	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	AE I (Mridul)	AE II (Mridul)	AE III (Palash)	Hardware (Debdeep)
Wed Sept. 21	RT I (Minematsu)	RT II (Mridul)	RT III (Donhoong)	RT IV (Somitra)
Thu Sept 22.	RT V (Palash)	RT IV (Shay)	RT V (Minematsu)	

BSKP Basic Symmetric Key Primitives
AE Authenticated Encryption
RT Research Talk

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
AE I Basic notions of AE, AEAD, with examples
AE II Attacks on AE schemes, examples
AE III New attacks and new security models: Nonce misuse, taglength variability, INT-RUP

The research talks in the last two days would be on more advanced and recent topics, they are to be finalized with the input from the speakers.