11/29/22: Calculators are allowed.

(No Num Theory - V slides. ✗ Just know the names of the Int Fact-& -ring last slide. No: 23.)

1 to 3 PM Tuesday

30% objective → (10 Points Matching, 15 Points Fill in the blanks)

Short Answer Questions (or) Fill in the blanks:-

1) FLT (Terminology (Carmichael numbers) & Some proof + Sign up) Num Theory 3 - Slide. No: 19, 20, 21.

2) Miller Rabin (Attempt No 3) Num Theory 3 - Slide No: 22 & notes.

3) Num Theory 4 - Slide. No: 5, 6, 7, 8, 9, 10 (Just need to know what each does.)

4) Num Theory 5 - Slide. No: 2 & 23. Factoring names. → Just be familiar with integer

5) Num Theory 5 - Slide. No: 20, 21 (Time complexities) (not Imp)

★ Pohlig Hellman works for composite order group not for prime order group.

★ Baby-step-Giant-step works for prime order group.

6) DSA, RSA - $\mathbb{Z}_n^*$; ElGamal, Schnorr Signature Schemes. Public key Crypto II - Slide. No: 1, 2, 3.

Signatures - Slide. No: 21, 26 (in diagram, $m \in \{0,1\}^*$)

7) Public key Crypto II - Slide. No: 8, 9, 10.

8) Signatures - Slide. No: 4.

9.) Signature — Slide.No: 9 (It is already given in descending order in the slide.)

10.) Signature — slide.no: 11.

11.) Signature — slide.no: 13. (Malleability attack).

12.) Signature — slide.no: 27, 28.

13.) How Lamport signature works?

Signature — Slide.No: 32, 33, 34, 35, 36.

* If the message is 'n' bits then the vector containing 'n' bits is '2n' elements.

14.) Signature — slide.no: 38; 39, 40, 41, 42, 43.

15.) Signature — slide.no: 46 to 51. (Also see the notes)

16.) Signature — slide.no: 55 (objective style question)

17.) Signature — slide.no: 53, 58.

18.) HashFunctions — slide.no: 5, 6.

19.) Small-space-birthday attack — slide.no: 20, 21 (Also see the notes) (Possible problems)

20.) Hash Function — slide.no: 22, 23, 24, 27 (Naive way Time complexities) (objective style question.)

21) Hash Function — Slide no: 32 (First two differences)

22) Hash Function — Slide no: 41.

Problems:

(1) FLT — Assignment 4.

(2) Finding Generators, subgroups — Assignment 4. (Problem 1)

(3) Find $x^y \bmod n$ — we can use group order rule, CRT. (Assignment — 4 & 5)

(4) (See question 19 from above)

(5) Num Theory Final set of problems slides.

(6) Lamport Signature Scheme:

Given, $M = 101111$.

$H: \{0,1\}^* \rightarrow \{0,1\}^{128}$.

$|x_{i,j}| = 64$ bits.

$$SK = \begin{Bmatrix} x_{10}, x_{20}, \ldots, x_{60} \\ x_{11}, x_{21}, \ldots, x_{61} \end{Bmatrix}$$

$|SK| = 12 * 64$.

$$P_K = \begin{Bmatrix} y_{10}, y_{20}, \cdots, y_{60} \\ y_4, y_{21}, \cdots, y_{61} \end{Bmatrix}$$

$|P_K| = 128 \times 12.$

$$\sigma = (x_{11}, x_{20}, x_{31}, x_{41}, x_{51}, x_{61})$$

$|\sigma| = 6 \times 64.$

$\sigma, P_K = 6 \times 64 + 128 \times 12.$

verification:

If $t(x_{11}) \stackrel{?}{=} y_{11}$

If $t(x_{61}) \stackrel{?}{=} y_{61}$ } 6.

7. RSA Problem — see Assign 4.

8. ElGamal Encryption Problem — see Assign 5.

Small-Space Birthday Attack :-

Ex:- (For slide no: 21 (Applying Result step))

- Say, $x_3 = x_6$

  collision space $(x_0, \cdots, x_5)$

- $i = 3, 2i = 6$

  Find j, s.t, $x_j = x_{3+j}$.

then $T = 3$.

- output,

  $(x = 2, 85)$

  "colliding".