Proposed Undergraduate Course Title: **Cryptographic Hardware for Embedded Systems**
Proposed Credits: **3 lecture hours + 3 lab hours per week = 4 credit hours total**
Proposed Number: **3XXX (3000-level)**

Prerequisites: ECE 2040 and ECE 2031

Proposed course material:
(Book) Bruce Schneier. Applied Cryptography, John Wiley & Sons, 1996
(Lecture Notes) To be distributed via a course website

Course Syllabus and Topical Outline
Module 1: Authentication
- Access control, challenge-response, keys
- One-way functions
- VLSI circuits and characteristics

Module 2: Cryptography from a hardware-centric perspective
- Data integrity and authenticity
- Historic ciphers: substitution, permutation/transposition and one-time pads
- Symmetric and asymmetric keys, models and protocols
- DES and associated cryptographic hardware

Module 3: Power Analysis Attacks
- Simple Power Analysis
- Differential Power Analysis
- Electro-Magnetic (EM) Analysis

Module 4: Cryptographic Hardware and Vulnerabilities
- ASIC versus FPGA versus Microprocessor (i.e., software)
- Side Channel Analysis

Module 5: VLSI Test, Supply Chain and Hardware Attacks
- Design verification and manufacturing test
- Relationship between physical faults (test) and malicious attack (Hardware Trojans)

Evaluation Criteria: The course will have two midterm exams, a final exam and frequent homeworks/labs (typically each week except the week of an exam). Labs will be based on VHDL and associated digital design and simulation tools (e.g., ModelSim).

Learning Objectives: As a part of this course, students perform the following:
1. Apply knowledge of mathematics and computing to understand cryptography and authentication.
2. Master core concepts of cryptographic hardware design.
3. Obtain laboratory experience in protection, analysis and side-channels of cryptographic digital logic.

4. Learn modern automatic VLSI synthesis, simulation and analysis tools using state-of-the-art facilities.
5. Apply the engineering design process to design cryptographic hardware that meets the constraints of time, cost, energy and security.

Learning Outcomes: Upon successful completion of this course, students will be able to do the following:

1. Analyze the level of security provided by symmetric encryption algorithms such as DES and asymmetric encryption algorithms such as RSA.
2. Write VHSIC Hardware Description Language (VHDL) code to implement encryption algorithms including synthesis to hardware logic gates.
3. Provide approaches to authentication able to resist attacks such as man-in-the-middle and replay.
4. Explain dangers associated with hardware Trojan insertion of logic gates in the chip design process including the manufacturing supply chain.
5. Make tradeoffs between execution speed, area, energy/power and resistance to side-channel analysis and attacks for practical digital logic implementations of encryption and authentication.

Attendance & Absences: Students with medical, family or other critical emergencies should contact the Office of the Dean of Students. Students should familiarize themselves with http://www.catalog.gatech.edu/rules/4/. To the extent possible, students should communicate excused absences in advance; when not possible, student shall communicate their excused absence as soon after the emergency as can reasonably be expected for the situation. Late assignments will not be accepted for credit without an excused absence.

Honor Code: Students are expected to hold the highest ethical standards not only for this class but for the rest of their professional careers. Hardware security is a very serious topic and is critical to ensuring privacy, confidentiality and a healthy society. However, ethics in this course start and end in the human person. The Georgia Tech Honor http://www.policylibrary.gatech.edu/student-affairs/academic-honor-code Code http://catalog.gatech.edu/rules/18/ holds in all of its parts. When there is reasonably clear evidence of a violation, a referral to the Office of the Dean of Students will occur, and all hearings and other resulting procedures will be followed to completion.

Office of Disability Services: Students who are registered with the Office of Disability Services (ODS) shall provide appropriate forms and paperwork in person to the course instructor. If you think you may have learning needs, feel free to contact the Office of Disability Services at (404) 894-2563 or https://disabilityservices.gatech.edu/. An accommodation letter must be obtained from ODS in order to receive accommodations.