CMSC 28400: Introduction to Cryptography, Autumn 2021
University of Chicago
Course Staff: Akshima, David Cash (instructor), Andrew Chu, Alex Hoover

Problem Set 1

Due in Thursday, October 7 at 11:59pm

Collaboration policy. Please respect the following collaboration policy: You may discuss problems together in groups of up to four *but you must write up your own solutions. You should never see your collaborators' papers or code.* At the beginning of your submission, indicate the names of your (1, 2, or 3) collaborators, if any. You may switch groups between problem sets but not within the same problem set.

Sources. Cite any sources you use. Citing lecture, providing readings, or the other free textbooks linked from the course syllabus webpage is allowed. You may use results proved in those sources or in lecture without repeating their proofs. Using Google, Chegg, or searching for posted solutions from other universities, is not allowed.

Grading. Responses to theory problems will be graded for correctness, precision, *and clarity.* Simple, well-explained proofs are preferred. Point values of problems vary, and are listed. You are encouraged to ask for help and advice from the staff in writing up your solutions.

Submitting your solutions. Solutions will be accepted on Gradescope. Check Campuswire for instructions.

You may submit well-lit, clear photographs of handwritten solutions. You may also type up your solutions by modifying the included tex file – The course staff will be happy to provide support if you choose to learn the Latex typesetting language.

---

1. **(25 pts)** Warm-up: Let $\Sigma = \{1, 2, 3, 4, 5, 6\}$, and let π and σ be permutations on Σ defined by

$$\begin{array}{c|cccccc} x & 1 & 2 & 3 & 4 & 5 & 6 \\ \hline \pi(x) & 4 & 2 & 1 & 6 & 3 & 5 \end{array} \quad \text{and} \quad \begin{array}{c|cccccc} x & 1 & 2 & 3 & 4 & 5 & 6 \\ \hline \sigma(x) & 3 & 6 & 1 & 2 & 4 & 5 \end{array}.$$

For each part here, you don't need to show any work.

- Write each of π and σ as products of disjoint cycles.
- Find π^{-1} and σ^{-1}, written as products of disjoint cycles.
- Find $\pi\sigma$ and $\sigma\pi$, written as products of disjoint cycles.

2. **(50 pts)** Define the *order of a permutation* π to be the minimum $k \geq 1$ such that π^k is the identity, where π^k means π composed with itself k times.

(a) Find the order of a cycle $(a_1\ a_2\ \cdots\ a_t)$. (Explain.)

(b) Find the order of an arbitrary permutation π in terms of its type. (Explain.)

3. **(50 pts)** Find the inverse of a cycle $(a_1\ a_2\ \cdots\ a_t)$. Use this (or another approach if you prefer) to prove that π^{-1} has the same type as π.

4. **(25 pts)** We have seen that there is a one-to-one correspondence between permutations π on a set Σ and cycle-partition graphs G_π on the vertex set $V = \Sigma$. Consider now directed graphs on $V = \Sigma$ that correspond to arbitrary functions $f : \Sigma \to \Sigma$ (as before, for each $x \in \Sigma$ there is a directed edge from x to $f(x)$).

   The components of G_f will not be directed cycles when f is not a permutation, but they cannot be arbitrary directed graphs either. Give a description of the components of G_f. [You don't need to prove your answer here; a one-sentence description is fine.]

   We will see more of the graphs G_f later in the course.

5. **(50 pts)** Rejewski states that the number of reflector permutations on a set Σ of size 26 is

$$\frac{26!}{2^{13}13!}.$$

   Prove this formula by explaining how it counts these permutations.