



College of Computing and Informatics  
Department of Software and Information Systems

## ITIS 6240/8240 | Applied Cryptography | 3 credits

**Faculty:** Dr. Yongge Wang

**Email:** [yonwang@uncc.edu](mailto:yonwang@uncc.edu)

**Office:** Woodward 330G

**Phone:** 708-687-8665

**Office Hours:** Online through WebEx Thursday, 3:00 PM to 6:00 PM

*My preferred method of contact is by email. I will respond to all emailed questions within 24 hours Mon-Fri. I do not respond to emails over the weekend.*

### Course Description:

This course will provide students with an understanding of modern cryptographic techniques, algorithms and protocols that are of fundamental importance to the design and implementation of security critical applications. Covers not only standard cryptographic techniques, but also exposes students to the latest advances in applied cryptography. Topics include: secret and public key ciphers, stream ciphers, one-way hashing algorithms, authentication and identification, digital signatures, key establishment and management, secret sharing and data recovery, public key infrastructures, and efficient implementation.

### Pre or Co-requisite:

Full graduate standing, or permission of department.

### Meeting Times:

Online, asynchronous or Thursdays 7:00–9:45 p.m. in WH 140. Class meeting time: August 22, 29, September 5, 12, 19, 26, October 3, 10, 17, 24, 31, November 7, 14, 21

### Course Objectives:

- Understand symmetric key encryption algorithms, hash function algorithms, public key cryptography algorithms and key agreement protocols.
- Understand the attacks and vulnerabilities with respect to current industrial standards for cryptography.
- Understand quantum computing techniques and their impact with respect to security of current cryptographic techniques.

- Apply cryptographic algorithms and protocols to solve security problems (such as confidentiality, integrity and authenticity problems)
- Use open source cryptographic techniques to design and implement secure software products, both commercial and non-commercial.

### Required Materials:

- Handbook of Applied Cryptography, CRC Press. ISBN: 0-8493-8523-7. October 1996. Online version available at: <http://cacr.uwaterloo.ca/hac/>
- Online lectures: <https://www.youtube.com/channel/UC1usFRN4LCMcfIV7UjHNUQg/videos>

Course Element	Point Value	Percentage
Efficient AES implementation	10	10%
Efficient SHA implementation	10	10%
OpenSSH	20	20%
VPN	20	20%
Two exams	40	40%
Total	100	100%

### Grading Scale:

A 100 % to 90.0%  
 B <90.0 % to 80.0%  
 C <80.0 % to 70.0%  
 U <70.0 % to 0.0%

### Course Policies:

#### Syllabus Revision:

The standards and requirements set forth in this syllabus may be modified at any time by the course instructor. Notice of such changes will be by Canvas announcement or email notice.

#### Classroom Conduct:

I will conduct this class in an atmosphere of mutual respect. I encourage your active participation in class discussions. Each of us may have strongly differing opinions on the various topics of class discussions. The conflict of ideas is encouraged and welcome. The orderly questioning of the ideas of others, including mine, is similarly welcome. However, I will exercise my responsibility to manage the discussions so that ideas and argument can proceed in an orderly fashion. You should expect that if your

conduct during class discussions seriously disrupts the atmosphere of mutual respect I expect in this class, you will not be permitted to participate further.

**Late Work and Make-Ups:**

- Small assignments that are submitted late will receive a zero.
- Major Writing Assignments submitted after the due date and time will receive an automatic one-time deduction of 25%. Assignments submitted more than a week after the due date will receive a zero.

**Feedback:**

Typically, feedback will be returned within one week for small assignments and two weeks for larger papers.

**Code of Student Responsibility:**

“The UNC Charlotte Code of Student Responsibility (the Code) sets forth certain rights and responsibilities in matters of student discipline. The Code defines these responsibilities and guarantees you certain rights that ensure your protection from unjust imposition of disciplinary penalties. You should familiarize yourself with the provisions and procedures of the Code” (Introductory statement from the UNC Charlotte brochure about the Code of Student Responsibility). The entire document may be found at this Internet address: <http://legal.uncc.edu/policies/ps-104.html>

**Academic Integrity:**

All students are required to read and abide by the Code of Student Academic Integrity. Violations of the Code of Student Academic Integrity, including plagiarism, will result in disciplinary action as provided in the Code. Students are expected to submit their own work, either as individuals or contributors to a group assignment. Definitions and examples of plagiarism and other violations are set forth in the Code. The Code is available from the Dean of Students Office or online at: <http://legal.uncc.edu/policies/up-407> Faculty may ask students to produce identification at examinations and may require students to demonstrate that graded assignments completed outside of class are their own work.

**Course Credit Workload:**

This 3-credit course requires 9 hours of work a week. Class work may include but is not limited to: required readings, library research, written assignments, discussion posts, viewing of course videos, reviewing feedback from the instructor, and completing assessments.

**Non-Discrimination:**

All students and the instructor are expected to engage with each other respectfully. Unwelcome conduct directed toward another person based upon that person's actual or perceived race, actual or perceived gender, color, religion, age, national origin, ethnicity, disability, or veteran status, or for any other reason, may constitute a violation of University Policy 406 (<https://legal.uncc.edu/policies/up-406>). The Code of Student

Responsibility. Any student suspected of engaging in such conduct will be referred to the Office of Student Conduct.

