Tentative Time Table

	10:00-11:20	**11:35-12:55**	**14:30-15:50**	**16:05-17:25**
Mon Sept. 19	BSKP I (Somitra)	BSKP II (Debrup)	BSKP III (Debrup)	S/w implem. (Shay)
Tue Sept. 20	Basics of AE I (Palash)	Basics of AE II (Palash)	CAESAR & AE (Mridul)	Differential Fault analysis of Block Ciphers (Debdeep)
Wed Sept. 21	Leakage resilient AE (Donghoon)	Lightweight AE (Somitra)	CLOC & SILC (Kazuhiko)	ElmD and Trivia (Mridul)
Thu Sept 22.	DAE for Disk Encryption (Debrup)	GCM-SIV (Shay)	Research talk (Mridul)	Research talk (Kazuhiko)

BSKP Basic Symmetric Key Primitives
AE Authenticated Encryption

Tentative contents of the basic modules:

BSKP I	Basics of block and stream ciphers
BSKP II	Formal models for Block ciphers, stream ciphers, Modes for Encryption and Authentication.
BSKP III	Formal models for Block ciphers, stream ciphers, Modes for Encryption and Authentication.
Basics of AE	Basic security notions of AE, AEAD, DAE, DAEAD with examples.
CAESAR and Advanced AE	About CAESAR and different types of candidates. New attacks and new security models: Nonce misuse,taglength variability, INT-RUP.
Software Implementations	Software optimization of cryptographic algorithms for modern processors.
Hardware	Basics of Hardware, Fault attack of blockcipher/streamcipher, diagonal fault attacks
GCM-SIV	Recent development in AESGCM authenticated encryption optimization and deployments, and the nonce misuse resistant AESGCMSIV.