Teaching Philosophy

Teaching and research are complementary activities continually supporting each other. Yet, they are generally treated as separate activities in academia. It is unavoidable that teaching fundamentals has a priority at the early stages of undergraduate education. However, the current trend of separating teaching and research creates problems at the later stages of academic education. Besides, this approach often causes significant productivity loss for both industry and academia in long terms.

My teaching philosophy concentrates on creating a synergy between teaching and research. However, creating such a synergy primarily requires a good education on computer science fundamentals (e.g., algorithms/data structures, computer networking and systems). After a solid background on these fundamentals are formed, I will devote a significant effort to combine teaching and research whenever possible. This approach aims to inspire the creativity and productivity without omitting fundamentals. My goal is to train passionate and creative IT professionals and academics who can fulfill the rapidly growing needs of both industry and academia.

I plan to realize my teaching philosophy based on the following principles:

- **Encouraging Active Participation:** Students should not be passive observers but active participants in the learning process. I will encourage students to engage the classroom activities via in-class discussions.

- **Project-Oriented Approach:** I strongly believe that the best way of learning a complicated concept is to realize it on real problems. This is even valid for many theoretical subjects (e.g., cryptography) once they are properly tied with a real-life application. In this direction, I will pursue a project-oriented and take-home-based course structure. I observed that students learn much better when they put an effort to understand and realize the course subject via term projects. This approach also enables a permanent learning, which might not be achieved by classical exam-only classes. These projects will be supported by plenty of take-home assignments that include difficult questions but with sufficiently long deadlines. The assignments encourage students to investigate topics from different angles by conducting short research assignments.

- **Integrating Teaching, Research and Practicality:** I believe that exposing students to open problems and recent research results, even at the early undergraduate level, is highly beneficial. I observed that students are much more excited, once they realize that there is a lot of room to explore the subjects they work on.

At the undergraduate level, I plan to present the recent research results from a high-level perspective, and then encourage students to write surveys and short technical reports on a subject of their choice. I would offer generous extra credits to increase the interest.

At the master level, I will give project-oriented approach a higher priority along with laboratory projects to strengthen the practical side. These projects will focus on state-of-art technologies such that students will have rudimentary skills to meet the needs of emerging trends in industry. At the PhD level, I will focus on research proposals, recent papers published in flagship conferences and literature scanning via comprehensive survey assignments. Depending on class size, I plan to conduct frequent one-on-one meetings with each student, providing detailed feedback on their research proposals.

Another essential point is to form the correct research habits as early as possible. Once an incorrect research habit forms, it is very difficult to remove it later. I will prevent my students to form such habits via continuous guidance. I will inform students about common mistakes repeated by researchers and how to avoid such mistakes.

- **Bridging Theory and Practice with Motives:** Forming a solid theoretical computer science fundamentals is a crucial requirement for students. Such fundamentals establish a common framework for communication, collaboration, and provide the necessary tools for the student to pursue their career. However, fundamentals alone, might not always be sufficient to create high impact results. Moreover, I observe that it is challenging to motivate students to learn these fundamentals without demonstrating their essential role in modern computer systems and applications.

I will put a relentless effort to bridge theory and practice while forming the fundamentals. I will achieve this objective by showing that these fundamental concepts are the enablers of all real-life computer applications exist today. This approach will encourage students to commit their efforts to learn these fundamentals, and then apply them to create practical solutions for challenging problems.

- **Improving Technical Writing and Presentation Skills:** A common but grave mistake is to consider the technical writing and formal presentation of ideas as a secondary task during the education process. Despite how good the idea is, if it is not presented in a correct way, convincing the reader/listener might not be possible. I will provide the same guidance that I received from my PhD advisors Prof. Dr. Peng Ning and Prof. Dr. Michael K. Reiter on this matter. This will help students to secure highly competitive industrial and academic positions in their future career.

- **Grading Fairly:** Fair grading is essential for evaluating and motivating students. My TA experiences enable me to reward the productivity without sacrificing fairness.
Teaching Experience

During my PhD, I served as a Teaching Assistant (TA) for various computer science courses including undergraduate, master and PhD level courses.

- **CSC 226 Discrete Mathematics (undergraduate)**: This course was a large-size class with more than hundred students. This class helped me to understand the special needs of early stage undergraduate students. Moreover, I suggested improvements on the curriculum, which modernize the course content by covering recent advances in applied mathematics. These improvements are now a part of CSC 226 offered by Prof. Dr. Robert Rodman.

- **CSC 574 Network Security (MS)**: I served as a TA for MS level network security classes for three semesters, generally mid-size classes with mixed MS and PhD students. I have learned various aspects of teaching this course, since I worked with three excellent instructors as a TA. I guided master students for their research projects, in which they proposed their own ideas and then implemented them on the real-systems. Furthermore, I helped students for mid-size laboratory exercises focusing on network attack/defense techniques. I received a very positive feedback from students and the course instructors.

- **CSC 579 Computer Networks Performance Analysis (MS)**: In this course, I gained experience on guiding students for advanced networking topics such as queuing theory and probabilistic network modeling. Moreover, I wrote some chapters of “Definitive Introduction: Computer Simulation”, which is used as one of the course books for CSC 579 offered by Prof. Dr. Harry Perros.

- **CSC 774 Advanced Network Security (PhD)**: I served as a TA for an advanced network security class for two semesters, a small/mid-size class with PhD students as well as post-docs. I had a privilege to receive one-on-one teaching training from my advisor Prof. Dr. Peng Ning on this course for one year. I acquired an invaluable experience on how a research-oriented course can be taught in a very understandable and enjoyable way. I helped PhD students on their research proposals via one-on-one meetings during my office hours. I also helped students for laboratory exercises, which implement advanced Wireless Sensor Network (WSN) security protocols on a large WSN testbed.

