Lahore University of Management Sciences

EE 5216 – 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	muhammad_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 / 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). With the increasing need for comprehensive security measures in IoT devices, this course explores the integration of digital techniques to address the unique security challenges faced by IoT hardware. 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 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.

Lahore University of Management Sciences

Grading Breakup and Policy
Class quizzes: (2-4): 10% Assignments: (1-2): 10% Midterm exam: 40% Final exam: 40%

Examination Detail	
Midterm Exam	Yes/No: Yes Combine Separate: Combine Duration: 120 minutes Preferred Date: TBA Exam Specifications: TBA
Final Exam	Yes/No: Yes Combine Separate: Combine Duration: 150 minutes Exam Specifications: TBA

Course Learning Outcomes
CLO1: Analyze a conventional block cipher (e.g., AES) and implement it efficiently in hardware. CLO2: Analyze lightweight block ciphers and assess their suitability for low-power design in security 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	CLO Attainment checked in
CLO1	TBD	TBD	Midterm, Final, Quizzes
CLO2	TBD	TBD	Midterm, Final, Quizzes
CLO3	TBD	TBD	Midterm, Final, Quizzes
CLO4	TBD	TBD	Final, Quizzes

Campus supports & Key university policies
Campus Supports

Lahore University of Management Sciences

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		CLO1
2	Review of Digital Logic Fundamentals		
3			
4	Modular Arithmetic and Historical Ciphers	Chapter 1 (textbook)	
5	Stream Ciphers, Random Numbers and Linear Feedback Shift Registers	Chapter 2 (textbook)	
6			
7	Introduction to Galois Fields (for AES) Advanced Encryption Standard (AES) Implementing AES in Hardware	Chapter 2 (textbook)	
8			
9			
10	Lightweight Cryptography (GIFT, SIMON etc)		CLO2
11			
12	Low-power Design for security		
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)	
17			

18	Efficient implementation of RSA		
19			
20	Efficient Exponentiation		
21			
22	Secure Key-Exchange and Communication Protocols		
23			
24	Bluetooth LE security		CLO4
25	Battery-depletion attacks and Countermeasures		
26	Side-Channel Analysis and Countermeasures		
27			
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

Rubric Based Assessment of CLO	
Rubric Details	Rubric used for CLOs: TBD CLO-wise details of each rubric design per assessment module: TBD

Prepared by:	**Muhammad Ali Siddiqi**
Date:	**19 July 2023**