Preparing for Midterm #1

MATH 481/581 — Cryptography
Wednesday, Feb 26

Please print your name:

Problem 1.

(a) Do the practice problems that were compiled from the examples from lectures. (Solutions to these can be found in the corresponding lecture sketches.) In particular, fill in all the conceptual empty boxes. To save time, you don't need to work through all details. However, make sure that you know how to do each problem.

(b) A collection of online homework questions that are particularly relevant for the midterm is posted on our website. (Recall that redoing problems can never hurt your scores.)

(c) Do the problems below. (Solutions are posted separately.)

Bonus challenge. Let me know about any typos you spot in the posted solutions (or lecture sketches). Any typo, that is not yet fixed by the time you send it to me, is worth a bonus point.

Problem 2. Eve intercepts the ciphertext $c = (1111\ 1011\ 0000)_2$ from Alice to Bob. She knows that the plaintext begins with $m = (1100\ 0\ldots)_2$.

(a) Eve suspects that a stream cipher with PRG $x_{n+1} \equiv 5x_n + 1 \pmod{16}$ was used for encryption. If that's the case, break the cipher and determine the plaintext. What is your verdict on Eve's suspicion?

(b) On second thought, Eve thinks a stream cipher using a LFSR with $x_{n+3} \equiv x_{n+2} + x_n \pmod{2}$ was used. If that's the case, what would be the plaintext?

(c) If a nonce was used, how would that affect Eve's attack?

(d) What should Alice learn from this? (Obviously, apart from the fact that the key space is too small.)

Problem 3.

(a) Evaluate $850^{6677} \pmod{77}$.

(b) Evaluate $100^{7300} \pmod{91}$.

(c) Determine all solutions to $x^2 \equiv 9 \pmod{91}$.

Problem 4.

(a) Using the Chinese remainder theorem, solve $x \equiv 3 \pmod{4}$, $x \equiv 1 \pmod{7}$, $x \equiv 2 \pmod{11}$.

(b) Using the Chinese remainder theorem, find all solutions to $x^3 \equiv 1 \pmod{70}$.

(c) Determine the number of solutions to $x^3 \equiv 1 \pmod{182}$.

If you wish additional practice using the CRT, find all (or just a select few) solutions.

Problem 5.

(a) When using a stream cipher, why must we not use the same keystream a second time?

(b) Explain how a nonce makes it possible to use the same key in a stream cipher multiple times.

(c) During a conversation you hear the statement that "the one-time pad is perfectly secure". What is your reaction?

(d) Your company is implementing measures for secure internal communication. As part of that, a random secret key is to be generated for each employee. A colleague says: "That's easy, let me do it! Java has a built-in class called `Random`. It shouldn't be more than a few lines of code." What is your reaction?

(e) We observed that many programming languages use linear congruential generators when producing pseudorandom numbers. If these are predictable, why are they still used?

Problem 6.

(a) If you can only do a single modular computation, how would you check whether a huge randomly selected number N is prime or not?

(b) Which flaw of the Fermat primality test renders it unsuitable as a general primality test? How can this flaw be fixed?

(c) Despite the flaw in the previous item, in which scenario is it fine to use the Fermat primality test regardless?

(d) We want to use the Miller–Rabin primality test to decide whether $N=377$ is prime. Each time, we randomly choose a base a (and only do a single iteration of Miller–Rabin) and compute the following:

- $a=12$: $12^{47}\equiv 220$, $12^{94}\equiv 144$, $12^{188}\equiv 1$, $12^{376}\equiv 1 \pmod{377}$
- $a=70$: $70^{47}\equiv 307$, $70^{94}\equiv 376$, $70^{188}\equiv 1$, $70^{376}\equiv 1 \pmod{377}$
- $a=80$: $80^{47}\equiv 332$, $80^{94}\equiv 140$, $80^{188}\equiv 373$, $80^{376}\equiv 16 \pmod{377}$
- $a=233$: $233^{47}\equiv 233$, $233^{94}\equiv 1$, $233^{188}\equiv 1$, $233^{376}\equiv 1 \pmod{377}$

In each case, what do we conclude? (Also point out which calculations were unnecessary.) Which of the a are strong liars? Which are Fermat liars?

(e) Repeat the previous problem for $N=247$ and the following computations:

- $a=12$: $12^{123}\equiv 246$, $12^{246}\equiv 1 \pmod{247}$
- $a=17$: $17^{123}\equiv 64$, $17^{246}\equiv 144 \pmod{247}$
- $a=27$: $27^{123}\equiv 170$, $27^{246}\equiv 1 \pmod{247}$
- $a=68$: $68^{123}\equiv 1$, $68^{246}\equiv 1 \pmod{247}$

Problem 7.

(a) Express 123 in base 2 (and then in base 7).

(b) Predict the number of solutions to $x^2\equiv 4 \pmod{1001}$.

(c) After how many terms must the LFSR $x_{n+7}\equiv x_{n+3}+x_n \pmod{2}$ repeat?