CS 409 : Introduction to Cryptography Fall 2025

Assignment 1
Enter the Security of Cryptosystems

Instructor: Sruthi Sekar *TAs:* Lakshya Gadhwal, Ravi B Prakash

Problem 1: Alternate Definition of Perfect Secrecy?

Prove or refute: An encryption scheme with message space $\mathcal{M}$ is perfectly secret if and only if every probability distribution over $\mathcal{M}$ and every $c_0, c_1 \in \mathcal{C}$ we have $\mathbb{P}[C = c_0] = \mathbb{P}[C = c_1]$.

Problem 2: Truly Secure One-Time Pad?

When using the one-time pad with the key $k = 0^\ell$, we have $\mathtt{Enc}_k(m) = k \oplus m = m$ and the message is sent in the clear! It has therefore been suggested to modify the one-time pad by only encrypting with $k \neq 0^\ell$ (i.e., to have $\mathtt{Gen}$ choose k uniformly from the set of *nonzero* keys of length ℓ). Is this modified scheme still perfectly secure? Explain.

Problem 3: Bounds for Perfect Indistinguishability

Prove that a scheme $\Pi = (\mathtt{Gen}, \mathtt{Enc}, \mathtt{Dec})$ satisfying perfect indistinguishability (Definition 4 from Lecture 2) must have $|\mathcal{K}| \geq |\mathcal{M}|$ without using Lemma 2.6 (from the book[1]):

> **Lemma 2.6**
>
> Encryption scheme Π is perfect secret if and only if it is perfectly indistinguishable.

Specifically, let Π be an arbitrary encryption scheme with $|\mathcal{K}| < |\mathcal{M}|$. Show an adversary Eve for which $\mathbb{P}[\mathtt{Priv}_{\mathsf{Eve},\Pi} = 1] > \frac{1}{2}$ (refer to Def 4, Lec 2 for $\mathtt{Priv}_{\mathsf{Eve},\Pi}$).
Hint: It may be easier to let Eve be randomised.

Problem 4: Correctness with Errors

Assume we require only that an encryption scheme $(\mathtt{Gen}, \mathtt{Enc}, \mathtt{Dec})$ with message space $\mathcal{M}$ satisfy the following: For all $m \in \mathcal{M}$, we have $\mathbb{P}[\mathtt{Dec}(k, \mathtt{Enc}(k, m)) = m] \geq 2^{-t}$. (This probability is taken over the choice of the key as well as any randomness used during encryption.) Show that perfect secrecy can be achieved with $|\mathcal{K}| < |\mathcal{M}|$ when $t \geq 1$. Prove a lower bound on the size of $\mathcal{K}$ in terms of t.

[1] Introduction to Modern Cryptography, Second Edition - Jonathan Katz, Yehuda Lindell

Problem 5: Perfect Secrecy over Product Distributions

In this problem we consider definitions of perfect secrecy for the encryption of two messages (using the same key). Here we consider distributions over pairs of messages from the message space $\mathcal{M}$; we let M_1, M_2 be random variables denoting the first and second message, respectively. (We stress that these random variables are not assumed to be independent.) We generate a (single) key k, sample a pair of messages (m_1, m_2) according to the given distribution, and the compute ciphertexts $c_1 \leftarrow \mathtt{Enc}_k(m_1)$ and $c_2 \leftarrow \mathtt{Enc}_k(m_2)$; this induces a distribution over pairs of ciphertexts and we let C_1, C_2 be the corresponding random variables.

a) Say encryption scheme $(\mathtt{Gen}, \mathtt{Enc}, \mathtt{Dec})$ is *perfectly secret for two messages* if for all distributions over $\mathcal{M} \times \mathcal{M}$, all $m_1, m_2 \in \mathcal{M}$, and all ciphertexts $c_1, c_2 \in \mathcal{C}$ with $\mathbb{P}[C_1 = c_1 \wedge C_2 = c_2] > 0$:

$$\mathbb{P}[M_1 = m_1 \wedge M_2 = m_2 \mid C_1 = c_1 \wedge C_2 = c_2] = \mathbb{P}[M_1 = m_1 \wedge M_2 = m_2].$$

Prove that no encryption scheme can satisfy this definition.
Hint: Take $c_1 = c_2$.

b) Say encryption scheme $(\mathtt{Gen}, \mathtt{Enc}, \mathtt{Dec})$ is *perfectly secret for two distinct messages* if for all distributions over $\mathcal{M} \times \mathcal{M}$ where the first and second messages are guaranteed to be different (i.e., distributions over pairs of distinct messages), all $m_1, m_2 \in \mathcal{M}$, and all $c_1, c_2 \in \mathcal{C}$ with $\mathbb{P}[C_1 = c_1 \wedge C_2 = c_2] > 0$:

$$\mathbb{P}[M_1 = m_1 \wedge M_2 = m_2 \mid C_1 = c_1 \wedge C_2 = c_2] = \mathbb{P}[M_1 = m_1 \wedge M_2 = m_2].$$

Show an encryption scheme that provably satisfies this definition.
Hint: The encryption scheme you propose need not be efficient, although an efficient solution is possible.

