryptography works in real life.

Pre-requisites

Pre-requisite (Mandatory)	Pre-requisite (Desirable)	Pre-requisite(other)
		Discrete mathematics, Applied cryptography or Foundations of computer security

*Please insert more rows if required

Post Conditions*(For suggestions on verbs please refer the second sheet)

CO1	CO2	CO3	CO4
The students are expected to understand what is the requirement and procedure of developing secure modules or secure devices to sell those products to the Federal Government of USA.	The students are expected to understand how modern cryptography techniques can solve security and privacy issue.	The students are expected to learn about blockchain, crypto-currency, hardware-based security (ex, PUF).	

Weekly Lecture Plan

Week Number	Lecture Topic	COs Met	Assignment/Labs/Tutorial/Projects

Week 1 and 2	Introduction to this course, basic probability theory, Security Notions and Indistinguishability, Cipher Block Chaining construction (CBC)		Project, 6 hours per week
Week 2 and 3	Pseudorandomness (PRF/PRP), PRF security Proof of CBC, Relation between MAC Security and PRF Security, Basic of Game-playing Technique		Project, 6 hours per week
Week 3 and 4	Uniform/Non-uniform Adversary, One-way Function, Hard-core Predicate. A Trapdoor One-way "Family of Permutations" and Its Applications		Project, 6 hours per week
Week 5 and 6	Public-key Encryption Schemes (Theory and Practice) Security Evaluation of OAEP and OAEP+, Detailed Security Proof of OAEP+ using Game-based Proving Technique		Project, 6 hours per week
Week 7 and 8	Yao's Two-party Secure Computation based on Garbled Circuit (with Oblivious Transfer), GMW's Multi-party Secure Computation based on Secret Sharing (with Oblivious Transfer), Two-party Secure Computation based on Homomorphic Encryption, Very Efficient Three-party Secure Computation only based on Secret Sharing		Project, 6 hours per week

Week 9 and 10	Universal Composability (necessary for security proof of MPC), The First Fully Homomorphic Encryption (designed by Gentry)		Project, 6 hours per week
Week 11-15	Project-based Presentations		Project, 6 hours per week

*Please insert more rows if required

Weekly Lab Plan			
Week Number	**Laboratory Exercise**	**COs Met**	**Platform (Hardware/Software)**

*Please insert more rows if required

Assessment Plan	
Type of Evaluation	% Contribution in Grade
Homework	10
Mid-sem	20
End-sem	20
Project	50

*Please insert more row for other type of Evaluation

Resource Material	
Type	**Title**
Textbook	1. Jonathan Katz and Yehuda Lindell, “Introduction to Modern Cryptography”
	2. Oded Goldreich, “Foundations of Cryptography”

	3. M. Bellare and P. Rogaway, “Introduction to Modern cryptography”
	4. S. Goldwasser and M. Bellare, “Lecture Notes on Cryptography”