

CRYPTOGRAPHIC ENGINEERING

NOVEMBER 16-27, 2026

On-Line Course using Microsoft TEAMS



WEEK 1		November 16-20, 2026	10 Modules (1:30hr each), 2 Modules per day		
WEEK 2		November 23-27, 2026	10 Modules (1:30hr each), 2 Modules per day		
		Central European Time	Eastern Standard Time	Pacific Standard Time	India Standard Time
DAILY		CET	EST	PST	IST
Module 1		3:30-5:00 pm	9:30-11:00 am	6:30-8:00 am	8:00-9:30 pm
Module 2		5:30-7:00 pm	11:30 am -1:00 pm	8:30-10:00 am	10:00-11:30 pm
WEEK 1	Module				
DAY 1, MON, Nov. 16	1	Introduction to Block Ciphers; DES and AES			
	2	Lightweight Block Ciphers for RFIDs			
DAY 2, TUE, Nov. 17	3	Public-Key Cryptography: Algorithms and Protocols			
	4	Integer Arithmetic Algorithms and Architectures			
DAY 3, WED, Nov 18	5	Specialized Hardware for Secret-Key Algorithms			
	6	Introduction to PUFs (Physically Unclonable Functions)			
DAY 4, THU, Nov. 19	7	Finite Field Arithmetic Algorithms and Architectures			
	8	Public-Key Cryptographic Hardware and Software Design			
DAY 5, FRI, Nov. 20	9	Post-Quantum Cryptography Algorithms			
	10	Post-Quantum Cryptography Implementations			
WEEK 2	Module				
DAY 6, MON, Nov. 23	11	Introduction to Side-Channel Analysis			
	12	Trusted Computing Architectures, SSL and IPsec			
DAY 7, TUE, Nov. 24	13	Block Ciphers: Attacks and Countermeasures			
	14	RSA/ECC - Side Channel Attacks & Countermeasures			
DAY 8, WED, Nov. 25	15	Electromagnetic Attacks, Countermeasures and Advanced Analysis Techniques			
	16	Fully Homomorphic Encryption			
DAY 9, THU, Nov. 26	17	Random Number Generators for Cryptographic Applications			
	18	Evaluation Criteria Non-Deterministic Random Number Generators			
DAY 10, FRI, Nov. 27	19	Random Number Generator Design Constraints and Challenges			