**ABET Course Syllabus – CS4780**

|  |  |  |  |
| --- | --- | --- | --- |
| **Code** | CS4780 | **Credits** | 3 |
| **Title** | Cryptography and Information Security | **Coordinator** | Huiping Guo |

**Course Information**

1. **Catalog Description:** Principles and practice of cryptography and information security; basic concepts of cryptology, classical ciphers, modern symmetric ciphers, Advanced Encryption Standard, public key cryptography, data integrity and digital signature schemes.
2. **Prerequisite**: CS3112
3. **Contact Hours**: 3 hours/week
4. **Required/Elective:** This course is an elective in the BS program.

**Textbook**

Behrouz A. Forouzan, Cryptography and Network Security, McGraw Hill Higher Education,   ISBN:  0072870222

**Course Goals**

The Student Learning Outcomes that are addressed by the course are:

* SLO #1. Students will be able to apply concepts and techniques from computing and mathematics to both theoretical and practical problems.
* SLO #3. Students will have a strong foundation in the design, analysis, and application of many types of algorithms.
* SLO #5. Students will have the training to analyze problems and identify and define the computing requirements appropriate to their solutions.
* SLO #8. Students will have the knowledge, skills, and attitudes for lifelong self-development
* SLO #9. Students will have the ability to analyze the local and global impact of computing on individuals and society

Other outcomes of instruction:

At the end of the course, students are able to

* understand fundamental concepts in number theory.
* apply number theory to cryptographic algorithms
* illustrate modern cryptographic algorithms
* identify and solve real-world security problems

**Topics Covered**

* Introduction to security and attacks
* Mathematics of cryptography
* Symmetric cryptography
* Classical ciphers
* Modern symmetric ciphers
* Modes of operation
* S-AES
* Encipherment
* Asymmetric key cryptography
* Public-key cryptography Hash function
* Digital signature
* Message Authentication Algorithms
* Digital Signature
* Authentication Protocols
* Key Management Protocols