

JUNE

07

Thursday  
CSES40

## RESEARCH IN INFORMATION SECURITY

4.8.2020

2018

Week 23

158-207

9 TAUGHT BY

- 10 • prof. ashok kumar das

11

### COURSE TOPICS

12

- 1 • elliptic-curve cryptography (ECC)

- 2 • Key management in hierarchical access control

- 3 • lightweight security protocols for wearable devices

- 4 • Security protocols for implantable medical devices

- 5 • Key management in wireless sensor networks

- 6 • user authentication in wireless sensor networks

- 7 • user access control in wireless sensor networks

- access control in wireless sensor networks and wireless body area sensor networks

- proxy signature

- password based remote user authentication and key agreement using smart cards

JUN  
2018

S M T W T F S  
\* \* \* \* \* 1 2

S M T W T F S  
3 4 5 6 7 8 9

S M T W T F S  
10 11 12 13 14 15 16

S M T W T F S  
17 18 19 20 21 22 23

S M T W T F S  
24 25 26 27 28 29 30

2018

Week 23  
159-206

Friday

4.8.2020  
2 JUNE

08

• biometric-based remote user authentication and key management using smart cards.

• Security in vehicular ad-hoc networks.

• Security in smart grid

• Security in cloud computing

• intrusion detection in wireless network security.

### TEXT BOOKS

1. any compiler book for dataflow analysis.

2. assembly book for x86.

3. practical malware analysis; sikorski.