



Cryptographic Engineering

ON-LINE CLASS by Microsoft TEAMS

May 31 - June 11, 2021

WEEK 1	MAY 31 - JUNE 4	10 Modules (1:30hr each), 2 Modules per day		
WEEK 2	JUNE 7-11	9 Modules (1:30hr each), 2 Modules per day, except on Friday 1 module		
DAILY	Central European Time	Eastern Standard Time	Pacific Standard Time	India Standard Time
	CET (Lausanne)	EST (New York)	PST (California)	IST (India)
Module 1	3:00-4:30 pm	9:00-10:30 am	6:00-7:30 am	7:30-9:00 pm
Module 2	5:00-6:30 pm	11:00 am -12:30 pm	8:00-9:30 am	9:30-11:00 pm
WEEK 1	Module			
Monday, May 31	1	Introduction to Block Ciphers; DES and AES		Christof Paar
	2	Lightweight Block Ciphers for RFIDs		Christof Paar
Tuesday, June 1	1	Specialized Hardware for Secret-Key Algorithms		Ingrid Verbauwhede
	2	Introduction to PUFs (Physically Unclonable Functions)		Ingrid Verbauwhede
Wednesday, June 2	1	Integer Arithmetic Algorithms and Architectures		Cetin Koc
	2	Finite Field Arithmetic Algorithms and Architectures		Cetin Koc
Thursday, June 3	1	Public-Key Cryptography: Algorithms and Protocols		Cetin Koc
	2	Public-Key Cryptographic Hardware and Embedded Systems		Cetin Koc
Friday, June 4	1	Trusted Computing Architectures, SSL and IPSec		Pankaj Rohatgi
	2	Introduction to Side-Channel Analysis		Marc Joye
WEEK 2	Module			
Monday, June 7	1	RSA - Side Channel Attacks & Countermeasures		Marc Joye
	2	Electromagnetic Attacks, Countermeasures & Advanced Analysis Techniques		Pankaj Rohatgi
Tuesday, June 8	1	ECC - Side Channel Attacks & Countermeasures		Marc Joye
	2	Implementations of Fully Homomorphic Encryption Methods		Cetin Koc
Wednesday, June 9	1	Side Channel Attacks to Block Ciphers: DES & AES		François-Xavier Standaert
	2	Countermeasures for Block Ciphers		François-Xavier Standaert
Thursday, June 10	1	Random Number Generators for Cryptographic Applications		Werner Schindler
	2	Evaluation Criteria Non-Deterministic Random Number Generators		Werner Schindler
Friday, June 11	1	Random Number Generator Design Constraints and Challenges		Viktor Fischer
	0.5	Course Evaluation		Vlado Valence, All