Lahore University of Management Sciences

EE 5216 / CS 595 – Hardware Design for IoT Security

Fall 2023/24

To understand how to navigate course outlines, consult: How to Use a Course Outline (http://surl.li/gpvuw)

Instructor	Muhammad Ali Siddiqi
Room No.	9-211A
Office Hours	TBA
Email	m.siddiqi@lums.edu.pk
Telephone	8490
Secretary/TA	TBA
TA Office Hours	TBA
Course URL (if any)	LMS will be used
Support Services	LUMS offers a range of academic and other services to support students. These are mentioned below, and you are encouraged to use these in addition to in-class assistance from course staff. For a complete list of campus support services available for you click here (https://advising.lums.edu.pk/#supportservices)

Course Basics				
Credit Hours	3			
Lecture(s)	Nbr of Lec(s) Per Week	2	Duration	75 min
Recitation/Lab (per week)	Nbr of Lec(s) Per Week	X	Duration	
Tutorial (per week)	Nbr of Lec(s) Per Week	X	Duration	

Course Distribution	
Core	None
Elective	MS in EE / CS / Digital and Embedded Systems
Open for Student Category	PhD / MS / Junior / Senior
Close for Student Category	Freshman / Sophomore

COURSE DESCRIPTION
The course focuses on utilizing digital design principles to enhance the security of the Internet of Things (IoT). In light of the growing necessity for robust security measures within IoT devices, and in response to the distinctive security challenges inherent to these devices, this course delves into the area of security-primitive implementation in hardware. This emphasis on hardware-based implementations stems from their demonstrated efficiency, particularly when contrasted with software-based approaches. This is especially important given the resource-constrained nature of IoT devices in general. Topics covered include cryptographic algorithms, lightweight cryptography, low-power design for security, secure communication protocols, battery-depletion attacks/countermeasures, side-channel attacks/countermeasures, and more. Through theoretical knowledge and practical implementation, students will develop the skills necessary to design and implement security measures for IoT devices, ensuring the confidentiality, integrity and availability of such devices in an ever-evolving landscape.

COURSE PREREQUISITE(S)	
	CS225 Fundamentals of Computer Systems OR EE324 Microcontroller and Interfacing OR EE/CS-320 Computer Organization and Assembly Language OR GRAD

COURSE OBJECTIVE

To equip students with the knowledge and skills to enhance the security of IoT devices through the utilization of digital design principles and techniques.

Grading Breakup and Policy

Class quizzes (4-6): 15%
Assignments (1-2): 5%
Project + Presentation: 10%
Midterm exam: 35%
Final exam: 35%

Examination Detail

Midterm Exam	Yes/No: Yes Combine Separate: Separate Duration: 120 minutes Preferred Date: TBA Exam Specifications: TBA
Final Exam	Yes/No: Yes Combine Separate: Separate Duration: 120 minutes Exam Specifications: TBA

Course Learning Outcomes

CLO1: Analyze conventional block/stream ciphers.
CLO2: Efficiently implement block/stream ciphers in hardware to ensure suitability for IoT applications.
CLO3: Explain the concept of public key cryptography (PKC) and the RSA crypto system, and implement it efficiently. Additionally, demonstrate the use of PKC in key-exchange protocols for ensuring security.
CLO4: Evaluate the security of Bluetooth LE and assess the impact of battery-depletion attacks on medical IoT devices. Identify various types of side-channel attacks and propose countermeasures.

Relation to EE Program Outcomes

	Related PLOs	Levels of Learning	Teaching Methods	CLO Attainment checked in
CLO1	PLO1, PLO2	Cog-2	Instruction, Assignments	Midterm, Quizzes
CLO2	PLO1, PLO2	Cog-2	Instruction, Assignments	Midterm, Quizzes
CLO3	PLO1, PLO2	Cog-3	Instruction, Assignments	Final, Quizzes
CLO4	PLO1, PLO2	Cog-4	Instruction, Assignments	Final, Quizzes

Campus supports & Key university policies

Campus Supports

Students are strongly encouraged to meet course instructors and TA's during office hours for assistance in course-content, understand the course's expectations from enrolled students, etc. Beyond the course, students are also encouraged to use a variety of other resources. (Instructors are also encouraged to refer students to these resources when needed.) These resources include Counseling and Psychological Services/CAPS (for mental health), LUMS Medical Center/LMC (for physical health), Office of Accessibility & Inclusion/ OAI (for long-term disabilities), advising staff dedicated to supporting and guiding students in each school, online resources (https://advising.lums.edu.pk/advising-resources), etc. To view all support services, their specific role as well as contact information click here (https://advising.lums.edu.pk/#supportservices).

