Tentative Time table.

	10:00-11:20	**11:35-12:55**	**14:30-15:50**	**16:05-15:25**
Mon Sept. 19	BSKP I (Somitra)	BSKP II (Debrup)	BSKP III (Debrup)	S/w implem. (Shay)
Tue Sept. 20	Basics of AE (Palash)	CAESAR (Mridul)	AE Advanced (Mridul)	Hardware (Debdeep)
Wed Sept. 21	CLOC-SILC (Kazuhiko)	Leakage Resilent AE (Donhoong)	Lightweight AE (Somitra)	ElmD and TriviA (Mridul)
Thu Sept 22.	Research Talk-I (Palash)	Research Talk-II (Debrup)	GCM-SIV (Shay)	Recent Advances of AE (Kazuhiko)

BSKP	Basic Symmetric Key Primitives
AE	Authenticated Encryption
RT	Research Talk (the research talks in the last two days would be on more advanced and recent topics, they are to be finalized.)

Tentative contents for 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, with examples. Soem Attacks on AE schemes.
CAESAR	About CAESAR and different types of candidates.
Advanced AE	New attacks and new security models: Nonce misuse, taglength variability, INT-RUP.
S/w implem.	Software optimization of cryptographic algorithms, for modern processor architectures.
Hardware/ Fault	Basics of Hardware, Fault attack of blockcipher/streamcipher, diagonal fault attacks/
GCM-SIV	Recent development in AES-GCM authenticated encryption optimization and deployments, and the nonce misuse resistant AES-GCM-SIV.