CS 380/525: Intro to Crypto
Fall 2022
Final Review

November 19, 2022

The final will be mainly problems and objective questions, (fill in the blank, and/or match the column), and maybe a short-answer question or two. The purpose of this review sheet is to give you an idea of the kind of questions you can expect to see on the final exam, but this isn't an exhaustive list of questions for the exam. Syllabus is:

1. Everything starting from "numTheoryIII.pdf" up until and including "hashFunctions.pdf".
2. For numberTheoryV – just make sure you're familiar with the first couple of slides, and the last slide with the table and numbers.

Where to read from: Please read from the slides, and the class written notes (for problems) and assignments. Calculators are permitted during the exam. *Please get your calculators – I won't be providing them!*

Conceptual/analytical/fact-based questions: Some of these can also be fill-in-the-blank questions and/or match-the-column questions.

1. Be familiar with Fermat's little theorem and related primality-testing terminology (Carmichael, strong liar, strong witness, etc.).
2. Be familiar with Miller-Rabin primality testing.
3. Know CDH/DDH/DL.
4. Be familiar with integer factorization algorithms (just names).
5. Be familiar with time complexities of Pohlig-Hellman, Baby-step-giant-step.
6. What are the message/ciphertext.signature spaces for RSA, ElGamal, DSA, Schnorr?
7. Setup Charlie's keys in Diffie-Hellman man-in-the-middle attack.
8. Point out a few differences between signatures and MACs.
9. What are 4 types of signature forgeability? Arrange them in descending order of level of security. Which is the strongest level?
10. What properties do we want a hash-and-sign signature scheme to have?
11. Why are RSA signature malleable? Show a simple attack.
12. Describe two attacks on DSA (both relate to bad choices for $k \leftarrow \mathbb{Z}_q^*$). Why do they work?

13. Simple Lamport-based question: what is $|SK|, |PK|, |\sigma|$ for an $|m| = n$ bits, and an $H : \{0,1\}^* \rightarrow \{0,1\}^{128}$? Assume $|x_{i,j}|$ is, say, 64 bits.

14. Be able to write a sentence each on the 4 kinds of PKI.

15. Write sender/receiver expressions for two kinds of signcryption (encrypt-then-authenticate, authenticate-then-encrypt) – with the fixes, of course.

16. What are the necessary and sufficient properties of a group signature scheme?

17. Be familiar with the basic group sig. definition. Possible extension-type question: How would you extend the basic definition to support POW, in case of corrupt group managers? Only function prototype is needed. (Just add a POW with every group manager output, don't forget to verify the POW.)

18. 3 properties of hash function, and implications – which ones we get "for free"?

19. Small-space birthday attack – given $x_i = x_j$, what is the collision-output? Write out the sequence of $x_1, \cdots, x_{2^{(l/2)+1}}$. You'll be given l. Just need to know the formula for this.

20. Time-complexities of Naïve way, Smart-way-1, Smart-way-2 algorithms for hash inversion.

21. What are 2 differences between random oracle model H and real-world hash function, H'?

22. Possible Merkle hash-tree question: given a tree with n leaves, write expressions for all internal nodes.

Problems:

1. Find witnesses that n is not prime using Fermat's little theorem, also strong liars. E.g., Find witnesses in $\mathbb{Z}_8^*$, verify 50% rule, etc. (see assign 3).

2. Finding generators of some group $\mathbb{Z}_N^*$, finding prime-order subgroups in a composite-order group, verifying every element of a prime order subgroup is a generator (not using formula), and related stuff (see assignment 4).

3. Find $x^y \bmod n$ using any method you see fit. You'll are experts at this by now. Some options:
   (a) Chinese remainder theorem – won't work if n is prime.
   (b) Group-order-trick – won't help if $y < |\mathbb{Z}_n^*|$.
   (c) Square-and-multiply. Will work in general-case, but more work than previous two.

4. Assume a cyclic $H : \{0,1\}^* \rightarrow \{0,1\}^7$. Mark *all* possible outputs of H on the circumference. Standard segment-size is $\sqrt{N}$.

   Use "Smart-way 2" hash inversion algorithm. $l = 7$. Set $N = 2^7$; take $\lfloor \sqrt{N} \rfloor = 11$. Then use $(x_{i \cdot \sqrt{N}}, x_{(i+1) \cdot \sqrt{N}})$ to find start/end points.

5. Pohlig-Hellman, Baby-step-giant-step problems: Find $x = log_g h \bmod n$, given g, h in $\mathbb{Z}_n^*$ (see assign 5).

6. Lamport signatures: For an n-bit M (e.g., 101111), $H : \{0,1\}^* \rightarrow \{0,1\}^{128}, |x_{i,j}| = 64$ bits, write the SK, PK, σ vectors, along with their sizes. How many bits of info. need to be transmitted to the verifier? Do not forget verifier needs to know PK. Show the computation/checks on the verifier's side.

7. RSA problem: given p, q, e, M, find C. Decrypt C and verify you get M back. Main challenge here is finding d, s.t., $d \cdot e \equiv 1 \bmod \phi(n)$ (see assign 4).

8. ElGamal encryption problem: given $\mathbb{G}, g, q$, and an $m \in \mathbb{G}$, set up PK, SK – there could be multiple choices for SK, all should work. Compute C, then decrypt it and verify you get m back. (see assign 5)