Academic Honesty/Plagiarism

LUMS has zero tolerance for academic dishonesty. Students are responsible for upholding academic integrity. If unsure, refer to the student handbook and consult with instructors/teaching assistants. To check for plagiarism before essay submission, use similarity@lums.edu.pk. Consult the following resources: 1) Academic and Intellectual Integrity (http://surl.li/gpvwb), and 2) Understanding and Avoiding Plagiarism (http://surl.li/gpvwo).

LUMS Academic Accommodations/ Petitions policy

Long-term medical conditions are accommodated through the Office of Accessibility & Inclusion (OAI). Short-term emergencies that impact studies are either handled by the course instructor or Student Support Services (SSS). For more information, please see Missed Instrument or 'Petition' FAQs for students and faculty (https://rb.gy/8sj1h)

LUMS Sexual Harassment Policy

LUMS and this class are a harassment-free zone. No behavior that makes someone uncomfortable or negatively impacts the class or individual's potential will be tolerated.

To report sexual harassment experienced or observed in class, please contact me. For further support or to file a complaint, contact OAI at oai@lums.edu.pk or harassment@lums.edu.pk. You may choose to file an informal or formal complaint to put an end to the offending behavior. You can also call their Anti-Harassment helpline at 042-35608877 for advice or concerns. *For more information: Harassment, Bullying & Other Interpersonal Misconduct: Presentation (http://surl.li/gpvwt)*

COURSE OVERVIEW

Lecture	Topics	Recommended Readings	Objectives/ Application/related CLO
1	Introduction to Cryptography and IoT Security	Chapter 1 (textbook)	CLO1
2	Modular Arithmetic and Historical Ciphers	Chapter 1 (textbook)	
3	Stream Ciphers, Random Numbers and Linear Feedback Shift Registers	Chapter 2 (textbook)	
4			
5	Introduction to Block ciphers, and Galois Fields (for AES)	Chapter 4 (textbook)	
6	Advanced Encryption Standard (AES)		
7	Block-cipher modes of operations	Chapter 3 and 5 (textbook)	
8	Multiple encryption attacks		
9	Low-power Design for IoT security	Handouts	CLO2
10	Battery-lifetime analysis		
11	Implementing AES in Hardware		
12	Lightweight Cryptography (GIFT, SIMON, PRESENT etc.)	Chapter 3 (textbook) and handouts	
13			

14	Midterm Review		
	Midterm		
15	Number Theory for Public-key crypto: Euclidean Algorithm, Euler's Phi Function & Euler's Theorem	Chapter 6 (textbook)	CLO3
16	The RSA Cryptosystem	Chapter 7 (textbook) and handouts	
17	Efficient implementation of RSA		
18	Efficient Exponentiation		
19	Diffie-Hellman Key Exchange Finite Groups, Cyclic groups and Discrete Log Problem	Chapter 8 (textbook)	
20	Digital Signatures and Security Services	Chapter 10 (textbook)	
21	Hash functions and Message Authentication Codes	Chapter 11 & 12 (textbook)	
22	Secure Key-Exchange and Communication Protocols	Chapter 13 (textbook) and handouts	
23			
24	Bluetooth LE security	Handouts	CLO4
25	Battery-depletion attacks and Countermeasures	Handouts	
26	Side-Channel Analysis and Countermeasures	Handouts	
27		Handouts	
28	Final-exam Review		
	Final exam		

Textbook(s)/Supplementary Readings

Textbook:
“Understanding Cryptography: A Textbook for Students and Practitioners” by Christof Paar and Jan Pelzl
Supplementary Reading:
Hand-outs and online links will be provided where needed

Prepared by:	**Muhammad Ali Siddiqi**
Date:	**21 August 2023**