10/11/22. Revision sheet:- Short Answer, objective style:-

(1.) Some plaintext translates into same way if we don't randomize the initial value. (For example see notes)

(2.) Slide.NO: 20, 21 (Crypto Overview → First two lines)

(3.)

(4.) Crypto Primitives I → Slide. No: 8.

(5.) Notions of security II → Slide. NO: 287 (diagram ☆)
(CPA & CCA)

(5a) CPA games for — CBC, OFB, CTR (Block Cipher → Slide. NO: 9)

(6.) Crypto primitives I → Slide. NO: 17 & 18.

(7.) 4 Modes → ECB, CBC, OFB, CTR (in Block Cipher)
(diagram ☆)

(8.) ECB & CTR are parallizable, OFB is partially parallizable & CBC is not parallizable.

(9.) Notions of security II → Slide. NO: 3 (bottom of the slide)

(10.) DES → Slide. NO: 3.

(11.) DES → Slide. NO: 6, 7 & 8.

(12.) DES → Slide. NO: 13 (bottom of the Slide) &
Slide. NO: 15 &
Slide. NO: 17 (Top of the slide)

13. DES → slide no: 15 & 16 (see the notes as well.)

14. DES → slide no: 14 & 16 (see the class notes as well)

15. DES → slide no: 22

Problems:-

1. No. of

2. Num Theory IV → slide no: 15 & 17 & 19 (use 19th slide Formula to solve.) (not imp).

3. Num Theory I → slide no: 12 (Modulo multiplication) & slide no: 13

↓

(Properties - 5, 6 & 7 in module Arithmetic Properties)

4. Num Theory II → slide no: 7 (Group Order Rule)

↓

(a should be a member of the group.)

8. Num theory III → slide no: 13, 15 & 16.