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

Problem Set 2

Due in Thursday, October 14 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. **(50 pts)** The n-bit one-time pad OTP_n may select the key $k = 0^n$ (meaning the string of n zeros), in which case encryption simply outputs the message m without changing it. A natural suggestion is to modify the scheme so that the key is never set to 0^n. To avoid having fewer keys than messages, we also need to remove a message; Say we take out $m = 0^n$ as well.

   More formally, define $\mathcal{K}' = \mathcal{M}' = \{0,1\}^n \setminus \{0^n\}$, $\mathcal{C} = \{0,1\}^n$, and $\mathrm{OTP}'_n : \mathcal{K}' \times \mathcal{M}' \to \mathcal{C}$ by $\mathrm{OTP}'_n(k,m) = k \oplus m$.

   Prove that OTP'_n is not perfectly secret.

2. **(75 pts)** Fix some positive integer n. Let $\mathcal{K}$ be the set of all permutations on $\{1,\ldots,2n\}$. Let $\mathcal{M} = \{0,1\}^n$, and $\mathcal{C} = \{0,1\}^{2n}$.

   For a bit-string $m \in \{0,1\}^n$, we write $\overline{m}$ for its *bit-wise complement*, i.e. m but with all of its bits flipped. So for example $\overline{0100} = 1011$. We write m_i for the i-th bit of m.

   Define $E : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$ as follows. It takes as input a key $\pi \in \mathcal{K}$ and $m \in \mathcal{M}$, and performs the following:

(a) Let $r = m \| \overline{m}$, where $\|$ denotes string concatenation. Thus r is $2n$ bits long.

(b) Define $c = r_{\pi(1)} r_{\pi(2)} \cdots r_{\pi(2n)}$. Thus c is also $2n$ bits long, and is equal to r but with its bits permuted according to π in the indicated manner.

(c) Output c.

Prove that E is perfectly secret.

3. **(100 pts)** Prove that a cipher $E : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$ is perfectly secret if and only if it has independent ciphertexts.

4. **(100 pts)** Consider the following definition:

Definition 1. *Let $E : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$ be a cipher and let $\mathbf{K}$ be a uniform random variable on $\mathcal{K}$. We say that E has* uniform ciphertexts *if the following holds: For every random variable $\mathbf{M}$ on $\mathcal{M}$ that is independent of $\mathbf{K}$, the random variable $\mathbf{C} = E(\mathbf{K}, \mathbf{M})$ is uniform on $\mathcal{C}$.*

Prove or disprove the following:

(a) If E is perfectly secret then it has uniform ciphertexts.

(b) If E has uniform ciphertexts then it is perfectly secret.