**DRAFT CSCE 5423 Cryptography (3 credit hours)**

**Catalog Description**: This course provides an introduction to cryptography and its applications, and practices such knowledge through homework and hands-on assignments. Topics covered include Cryptography Basics, Symmetric Key Cryptography, Public-Key Cryptography, Cryptographic Hash Function, Digital Signature, Authentication, Key Management, Password Security, SSL/TLS, IPsec, Cryptography-Assisted Anonymous Communications, Cryptocurrency, and Privacy-Aware Computing.

**Prerequisites**: Proficient in programming.

**Textbook / Required material**: Douglas Robert Stinson, and Maura Paterson, *Cryptography: Theory and Practice*, Fourth Edition, CRC Press, 2018.

**Goals**: The goal of the class is to learn cryptography, and develop skills to analyze and implement cryptographic solutions.

**Student Learning Outcomes. By the end of this course, students will be able to:**

* Understand how cryptography algorithms work and applications of cryptography
* Select the right cryptographic algorithms for the cybersecurity needs of different computing and engineering problems.
* Apply symmetric-key cryptography, asymmetric-key cryptography, message authentication code, digital signature and key exchange to solve computing and engineering problems.

**Grading**

The grading in this course will be distributed as follows.

* Homework: 60%
* Midterm: 20%
* Final: 20%

**Academic Dishonesty Policy**

As a core part of its mission, the University of Arkansas provides students with the opportunity to further their educational goals through programs of study and research in an environment that promotes freedom of inquiry and academic responsibility. Accomplishing this mission is only possible when intellectual honesty and individual integrity prevail. Each University of Arkansas student is required to be familiar with and abide by the University's ‘Academic Integrity Policy’ at honesty.uark.edu. Students with questions about how these policies apply to a particular course or assignment should immediately contact their instructor.

**Prepared by**: Qinghua Li **Date**: 2/3/2021