Mentoring Experience

During my TA duties for CSC574 and CSC774, it was my responsibility to guide MS and PhD students on various small research projects, including but not limited to, secure communication in P2P networks, key distribution mechanisms with threshold cryptography and secure key establishment techniques in ad-hoc networks. I helped students to develop their own original ideas to address challenging problems via continuous discussions and technical guidance. We implemented these ideas on actual systems (e.g., sensor testbeds) and test their validity via extensive experiments.

In my current position, as a research scientist, I guide MS and PhD students on various research projects via internships and academic collaborations:

- **Mr. Anvesh Ragi** is a MS student at the University of Texas at Dallas, Department of Computer Science. We currently work on “Efficient Symmetric Searchable Encryption Schemes”. I guide him on cryptographic scheme design and formal security analysis as well as high-performance cryptographic coding on C/C++. This internship currently yield a patent and we are actively work on a publication.

- **Mr. Shalabh Jain** is a PhD candidate at the University of Maryland College Park, Department of Electrical and Computer Engineering. We work on “Efficient Digital Signatures for Real-time Multicast Systems”. I guided him on design, analysis and deployment of advanced cryptographic algorithms on embedded wireless network platforms (e.g., MSP430, Micaz). This internship yielded a patent and a publication with ongoing collaboration on a research paper.

- **Ms. Alana Libonati** is a PhD candidate at the University of Chapel Hill at North Carolina, Department of Computer Science. We currently work on “User Friendly Authentication Methods”.

- **Mr. Yi Ding** is a PhD student at the Georgia Technical University, the School of Computer Science. We work on “Efficient and Secure Face Recognition via Multi-Party Computation”.

Teaching Preferences

My core expertise areas are network security, applied cryptography and algorithms. Therefore, I will be pleased to teach courses on those areas, both at the undergraduate and graduate levels. In addition to these, I can offer a broad variety of courses, in which I harness my algorithmic and applied research background.

Undergraduate Level

I will offer courses that will lay down a solid computer science foundation for undergraduate students. In this way, the students can target the most challenging academic or engineering career paths with a high confidence after their graduation. In all these courses, I will emphasis the breadth supported by depth in any opportunity.
Attila Altay Yavuz, Ph.D., Teaching Statement

At the undergraduate level, I can teach a broad variety of courses that cover both the theoretical and applied aspects of the computer science. At the theory side, I can assume the courses including but not limited to the following: Introduction to computer science, discrete mathematics, algorithm design and analysis, data structures, introduction to cryptography and introduction to numerical methods. At the applied side, I can assume the following courses: Introduction to programming with C, computer networks and information/network security.

Among a broad selection of undergraduate courses that I can offer, I would be especially pleased to teach the following ones:

I would like to teach discrete mathematics, as I have a TA experience and a substantial background on this class. I will cover basic discrete mathematic concepts to create a solid fundamental. I will add programming exercises to realize fundamental concepts (e.g., basic data structures, graph algorithms) for each homework (I also would like to introduce “Latex” as an editing tool for homeworks).

I would also like to teach algorithm design and analysis, wherein I will focus on data structures (e.g., trees, heap, linked list), fundamental algorithms (e.g., sort/search and graph theoretical) with their theoretical analysis and applications to the real-life problems. There will be plenty of programming assignments, complexity analysis and theorem proving exercises. Moreover, I plan to assign team (with a size of three to five students) projects, in which students will work on challenging system building or theoretical analysis tasks.

I will be pleased to teach introduction to cryptography and information and network security courses as they are my core expertise areas. In the cryptography track, I will teach basic cryptography concepts (e.g., symmetric/public key cryptography, digital signatures, security models), and fundamentals (e.g., number theory, finite field arithmetic, factorization and discrete logarithm problem) by giving a priority to the breadth instead of the depth. I will give small projects to ensure that students learn how to realize these cryptographic concepts with open source cryptographic libraries (e.g., NTL with C, MIRACL with C++ and JCA). In information and network security track, I will focus on commonly used security methods and concepts, supported with basic cryptography and network security fundamentals. I will give laboratory assignments to provide practical experience for students on recent security tools and mechanisms.

Graduate Level

At the graduate level, I would like to teach a network security course and an advanced information security course. I will utilize my TA experience (e.g., CSC 574 and CSC 774) for these courses by adding my own improvements and teaching style. Moreover, I plan to cover recent trends and emerging technologies on security and privacy in industry, by leveraging my recent industrial research experience.

In the network security course, I plan to cover a wide range of topics including cryptographic protocols and network security basics supported by plenty of application projects and laboratory assignments (e.g., SEED project). I expect that students completing this class can evaluate works in academic and commercial security, and will have essential skills in security research and industrial consultation. The course will cover topics; including but not limited to, basic elements of cryptography/cryptanalysis, network security, authentication, security protocol design and analysis, security modeling, trusted computing, key management, DDoS detection and mitigation, biometrics, web security, and other emerging topics.

In the advanced information security course, I will cover advanced security mechanisms, which can answer the security and privacy needs of recently emerging real-life applications. Some applications include heterogeneous wireless systems and sensors networks (e.g., internet of things and systems), resource-constrained networking environments (e.g., intra-car security, RFID/smarte-card security protocols) and cloud-based distributed systems (e.g., cloudlets). I will cover advanced crypto methods (e.g., ID-based crypto, polynomial/self-certified key exchange), trusted execution environments, access control and privacy policies.

I will ask students to write research reports based on the recently published papers in flagship security conferences (e.g., CCS, S&P). I will provide a detailed technical feedback to each student on her research proposal with one-on-one meetings. Moreover, I will ask students to present research papers of their interest in the class and give each student a feedback on her presentation.