Fall 2022 2022-10-07

Midterm Review Sheet

Roopa Vishwanathan *CS 380/525: Intro to Crypto*

The purpose of this review sheet is to give you an idea of the kind of questions you can expect to see on the midterm, but this isn't an exhaustive list of questions for the exam.

Type of questions: Exam will consist of short-answer questions, and a few objective-style questions. Some of these can also be fill-in-the-blank questions or match-the-column questions. No calculators/electronic devices permitted.
How to prepare: Please use the slides and class notes as reading material. Also, read through assignments and their solutions.
Slide sets: All slide sets until and including numberTheoryIII.pdf. In numberTheoryIII.pdf, only Chinese Remainder Theorem is included in midterm syllabus, i.e., slides 11-16. You can ignore the rest of numberTheoryIII.pdf for the midterm.

1. Why is deterministic encryption bad? Explain with an example (see written notes for the grading example).

2. Be familiar with standard/recommended key lengths (shared-key and PKC).

3. Properties each primitive provides – encryption: confidentiality, mac: integrity/authenticity sigs: integrity (with hash)/authenticity, hash: integrity/compression.

4. Give 2 reasons as to why poly/mono-alphabetic ciphers like Caesar, Vigenere ciphers are not used in practice.

5. Be familiar with basic structure of CPA/CCA (notions of security II slides, don't worry about the games, just be familiar with the figures).

   (a) Stateful vs. stateless CPA games for CBC/OFB/CTR modes (see assignment 2 solutions).

6. Difference between computational security vs. information-theoretic, a.k.a., *perfect* security?

7. Make sure you know how the 4 modes (ECB, CBC, OFB, CTR) work, at least for encryption.

8. Which modes are fully parallelizable, which are semi-parallelizable, which are non-parallelizable?

9. What is the minimum security requirement that an encryption algorithm needs to meet to be considered practically usable?

10. Shannon used the terms *diffusion* and *confusion* to describe the relationship between plaintexts, ciphertexts and keys. What do these terms mean?

11. Give 5 metrics for evaluating block ciphers.

12. Make sure you know how ciphertexts are generated in 2DES, 3DES, DESX (the equations).

13. In 3DES, what possible equalities could exist between K_1, K_2, K_3? Effective security w.r.t. key-length? (see class written notes.)

14. What specific property of 2DES makes it vulnerable to a meet-in-the-middle attack? What does an attacker need to be provided for this attack (see table and class written notes)? Same strategy can be extrapolated to 3DES too (Merkle-Hellman attack) but is considered infeasible. Why?

15. What assumptions does symmetric-key crypto rely on? What kind of security guarantees does it offer? (look at last slide of DES slide set.)

Problems (no calculators permitted):

1. Possible simple encryption mode problem: x bits of data gets encrypted, with block-size y, and key size z (all in bits) in some mode. What will be size of ciphertext(s) block(s)? Make sure to account for padding, if required.

2. Finding prime-order subgroups in a composite-order group, verifying them, and related stuff (see assignment 3).

3. Modular arithmetic problems: find $(x_1 \cdots x_n) \mod y$, or $x^{5000} \mod n$ (see number theory part I, slide 12, 13).

4. Group theory problems – order-rule (see number theory part II, slide 7, and assignment 3). If $\mathbb{G}$ is a group, $|\mathbb{G}|$ = n, then for all $a \in \mathbb{G}$, $a^y \bmod n = a^{y \bmod x} \bmod n$, for any $y \geq 1$. Note that this only works if $y \geq x$, e.g., won't help for $a^{50 \bmod 90} \bmod n$.

5. Finding $d = gcd(a, b)$ using Euclidean algorithm, and integers x, y, s.t., $d = ax + by$, using extended Euclid (see assign 2).

6. Find multiplicative inverse of $\mathbb{Z}_x$, or a (single) inverse, e.g., inverse of $x \mod n$, where $x, n \in \mathbb{Z}^+$ (see assign 2).

7. Find polynomials in $GF(x^y)$ (see assign 2).

8. Chinese remainder theorem problems. CRT usually applicable when N can broken up into primes p, q, else use other modulo properties.

   (a) Verify $\mathbb{Z}_N^* \simeq \mathbb{Z}_p^* \times \mathbb{Z}_q^*$, for some $N, p, q \in \mathbb{Z}^+$.

   (b) E.g., find $12^{50000} \bmod 55$.