**Title IX:**

Title IX UNC Charlotte is committed to providing an environment free of all forms of discrimination and sexual harassment, including sexual assault, domestic violence, dating violence, and stalking. If you (or someone you know) has experienced or experiences any of these incidents, know that you are not alone. UNC Charlotte has staff members trained to support you in navigating campus life, accessing health and counseling services, providing academic and housing accommodations, helping with legal protective orders, and more. Please be aware that many UNC Charlotte employees, including all faculty members, are considered Responsible Employees who are required to relay any information or reports of sexual misconduct they receive to the Title IX Coordinator. This means that if you tell me about a situation involving sexual harassment, sexual assault, dating violence, domestic violence, or stalking, I must report the information to the Title IX Coordinator. Although I have to report the situation, you will still have options about how your case will be handled, including whether or not you wish to pursue a formal complaint. Our goal is to make sure you are aware of the range of options available to you and have access to the resources you need. If you wish to speak to someone confidentially, you can contact any of the following on-campus resources, who are not required to report the incident to the Title IX Coordinator: (1) University Counseling Center ([counselingcenter.uncc.edu](http://counselingcenter.uncc.edu), 7-0311); (2) Student Health Center ([studenthealth.uncc.edu](http://studenthealth.uncc.edu), 7-7400); or (3) Center for Wellness Promotion ([wellness.uncc.edu](http://wellness.uncc.edu), 7-7407). Additional information about your options is also available at [titleix.uncc.edu](http://titleix.uncc.edu) under the “Students” tab.

**Religious Accommodation:**

Students who, acting in accordance with this Policy, miss classes, examinations or other assignments because of a religious practice or belief must be provided with a reasonable alternative opportunity to complete such academic responsibilities. It is the obligation of students to provide faculty with reasonable notice of the dates of religious observances on which they will be absent by submitting a [Request for Religious Accommodation Form](#) to their instructor prior to the census date for enrollment for a given semester. The census date for each semester (typically the tenth day of instruction) can be found in [UNC Charlotte’s academic calendar](#).

**Student Grievances:**

Student Grievances Students enrolled in courses at the University of North Carolina at Charlotte who would like to file a complaint regarding their experience may do the following: 1. Refer to the UNC Charlotte Student Grievance Procedure. Students may also contact UNC Charlotte’s regional accrediting agency, the Southern Association of Colleges and Schools Commission on Colleges. 2. Students residing outside of North Carolina while attending UNC Charlotte may file a complaint in their state of residence.

As required by federal regulations, students are directed to the list of resources here, compiled and updated by the State Higher Education Executive Officers.

**Withdrawals:**

Students are expected to complete all courses for which they are registered at the close of the add/drop period. If you are concerned about your ability to succeed in this course, it is important to make an appointment to speak with me as soon as possible. The University policy on withdrawal allows students only a limited number of opportunities available to withdraw from courses. It is important for you to understand the financial and academic consequences that may result from course withdrawal.

**Incompletes:**

The grade of I is assigned at the discretion of the instructor when a student who is otherwise passing has not, due to circumstances beyond his/her control, completed all the work in the course. The missing work must be completed by the deadline specified by the instructor, and no later than 12 months. If the I is not removed during the specified time, a grade of F, U, or N, as appropriate is automatically assigned. The grade of I cannot be removed by enrolling again in the same course, and students should not re-enroll in a course in which they have been assigned the grade of I. University policy addressing Incompletes.

**Student Support:****Disability Support Services:**

Students in this course seeking accommodations to disabilities must first consult with the Office of Disability Services and follow the instructions of that office for obtaining accommodations. The Office of Disability Services works with current undergraduate and graduate students along with prospective students to ensure equal access to UNC Charlotte's campus and educational programs.

All services are dependent upon verification of eligibility. Once approved for services, students receive accommodations which are based upon the nature of an individual's disability and documented needs. Students are strongly encouraged to register or check-in for their accommodations with a Disability Services counselor as soon as they have registered for classes. Accommodations are not retro-active and will not begin until the student notifies his or her faculty by providing the Letter of Accommodation. Please visit the Office of Disability Services at for additional resources, email questions to [disability@uncc.edu](mailto:disability@uncc.edu), or call 704-687-0040 (tty/v) for more information.

**Student Support Services:**

Be sure to take advantage of the wealth of resources and support available at UNC Charlotte. Some of the resources available to you include the University Writing Resource Center, University Counseling Center, and the J. Murrey Atkins Library.

- [University Center for Academic Excellent \(UCAE\) | \(704\) 687 7837 | uncc-ucae@uncc.edu](#)
- [University Writing Resources Center \(WRC\) | 704-687-1899 | wrchelp@uncc.edu](#)
- [Veteran Student Services | 704-687-5488 | veteranservice@uncc.edu](#)
- [University Counseling Center | 704-687-0311](#)
- [Multicultural Resource Center | 704-687-7121 | mrc@uncc.edu](#)
- [List of computer labs on campus](#)
- [Atkins Library Laptop Lending program](#)