Spring 2022 March 11, 2022

Midterm review sheet

Instructor: Roopa Vishwanathan *CS 478/513: Computer Security*

Syllabus, study material, etc.: The syllabus for the midterm is CS1-CS7, both inclusive, i.e., everything until hash functions. Please use the slides, class notes, written assignments and their posted solutions as study material. For the topic of signcryption, please read from the posted "signcryption.pdf", instead of the regular slides.

Exam will consist of mostly short-answer questions, objective-style questions, and a few problems. 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. Calculators are permitted, please get your own. Exams need to be written with pens, although you can use pencils for scratch work.

Questions:

1. What are 3 main goals of computer security?
2. Key-spaces for simple substitution ciphers: when shifted by a fixed value? When any permutation of alphabets? (see assignment 1)
3. Possible problem on double (matrix) transposition: given a plaintext P, create a key K, and ciphertext C.
4. What are the disadvantages of using a one-time pad?
5. Define confusion and diffusion.
6. What are the different kinds of cryptanalysis? What is the minimum requirement any encryption algorithm needs to satisfy?
7. What is the difference between stream cipher and block ciphers? Examples of both?
8. Be familiar with working of A5/1 stream cipher. Possible problem, maybe for a 1-2 register-steps (see assignment 2).
9. Problem on Feistel ciphers (see assignment 2, last problem).
10. DES block length, key length, no. of rounds – possible objective-style question.
11. How would you do an S-box lookup for DES on say, an input 100101? Or an S-box lookup in AES on input 01001100?
12. Why is double DES insecure? Explain with example. (see class notes for an example, and assignment 2 for another).
13. Key-length of 3DES? Key-length options, block-length options, no. of rounds corresponding to key sizes of AES – possible objective-style question (see class notes).

14. What is the weakness of ECB mode of block ciphers? Example? (see class notes.)
15. How does CBC mode work? Explain with example or diagram. Why does CBC decryption not suffer from propagation errors?
16. What is the advantage of CTR mode over ECB and CBC?
17. What security property do MACs provide? How?
18. Why does CBC-MAC suffer from propagation errors?
19. Difference between public-key crypto and shared-key crypto.
20. What properties does public-key crypto provide?
21. Possible RSA problem: given plaintext P, e, prime numbers p, q, compute ciphertext C. Decrypt C and verify you get plaintext P back.
22. What are the two kinds of signcryption? What are attacks possible, and how to fix them?
23. What are the 3 kinds of PKI trust models?