COMS BC3262 January 26, 2026

Problem Set 1

Instructor: Eysa Lee *Due: February 5, 2026*

Guidelines. Solutions will be graded for correctness and clarity. If you do not know how to solve a problem, you may write **"I don't know how to do this"** to receive 25% credit for any problem not marked as extra credit.

Collaboration. You are allowed to discuss problems with other students. However, you should write up your solutions on your own and may not read or copy the solutions of others. You should try solving each problem on your own before discussing with others. **If you work with others on a problem, you must note with whom you discussed the problem at the beginning of your solution write-up.** For example, "I discussed Problem 1 with Alice and Bob and Problem 2 with Carol." You may not use external resources apart from the recommended textbooks.

Generative AI Policy. The use of generative AI for anything related to assignments is prohibited in this class. **It is always prohibited to input any substantial portion of any assignment into any AI resource.** It is also always forbidden to incorporate any substantive portion of an AI resource's output into your answers, even if you paraphrase it or rewrite it in your own words.

Problem 1 (Negligible Functions) 5 points

Prove that if p is a polynomial and μ is a negligible function, then their product $f = p \cdot \mu$ (defined by $f(n) = p(n) \cdot \mu(n)$) is also negligible.

Problem 2 (Variant of the One-Time Pad) 5 points

Let q be prime. Suppose we want to use one-time pad over the group of integers mod q (i.e., $\{0, 1, \ldots, q-1\}$). If the key happens to be $k = 0$, then $\mathsf{Enc}(k, m) = k + m = m$. In other words, the ciphertext is equal to the message! Maybe, we should choose the key uniformly at random over all the **non-zero** elements to make sure we never select $k = 0$ so that the above does not happen. Is this suggestion a good idea? Explain why or why not.

Problem 3 (Encryption Schemes with $|\mathcal{K}| = |\mathcal{M}|$) 5 points

For the below statement, clearly state if you are proving or refuting. To prove the claim, justify every step and, if needed, write down definitions/theorems that were presented in class and that you rely on. To refute, provide a counterexample and show that it does not satisfy the required definition.

Prove or Refute: Every encryption scheme for which the size of the key space equals the size of the message space, and for which the key is chosen uniformly from the key space, is perfectly secret.

Problem 4 (Two-time Security?) 10 points

Part A: Here is a natural way to define perfectly secret encryption for two messages. For any two pairs of messages $(m_0, m_1) \in \mathcal{M}^2$ and $(m'_0, m'_1) \in \mathcal{M}^2$ and for any ciphertexts c_0, c_1 we have

$$\Pr[\mathsf{Enc}(K, m_0) = c_0 \wedge \mathsf{Enc}(K, m_1) = c_1] = \Pr[\mathsf{Enc}(K, m'_0) = c_0 \wedge \mathsf{Enc}(K, m'_1) = c_1]$$

Show that no encryption scheme (with a deterministic encryption procedure) can satisfy this definition.

Hint: Notice that the messages m_0, m_1 (or m'_0, m'_1) may or may not be equal to each other.

Part B: We could relax the definition from Part A by insisting that the messages being encrypted are different from each other. In other words, for any two pairs of messages $m_0 \neq m_1$ and $m'_0 \neq m'_1$ and for any ciphertexts c_0, c_1 we have

$$\Pr[\mathsf{Enc}(K, m_0) = c_0 \wedge \mathsf{Enc}(K, m_1) = c_1] = \Pr[\mathsf{Enc}(K, m'_0) = c_0 \wedge \mathsf{Enc}(K, m'_1) = c_1].$$

Let q be a prime number and $\mathbb{Z}_q^* = \{1, \ldots, q-1\}$[1]. Consider the scheme with $\mathcal{K} = \mathbb{Z}_q^* \times \mathbb{Z}_q^*, \mathcal{M} = \mathcal{C} = \mathbb{Z}_q^*$ defined by $\mathsf{Enc}(k, m) = x \cdot m + y$ and $\mathsf{Dec}(k, c) = (c - y)/x$ where $k = (x, y)$ and all of the operations are over $\mathbb{Z}_q^*$. Show that the above scheme satisfies the above notion of two-message security.

Problem 5 (Slightly-Imperfect Secrecy) Extra Credit 5 points

Imagine that we weakened the definition of perfect secrecy just a little bit. In particular, suppose we define the property of "ε-imperfect secrecy" to mean that for all $m_1, m_2 \in \mathcal{M}$ and every $c \in \mathcal{C}$,

$$|\Pr[\mathsf{Enc}(K, m_1) = c] - \Pr[\mathsf{Enc}(K, m_2) = c]| \leq \varepsilon.$$

Show that this notion does not provide any real guarantee of security even when ε is small, by constructing a scheme that achieves this notion of security with (say) $\varepsilon = 2^{-128}$, but where every ciphertext completely reveals the message[2].

[1] We will review this notation and more later in the course. The most relevant information for this question is that $\mathbb{Z}_q^*$ is finite set on which all standard arithmetic operations are defined and closed. Cryptographers frequently use $\mathbb{Z}_q$ as a shorthand to refer to the set of integers mod q (i.e., $\{0, 1, \ldots, q-1\}$), and $\mathbb{Z}_q^*$ are the elements coprime to q.

[2] When we say the ciphertext reveals the message, we don't mean the message is revealed through brute force or via some complicated or computationally inefficient method.