

## TENTATIVE SCHEDULE

**National Instructional Workshop on Cryptology: Code-based Cryptography, July 05-07, 2023**  
Department of Mathematical Sciences, Indian Institute of Technology (Banaras Hindu University)  
Varanasi 221005

### **Day 1: Wednesday, 5<sup>th</sup> July 2023**

Venue: Annie Besant Lecture Theatre

Time	Event	Speaker	Topic
8:30 am – 9:25 am	Registration		
9:30 am – 10:00 am	Inaugural (ABLT-4)		
10:00 am – 10:30 am	High Tea		
10:30 am - 11:30 am	Key Note Lecture	RBL	
11:40 am - 12:40 pm	Lecture-1,	BMP	A study of Algebraic concepts
12:40 pm – 2:15 pm	Lunch Break		
2:15 pm –3:15 pm	Lecture-2	AJG	Introduction to Coding Theory
3:15 pm –4:15 pm	Lecture-3	MHN	Bounds on Codes
4:15 pm –4:30 pm	Tea Break		
4:30 pm –5:30 pm	Lecture-4	PSM	Introduction to Cryptography: Symmetric-key cryptosystems

RBL: Prof R Balasubramanian

BMP: Prof. (Rtd.) B.M. Pandeya, IIT(BHU)

MHN: Prof. Maheshanand, IIT Roorkee

AJG: Dr. A J Gupta, IIT(BHU)

PSM: Dr. Prasanna Mishra, SAG Lab DRDO

## TENTATIVE SCHEDULE

**National Instructional Workshop on Cryptology: Code-based Cryptography, July 05-07, 2023**  
Department of Mathematical Sciences, Indian Institute of Technology (Banaras Hindu University)  
Varanasi 221005

### **Day 2: Thursday, 6<sup>th</sup> July 2023**

Venue: Annie Besant Lecture Theatre (ABLT-1)

Time	Event	Speaker	Topic
9:00 am – 10:00 am	Lecture-5	OMP	Cyclic Codes
10:00 am – 11:00 am	Lecture-6	RKS	Public-key Cryptosystems
11:00 am – 11:15 am	Tea Break		
11:15 am – 12:15 pm	Lecture-7	BPS	Need for Post-Quantum Cryptography
12:15 pm - 01:15 pm	Lecture-8	BKB	Make it: How the Code-based Cryptosystems are Implemented
01:15 pm – 2:45 pm	Lunch Break		
2:45 pm – 3:45 pm	Lecture-9	BKB	Break it: Cryptanalysis of Code-based Schemes
3:45 pm – 4:00 pm	Tea Break		
4:00 pm – 5:00 pm	Lecture-10	BPS	Quantum-safe Journey with Bit Flipping Key Encapsulation Mechanism (BIKE)

RKS: Prof. R. K. Sharma, IIT Delhi

OMP: Prof. Om Prakash, IIT Patna

BPS: Dr. Bhupendra Singh, CAIR Lab DRDO

BKB: Dr. Bhaskar Biswas, IIIT Kalyani

DSB: Dr. Debashish Bera, IIIT Kalyani

## TENTATIVE SCHEDULE

**National Instructional Workshop on Cryptology: Code-based Cryptography, July 05-07, 2023**  
Department of Mathematical Sciences, Indian Institute of Technology (Banaras Hindu University)  
Varanasi-221005

### **Day 3: Friday, 7<sup>th</sup> July 2023**

Venue: Annie Besant Lecture Theatre (ABLT-1)

Time	Event	Speaker	Topic
9:00 am – 10:00 am	Lecture-11	DSB	Code-based Encryption Scheme
10:00 am – 11:00 am	Lecture-12	DSB	Code-based Signature Scheme
11:00 am – 11:15 am	Tea Break		
11:15 am – 12:15 pm	Lecture-13	SDG	Linear Feedback Shift Registers (LFSR): Basics and Beyond
12:15 pm - 01:15 pm	Lecture-14	IDG	Overview of Post-Quantum Cryptography
01:15 pm – 2:45 pm	Lunch Break		
2:45 pm – 3:45 pm	Lecture-15	OSB	Non-malleable Codes and Secret Sharing Schemes
3:45 pm	Valedictory		
	High Tea		

SDG: Prof. Sudhir Ghorpade, IIT Bombay

IDG: Dr. Indivar Gupta, SAG Lab DRDO

BPS: Dr. Bhupendra Singh, CAIR Lab DRDO

DSB: Dr. Debashish Bera, IIIT Kalyani

OSB: Dr. O S L Bhavana, IIT(BHU)