CS6222 Grad Cryptography, Homework 1

Response by: Your Name, (Computing ID)

Total points: 50 awarded maximum. 54 available. Points are noted after each problem.

Instructions. For each problem, typeset your solution in the `answer` environment, and if there are sub-problems, mark them clearly. Feel free to use as much space as you require, and be sure to update your name and computing ID above, and the acknowledgements box at the end.

Policies. In short, you are encouraged to think about the problems on your own, and then discuss them and work toward solutions with your classmates. You must write and submit your own solutions. You may also read any published material that helps you come to an understanding of the problems, but you must acknowledge and/or reference any discussion or published material, with the exception of lecture notes, in-class and in-office-hours discussions, textbook sections we have covered, and basic LaTeX help or dictionary lookups. It is a violation of the honor code if any of the following occur:

- You copy text directly from any source.
- You use any material or discussion without acknowledgment or citation, excluding the above special cases.
- You are unable to explain your work orally.

See https://jackdoerner.net/teaching/2025/Fall/CS6222/#policies for more details.

This homework recaps a few preliminary concepts that we will use in later lectures, and asks a few simple questions about perfect security.

Notation. For any $n \in \mathbb{N}$, let $[n] = \{1, 2, ..., n\}$. For any finite set $\mathcal{S}$, let $|\mathcal{S}|$ be the cardinality of $\mathcal{S}$.

Problem 1 (Reductions, 2pt each)**.** For each sub-problem, indicate if the proposition is **True** or **False**, and justify your answer in one or two sentences.

Let $F, G : \{0,1\}^* \to \{0,1\}$ be two functions with boolean outputs. We say that F reduces[1] to G (we denote this $F \leq_p G$) if there is a polynomial-time computable function $R : \{0,1\}^* \to \{0,1\}^*$ such that for every $x \in \{0,1\}^*$, $F(x) = G(R(x))$. Let $\mathbf{P}$ be the class of all polynomial-time computable functions.

(a) $F \leq_p G$ and $G \in \mathbf{P}$ implies $F \in \mathbf{P}$.

(b) $F \leq_p G$ and $F \in \mathbf{P}$ implies $G \in \mathbf{P}$.

(c) $F \leq_p G$ and $G \leq_p F$ implies $F \in \mathbf{P}$.

Problem 2 (Statistically Close Distributions, 4pts)**.** Let X and Y be random variables over the domain $\mathcal{U}$. Their *statistical distance* (also known as statistical *difference* or *total variation distance*)

[1] Specifically, F is *Karp*-reducible to G.

is

$$\mathrm{SD}(X,Y) = \max_{\mathcal{T}\subseteq\mathcal{U}} |\Pr[X \in \mathcal{T}] - \Pr[Y \in \mathcal{T}]|.$$

Let $\mathcal{X} = \{X_1, X_2, \ldots\}$ and $\mathcal{Y} = \{Y_1, Y_2, \ldots\}$ be two *ensembles* of distributions.[2] Suppose that there exists a function $\varepsilon(n)$ such that for all $n \in \mathbb{N}$, $\mathrm{SD}(X_n, Y_n) \leq \varepsilon(n)$. Prove that for any deterministic algorithm D, for all $n \in \mathbb{N}$,

$$\left| \Pr_{t\leftarrow X_n}[D(t) = 1] - \Pr_{t\leftarrow Y_n}[D(t) = 1] \right| \leq \varepsilon(n).$$

Remark: we say that $\mathcal{X}$ and $\mathcal{Y}$ are *statistically close* if and only if ε is a negligible function. This proves that statistically close ensembles are always indistinguishable, even for unbounded-time D.

Problem 3 (Some Call it Δ, 4pts)**.** Prove that statistical distance obeys the triangle inequality. That is, prove that for any distributions X, Y, Z over some domain $\mathcal{U}$ it holds that

$$\mathrm{SD}(X,Z) \leq \mathrm{SD}(X,Y) + \mathrm{SD}(Y,Z)$$

Problem 4 (A Statistically Far Distribution, 4pts)**.** Let U_n be the uniform distribution over $\{0,1\}^n$ and let $G : \{0,1\}^n \to \{0,1\}^{n+1}$ be any unbounded-time deterministic function on n-bit inputs. Show that

$$\mathrm{SD}(U_{n+1}, G(U_n)) \geq \frac{1}{2}.$$

Problem 5 (Equivalence of Definitions, 6pts each)**.** Let $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be an encryption scheme on message-space $\mathcal{M}$ and ciphertext-space $\mathcal{C}$. In class, we established that such a scheme is *perfectly secret* if for every $m_0, m_1 \in \mathcal{M}$ and every $c \in \mathcal{C}$, we have

$$\Pr\left[\mathsf{Enc}_k(m_0) = c : k \leftarrow \mathsf{Gen}\right] = \Pr\left[\mathsf{Enc}_k(m_1) = c : k \leftarrow \mathsf{Gen}\right] \tag{1}$$

We also established that it is *perfectly indistinguishable* if for every two-part unbounded-time algorithm $D = (D_1, D_2)$, we have

$$\Pr\left[D_2(c,s) = b : (m_0, m_1, s) \leftarrow D_1, b \leftarrow \{0,1\}, k \leftarrow \mathsf{Gen}, c \leftarrow \mathsf{Enc}_k(m_b)\right] = \frac{1}{2} \tag{2}$$

(a) Prove that $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is perfectly indistinguishable if it is perfectly secret.

