Course Syllabus

IS492 Information Security

Catalog Description: This course extends the broad overview of information/cyber security presented in the prerequisite courses and introduces a rigorous and practical study of authentication codes and hash functions, smartcards, electronic payment systems, pseudorandom number generation, identification, zero knowledge proofs, side channel attacks and other related issues are addressed. Biometrics including fingerprint biometrics, biometric statistics, FAR and FRR rates and identification using biometrics are also considered.

Credit Hours: 3 Credit hours: 3 Lectures per week 0 Labs. per week 0 Recitation per week

Prerequisites: IS 380

Course Learning Outcomes:

1. Define the concepts related to advanced information security
2. Describe advanced cryptography and its implementation considerations
3. Apply advanced security technologies.
4. Evaluate the effectiveness of security technologies
5. Create and maintain a comprehensive security model.
6. Explain risk analysis and risk management.
7. Design an organization's security policy.
8. Function effectively on teams to accomplish a common goal.
9. Communicate effectively in oral and written form.

Major Topics:

- Introduction to Information Security
- Authentication codes and hash functions, smartcards, electronic payment systems, pseudorandom number generation, identification, zero knowledge proofs, side channel attacks and other related issues are addressed.
- Biometrics including fingerprint biometrics, biometric statistics, FAR and FRR rates and identification using biometrics are also considered.
- Project Discussions

Text Books:

- Information Security Principles and Practice, 2nd edition, Mark Stamp, Wiley Publications, 2011, ISBN 978-0470626399.

Course Syllabus

IS492 Information Security

Grading:

- The grading scale for this course is:

95 - 100	A+	Passing
90 - 94	A	Passing
85 - 89	B+	Passing
80 - 84	B	Passing
75 - 79	C+	Passing
70 - 74	C	Passing
65 - 69	D+	Passing
60 - 64	D	Passing
0 - 59	F	Failing

- Final grades will be determined based on the following components:
  . 60% Semester Work
  . 40% Final Exam
- Students may not do any additional work for extra credit nor resubmit any graded activity to raise a final grade.
- Late submissions will not be accepted for any graded activity for any reason.
- Students have one week to request the re-grading of any semester work.

Attendance Policy:

Students should attend 80% of the overall course hours taught in the semester as per the University regulations.

If a student fails to achieve this portion, he/she shall not be allowed to appear in the final exam and shall be awarded "DN" grade and repeat the course.

Cheating and Plagiarism Policy:

The instructor will use several manual and automated means to detect cheating and/or plagiarism in any work submitted by students for this course.

When a student is suspected of cheating or plagiarism, the instructor raises the issue to the disciplinary committee.

Course Syllabus

IS492 Information Security

Communications:

Registered students will be given access to a section of the Learning Management System (LMS) for this course. LMS will used as the primary mechanism to disseminate course information, including announcements, lecture slides, assignments, and grades.

Communication with the instructor on issues relating to the individual student should be conducted using CIS email, via telephone, or in person.