Course Title:	CS-880, Information Assurance
Credit Hours:	3+0
Pre-requisites:	▪ Software Construction ▪ Data Structures ▪ Computing Algorithms
Course Description:	This course is aimed at students who would like to learn security basics. The course enables students to satisfy NSA educational guidelines for professional training in Information Assurance (NSTISSI 4011). It gives a broad introduction to the major topics in computer and communication security and information assurance. The objective of this course is to provide students with a basic understanding of the problems of information assurance and the solutions that exist to secure information on computers and networks.
Tools and Technologies:	▪ SSH ▪ Linux Security Modules
Learning Outcomes:	Students taking this course can expect to acquire the following: 1. an understanding of Security Policy and Mechanisms and basic cryptographic techniques 2. Importance of the Confidentiality, Integrity and Availability (CIA) models in different Computer Science Areas 3. Basic quantitative and qualitative risk analysis and Security Planning Skills
Tentative MS Thesis:	▪ Automatic Security Logic Analyzers ▪ Rule Language for Web Application Firewalls
Text Books:	▪ Matt Bishop (2003): Computer Security Art and Science, Pearson Education.
Reference Books:	▪ Computer Security Principles and Practice, William Stallings and Lawrie Brown. Pearson Education 2008

Course Contents:	▪ Introduction to Information Assurance o Threats, Trust and Assumptions o High Assurance Systems ▪ Overview of Security Policy & Mechanisms o Natural Language Security Policies o Authorized System States, Policy Models o Policy Languages, Low-Level Policy Languages ▪ Security Planning and Risk Analysis o Elements of Risk Analysis o Quantitative vs Qualitative Analysis o Risk Management Cycle, Risk/Control Tradeoffs o Risk Analysis Frameworks ▪ Classic Cryptography o Transposition Ciphers, Substitution Ciphers o Cæsar cipher, Vigènere cipher, Solitaire cipher o One Time Pad, Book cipher, Enigma ▪ Private Key Cryptography o Stream and Block Ciphers, Confusion and Diffusion o Avalanche Effect, Feistel Network o Generation of Round Keys, DES and AES ▪ Public Key Cryptography o Diffie-Hellman, RSA, Direct Digital Signatures o Collisions, Birthday Paradox, MD5 and SHA ▪ Key Management o Session and Interchange Keys o Classical Key Exchange, Needham-Schroeder o Kerberos, PKI Trust Models, X.509, OpenPGP o Digital Signatures ▪ Authentication o Authentication System, Dictionary Attacks o Using Time, Using Salting, Detecting Trojan Login o BioMetrics

	▪ Access Control Matrices o Protection state of system o Boolean Expression Evaluation o Composite State Transitions, HRU Model o State Transitions from Primitive Commands o Confer rights and remove rights, Copy Rights o Attenuation of Privilege, The Safety Problem