University of Arkansas - Fort Smith
5210 Grand Avenue
P. O. Box 3649
Fort Smith, AR 72913-3649
479-788-7000
General Syllabus

CSCE 35133 Applied Cryptography

Credit Hours: 3 Lecture Hours: 3 Laboratory Hours: 0

Prerequisite(s): CSCE10204 Foundations of Programming II and CSCE 20503 Foundations of CyberSecurity

Effective Catalog: 2020-2021

I. Course Information

A. Catalog Description

Theoretical foundation and practical applications of a cryptographic system. Topics introduced are protocol generation and design, the symmetric and asymmetric cryptographic approaches, hash ciphers and functions and challenges to formulate in an adversarial environment.

II. Student Learning Outcomes

A. Subject Matter

Upon successful completion of this course, the student will be able to:

1. Discover security vulnerabilities in programming code.
2. Evaluate and assess when to use block ciphers, hash routines or public key encrypted systems.
3. Design and program cryptographic systems utilizing the concepts of a modern cryptographic technique.
4. Demonstrate the ability to communicate effectively the details of a cryptographic algorithm in both verbal and written form.

B. University Learning Outcomes

This course enhances student abilities in the following areas:

Communication Skills (Written and Oral)
Students will be able to communicate orally and through writing via presentations and programming documentation.

Analytical Skills
Critical Thinking Skills
Students will analyze security requirements and properties to implement the appropriate cryptographic solution.

Analytical Skills
Quantitative Reasoning Skills
Students will design various solutions to satisfy their class assignments. Proper implementation will include the ability to produce accurate output in both programming and written solutions and to measure effective solutions.

III. Major Course Topics

A. Historical overview of cryptography
B. Symmetric-key cryptography and the key-exchange problem
C. Public-key cryptography
D. Digital signatures
E. Security protocols
F. Applications (zero-knowledge proofs, authentication, and so on)
G. Block ciphers - modeling, implementing and uses
H. Hash functions - analyzing, developing, implementation and usage
I. RSA and Diffie-Hellman protocol
J. Network security protocols (SSL/TLS or IPSEc)
K. Message Authentication Codes