CRYPTOGRAPHIC ENGINEERING

JUNE 9-20, 2025

On-Line Course using Microsoft TEAMS

Mead Education

WEEK 1		**JUNE 9-13, 2025**	10 Modules (1:30hr each), 2 Modules per day		
WEEK 2		**JUNE 16-20, 2025**	10 Modules (1:30hr each), 2 Modules per day		
DAILY		**Central European Time**	**Eastern Standard Time**	**Pacific Standard Time**	**India Standard Time**
		CET	**EST**	**PST**	**IST**
Module 1		3:30-5:00 pm	9:30-11:00 am	6:30-8:00 am	7:00-8:30 pm
Module 2		5:30-7:00 pm	11:30 am - 1:00 pm	8:30-10:00 am	9:00-10:30 pm
WEEK 1	***Module***				
DAY 1, Mon. June 9	1	Introduction to Block Ciphers; DES and AES			Christof Paar
	2	Lightweight Block Ciphers for RFIDs			Christof Paar
DAY 2, Tue. June 10	3	Public-Key Cryptography: Algorithms and Protocols			Çetin Koç
	4	Integer Arithmetic Algorithms and Architectures			Çetin Koç
DAY 3, Wed. June 11	5	Specialized Hardware for Secret-Key Algorithms			Ingrid Verbauwhede
	6	Introduction to PUFs (Physically Unclonable Functions)			Ingrid Verbauwhede
DAY 4, Thu. June 12	7	Finite Field Arithmetic Algorithms and Architectures			Çetin Koç
	8	Public-Key Cryptographic Hardware and Embedded Systems			Çetin Koç
DAY 5, Fri. June 13	9	Introduction to Side-Channel Analysis			Marc Joye
	10	Block Ciphers: Attacks and Countermeasures			Marc Joye
WEEK 2	***Module***				
DAY 6, Mon. June 16	11	Trusted Computing Architectures, SSL and IPSec			Pankaj Rohatgi
	12	Electromagnetic Attacks, Countermeasures and Advanced Analysis Techniques			Pankaj Rohatgi
DAY 7,Tue. June 17	13	RSA/ECC - Side Channel Attacks & Countermeasures			Marc Joye
	14	Post-Quantum Cryptography Algorithms			Francisco R.-Henríquez
DAY 8, Wed. June 18	15	Post-Quantum Cryptography Implementations			Francisco R.-Henríquez
	16	Fully Homomorphic Encryption			Marc Joye
DAY 9,Thu. June 19	17	Random Number Generators for Cryptographic Applications			Werner Schindler
	18	Evaluation Criteria Non-Deterministic Random Number Generators			Werner Schindler
DAY 10, Fri. June 20	19	Random Number Generator Design Constraints and Challenges			Viktor Fischer