(b) Prove that $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is perfectly indistinguishable *only* if it is perfectly secret.

Hint: for part (b), consider that an encryption scheme is *not* perfectly indistinguishable if you can construct an algorithm D that violates Equation 2.

Problem 6 (Deterministic WLOG, 2pts each)**.** This question explores the role of randomness in the context of perfect security. Recall that we define *randomized* algorithms to have access to a string of *uniform* bits.

[2] That is, each of them is a set of distributions indexed by the natural numbers.

(a) Show that for any encryption scheme satisfying Equation 1, regardless of the distribution from which Gen samples k, there is another scheme (possibly with a different keyspace $\mathcal{K}'$) that samples k from $\mathcal{K}'$ *uniformly*, and produces the same distribution of ciphertexts for any given message as the original scheme did.

(b) Show that for any randomized encryption scheme satisfying Equation 1, there is another scheme (possibly with a different keyspace $\mathcal{K}'$) that has a deterministic encryption procedure, and produces the same distribution of ciphertexts for any given message as the original scheme did.

(c) Prove that in Equation 2 we may assume the distinguisher D is deterministic without loss of generality.

Problem 7 (Slightly-Imperfect Secrecy, 6pts)**.** 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 $c \in \mathcal{C}$,

$$\left|\Pr\left[\mathsf{Enc}_k(m_1) = c : k \leftarrow \mathsf{Gen}\right] - \Pr\left[\mathsf{Enc}_k(m_2) = c : k \leftarrow \mathsf{Gen}\right]\right| \leq \varepsilon$$

for some very small ε. Construct an encryption scheme and prove that it has the following properties:

- Perfect correctness.
- "ε-imperfect secrecy" with $\varepsilon = 2^{-1000}$.
- Ciphertexts completely reveal the plaintext with probability 1.

Problem 8 (Two-Time Perfect Encryption, 6pts each)**.** In class, we explored what might happen if we use one-time pad to encrypt multiple messages under the same key, and observed that our definition of perfect secrecy considers only a single encrypted message. Consider a seemingly-natural definition of security for *two* messages that are encrypted under the same key: For all $m_1, m_2, m_1', m_2' \in \mathcal{M}$ and all $c_1, c_2 \in \mathcal{C}$,

$$\Pr\left[\mathsf{Enc}_k(m_1) = c_1 \wedge \mathsf{Enc}_k(m_2) = c_2 : k \leftarrow \mathsf{Gen}\right] = \Pr\left[\mathsf{Enc}_k(m_1') = c_1 \wedge \mathsf{Enc}_k(m_2') = c_2 : k \leftarrow \mathsf{Gen}\right]$$

(a) Show that no *deterministic* encryption scheme can achieve the above definition. Show that randomizing Enc does not help if we insist that the scheme also be correct.

(b) To overcome the limitation we have just proved, let us modify our encryption and decryption procedures so that they both take the *index* of the message to be encrypted. That is, for $i \in \{1, 2\}$, the i^{th} message m_i is encrypted by computing $\mathsf{Enc}_k(m_i, i)$ and the resulting ciphertext is decrypted by computing $\mathsf{Dec}_k(c_i, i)$. Next, suppose that we modify our definition of two-time perfect encryption to insist that for all $m_1, m_2, m_1', m_2' \in \mathcal{M}$ and all $c_1, c_2 \in \mathcal{C}$,

$$\begin{aligned}&\Pr\left[\mathsf{Enc}_k(m_1, 1) = c_1 \wedge \mathsf{Enc}_k(m_2, 2) = c_2 : k \leftarrow \mathsf{Gen}\right] \\ &= \Pr\left[\mathsf{Enc}_k(m_1', 1) = c_1 \wedge \mathsf{Enc}_k(m_2', 2) = c_2 : k \leftarrow \mathsf{Gen}\right].\end{aligned}$$

Construct a simple scheme that meets this notion of security. For an optional extra challenge, can you do this with $|\mathcal{K}| \leq 2 \cdot |\mathcal{M}|$?

Hint: for part (b), your scheme need not be efficient.

Acknowledgments

In this box, you should acknowledge your collaborators and the resources you used, if any. For example:

Problem 1: I discussed this problem with Alice and Bob. In addition, I asked Carol for help understanding Conditional Probability, but we did not discuss the problem further.

Problem 2: I asked ChatGPT "What is a turing machine?", and it gave me the following transcript: https://chatgpt.com/share/68b4dba7-e19c-8013-a137-e8db901493b7.

Problem 3: It helped me to read the proof of [Vad12, Theorem X, Page Y].

Instructor's Acknowledgments

Problems in this homework have been borrowed from or inspired by a number of sources. Citations can be provided on request, after the homework is completed.

References

[Vad12] Salil P. Vadhan. *Pseudorandomness*. 2012. https://people.seas.harvard.edu/~salil/pseudorandomness/pseudorandomness-published-Dec12.pdf.