

Preparing for Midterm #1

MATH 481/581 — Cryptography
Wednesday, Feb 22

Please print your name:

Problem 1.

- (a) Retake all three quizzes. (Solutions to these are posted, too.)
- (b) 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.
- (c) Do the problems below. (Solutions will be posted soon.)

Bonus challenge. Let me know about any typos you spot in the posted solutions (surely, there should be some). Any typo that is not yet fixed on our course website by the time you send it to me, is worth a small bonus.

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

- (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 the multiplicative order of 9 $\pmod{91}$.
- (d) Determine all solutions to $x^2 \equiv 9 \pmod{91}$. Before doing so, what can you predict about the multiplicative order of these solutions? Afterwards, check your prediction.

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 pseudo-random numbers. If these are predictable, why are they still used?

Problem 6.

- (a) If x is a primitive root modulo n , what is the multiplicative order of x^a ?
- (b) Express 123 in base 2 (and then in base 7).
- (c) Predict the number of solutions to $x^2 \equiv 4 \pmod{1001}$.
- (d) After how many terms must the LFSR $x_{n+7} \equiv x_{n+3} + x_n \pmod{2}$ repeat?