CYBER SECURITY (CYSE)

CYSE 610 Applied Cryptography   **3 Credits**
Grade Mode: Standard Letter, Audit/Non Audit

The course covers cryptographic primitives such as one-way, collision-resistant hash functions, as well as the relevant number theory and discusses public-key encryption and basic key-exchange coupled with real-life applications. In a nutshell, the course studies how two parties who have a shared secret key can communicate securely when a powerful adversary eavesdrops and tampers with traffic. The course will also cover popular secure protocols such as zero-knowledge proofs. Throughout the course students will be exposed to a variety of open problems in the field.

CYSE 630 Computer and Network Security   **3 Credits**
Grade Mode: Standard Letter, Audit/Non Audit

This course covers the concepts of assets, vulnerabilities, controls, threats and attacks, security measures and mechanisms. The course will introduce the fundamental concepts of security technology for computer networks, and the applications of these technologies. Topics include an overview of fundamental cryptography, authentication, encryption, digital signatures, digital certificates, and network security protocols such as IP Sec, SSL, etc. Students will also obtain the fundamental knowledge on network security mechanisms such as firewall and network intrusion detection systems.

CYSE 640 Security Risk Analysis   **3 Credits**
Grade Mode: Standard Letter, Audit/Non Audit

This course explores the basic elements of risk and to introduce security risk assessment methodologies and related tools used by many of the world's major corporations. The choice of the tools and methods in this course are based on its popularity in practice and enables the course to address cybersecurity issues related compliance with security policies, external standards and with appropriate legislation.

CYSE 720 Data Privacy   **3 Credits**
Grade Mode: Standard Letter, Audit/Non Audit

This course covers the concepts, technologies, practices and challenges associated with Information Security and Privacy, and a broad view of the subject, which includes looking at relevant business, organizational, human, legal and policy issues. The course combines technical discussions with a wealth of examples from enterprise and government systems, social networking, mobile and pervasive computing, privacy standards like HIPAA or GLBA, and much more. The course combines formal lectures with discussion of recent, hot topics and how they relate to data privacy and the multi-facet challenges in practice and real world.

CYSE 727 Wireless Networks & Security   **3 Credits**
Grade Mode: Standard Letter, Audit/Non Audit

The course explores the fundamentals of wireless networks as well as its security techniques and challenges. Students will learn a general overview of wireless networking standards, security issues and challenges in wireless networks, and security mechanisms in wireless technologies. Students will also learn security techniques in existing networks such as mobile ad-hoc networks, sensor networks, and wireless mesh networks as well as emerging networks such as smart grids, internet of things, and vehicular networks. Finally, the course will cover a general overview of physical layer security that exploits wireless channels for improving security of wireless networks.

CYSE 728 Distributed Systems Security   **3 Credits**
Grade Mode: Standard Letter, Audit/Non Audit

This course focuses on fundamental and advanced concepts in Distributed Systems, addressing their foundations, current technologies, and security aspects. Topics include, but are not limited to, distributed hash tables (peer-to-peer systems), failure detectors, synchronization, election, distributed agreement, consensus, gossiping, replication, key-value stores, NoSQL, blockchain technology. These topics are discussed in the context of real-life and deployed systems such as clouds and datacenters, databases, peer to peer systems, clusters, cryptocurrencies.

CYSE 729 Multimedia Security   **3 Credits**
Grade Mode: Standard Letter, Audit/Non Audit

This course has several objectives: (i) delivering fundamental and advanced concepts about multimedia content representation, (ii) highlighting the trade-offs between quality and multimedia channel capacity, (iii) designing and implementing security tools to protect multimedia content.

CYSE 744 Network Forensics   **3 Credits**
Grade Mode: Standard Letter, Audit/Non Audit

This course exposes students to practical issues involving the monitoring and investigation of private data communications. Issues considered include such topics as network monitoring, network data collection, network flows, and visual security analysis. Students will learn how to perform forensic investigations of network-based attacks, through a series of lab exercises, hands-on assignments, and a term project.

CYSE 745 Computational Forensics   **3 Credits**
Grade Mode: Standard Letter, Audit/Non Audit

This course builds the necessary awareness required to assess physical and digital crimes at local, regional and global levels. Assessment, in this context, includes the evaluation of the nature of the crime, handling and tracking physical and digital evidence connected to the crime in a manner consistent with legal requirements for presenting forensic evidence. Students will learn about various state-of-art computational tools used in forensic analysis of different types of evidence. The course also builds awareness of intelligence practices across the globe that have bearing on crime investigation, especially of organized crime