Problem 6: BPP

(A) Recall Definition 5 from Lecture 3 for the complexity class BPP. Prove that $L \in \mathsf{BPP}$ (according to Definition 5), if there exists a polynomial $p(.)$ and a randomized Turing machine M such that

1. For every $x \in L$, it holds that $\Pr[M(x) = 1] \geq \frac{1}{2} + \frac{1}{p(|x|)}$, and
2. For every $x \notin L$, it holds that $\Pr[M(x) = 0] \geq \frac{1}{2} + \frac{1}{p(|x|)}$.

Hint: Given a probabilistic polynomial time machine M satisfying the above two conditions, construct an M' by running multiple copies of M (figure out how many copies) and output the majority. Use Chebyshev's inequality (refer to these slides or these notes for Chebyshev).

(B) Prove that for every $L \in \mathsf{BPP}$ (according to Definition 5, Lecture 3) and every $p(.)$, there exists a randomized Turing machine M such that

1. For every $x \in L$, it holds that $\Pr[M(x) = 1] \geq 1 - 2^{-p(|x|)}$, and
2. For every $x \notin L$, it holds that $\Pr[M(x) = 0] \geq 1 - 2^{-p(|x|)}$.

Hint: Similar to part (A) but use the stronger Chernoff bound (refer to slides or these notes for Chernoff).

Problem 7: On Negligence

Which of the following functions are negligible in terms of the security parameter λ?

a) $2^{-\lambda}$

b) $1/\lambda^{2^{100}}$

c) $\lambda^{-\log \lambda}$

d) $(\log 3)^{-\sqrt{\lambda^{3/2}}}$

e) If μ_1 and μ_2 are negligible functions, are the following functions always negligible? If yes, give a proof (by reduction), else give a counter-example:

i. $f_1(n) := \mu_1(n) + \mu_2(n)$

ii. $f_2(n) := \mu_1(n) \times \mu_2(n)$

iii. $f_3(n) := \mu_1(n) \div \mu_2(n)$

Problem 8: PRGs

You can use either of the two (equivalent) definitions 1 or 2 from Lecture 4 for a PRG. Let $G : \{0,1\}^n \to \{0,1\}^{\ell(n)}$ be a pseudorandom generator (PRG), with $\ell(n) > 2n$. In each case below, answer whether G' is a PRG or not. If yes, give a proof; if not, show a counterexample.

a) $G'(s) \stackrel{\text{def}}{=} G(s_1 \cdots s_{\lfloor n/2 \rfloor})$, where $s = s_1 \cdots s_n$.

b) $G'(s) \stackrel{\text{def}}{=} G(0^{|s|}||s)$, where $||$ means concatenation.

c) $G'(s) \stackrel{\text{def}}{=} G(s)||G(s+1)$.

d) $G'(s) \stackrel{\text{def}}{=} \begin{cases} 0^{\ell(n)}, & s = 0^{|s|} \\ G(s), & \text{otherwise} \end{cases}$

Problem 9: Unpredictability vs Pseudorandomness

Recall Definitions 1 (Unpredictability) and 2 (Pseudorandomness) from Lecture 4. Now let us define first-bit unpredictability exactly like Definition 1 for (next-bit) unpredictability for $G : \{0,1\}^n \to \{0,1\}^{\ell(n)}$: the predictor $\mathsf{Eve}^{\mathsf{pred}}$ can ask for bits $y_2, \ldots, y_i$ for any $i \in \{2, \ldots, \ell n\}$ of its choice and has to predict the first bit y_1.

a) Show that if a PRG G is pseudorandom (by Def 2), then it is also first-bit unpredictable.

b) Does the converse hold? That is, does first-bit unpredictability imply pseudorandomness? Either prove it or give a counter-example.

c) Does first-bit unpredictability imply next-bit unpredictability? Either prove it or give a counter-example.