4.8.2020

CSE418

PRINCIPLES OF INFORMATION SECURITY

9 TAUGHT BY

10
- prof. srinathan kannan

11

COURSE TOPICS

12

- classical cryptography and their cryptanalysis

1

- perfect secrecy

2

- shannon's theorem

3

- pseudorandom generators

4

- stream ciphers

5

- CPA-secure encryption

6

- pseudorandom permutations

7

- practical block ciphers (3-DES, AES)
- modes of operation
- MACs
- hash functions

MAY 2018	S	M	T	W	T	F	S
	*	*	1	2	3	4	5
	6	7	8	9	10	11	12
	13	14	15	16	17	18	19
	20	21	22	23	24	25	26
	27	28	29	30	31	*	*

4.8.2020

2018 — 2 MAY

Week 20
135-230

Tuesday 15

- CCA-secure encryption

9

- diffie-hellman key exchange

10

- public-key cryptosystems

11

  - RSA

12

  ~~el gamall~~

  - el gamal

1

  - pailler

2

  - rabin

3

  - goldwasser-micali

4

- PKCS v 1.5

5

- digital signatures

6

- DSS

7

- digital certificates and PKI
- basic cryptography protocols
- oblivious transfer
- secret sharing

JUN
2018

S	M	T	W	T	F	S
*	*	*	*	*	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

JUNE JULY AUGUST

MAY

16 Wednesday

4.8.2020
3

2018

Week 20
136-229

- byzantine agreement

9

- secure multi-party computation

10

- interactive proof systems

11

- cryptography in noisy channels

12

- quantum cryptography

1

2 TEXTBOOK

3 1. introduction to modern cryptography; lindell.

4 2. foundations of modern cryptography; goldreich. (2001)

5 3. handbook of applied cryptography; menezes. (1996)

6

7

MAY
2018

S	M	T	W	T	F	S
*	*	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31	*	*