COMP 537: Cryptography **Fall 2025**

Problem Set 1

Instructions: You **must** typeset your solution in LaTeX using the provided template. Please submit your problem set via Gradescope. Include your name and the names of any collaborators at the top of your submission.

Acknowledgment: Several of the problems in this problem set come from the Boneh-Shoup textbook.

Problem 1: Exercising the PRG definition [15 points]. Suppose G is a secure PRG that outputs bit strings in $\{0,1\}^n$. Which of the following generators derived from G are secure? For each one, either state "secure" or "insecure" followed by a short (1-2 sentence) justification. If it's insecure, your justification should state an attack on PRG security. Note: we use both the $x||y$ and (x,y) notations to denote concatenation.

(a) $G'(s) = (G(s), G(s))$

(b) $G'(s) = G(s) \oplus 1^n$

(c) $G'(s_1||s_2) = G(s_1) \oplus G(s_2)$

(d) $G'(s_1||s_2) = G(s_1) \wedge G(s_2)$ where $\wedge$ denotes bitwise AND

(e) $G'(s_1||s_2) = (s_1, G(s_2))$

Problem 2: PRG Security Proof [5 points]. Prove the following theorem for a PRG G' defined as $G'(s_1, s_2) = (s_1, G(s_1 \oplus s_2))$. Your proof does not need to be long – our example solution is less than half a page long. The proof will use a reduction.

Theorem 1. *Assuming that $G : \{0,1\}^\lambda \to \{0,1\}^N$ is a secure PRG, then the PRG $G' : \{0,1\}^{2\lambda} \to \{0,1\}^{N+\lambda}$ is a secure PRG. Specifically, for every adversary $\mathcal{A}$ who attacks G', there exists an adversary $\mathcal{B}$ attacking G such that* $\mathsf{PRGAdv}[\mathcal{A}, G'] \leq \mathsf{PRGAdv}[\mathcal{B}, G]$.

Problem 3: Encryption and Compression [10 points]. Suppose two standards committees propose to save bandwidth by combining (lossless) compression with encryption. This kind of compression generally works by removing often repeated sequences of bytes in a file to save space. Both committees plan on using a stream cipher for encryption.

(a) One committee proposes to compress messages before encrypting them. Explain why this is a bad idea from a security perspective.
Hint: Recall that compression can significantly shrink the size of some messages while having little impact on the length of other messages.

(b) The other committee proposes to compress ciphertexts after encryption. Explain what impact this would have, if any, on the security of the cipher, as well as how much compression you would expect to get.

Note: Over the years, many problems have surfaced when combining encryption and compression, including multiple attacks on widely-used cryptographic schemes.

Problem 4: Two-Time Pad [20 points]. The English department began encrypting all their texts with a one-time pad in order to better protect them. Unfortunately, they lost their key shortly after they started! They have turned to the intrepid cryptanalysts in Sitterson Hall for help recovering the encrypted content. Although the one-time pad is supposed to be unbreakable if used correctly, it is possible that they made some mistake that will allow you to recover what was encrypted.

The encrypted texts are provided in `encrypted_texts.txt`. The python script used to encrypt them is provided in `OTP_encrypt_texts.py`.

(a) What is the mistake that was made in `OTP_encrypt_texts.py` that makes it possible to recover information about the encrypted ciphertexts?

(b) How would you modify `OTP_encrypt_texts.py` to fix the problem?

(c) For each of the ten ciphertexts printed in `encrypted_texts.txt`, please write the **title AND author** of the corresponding plaintext.

Hint: Try XORing the ciphertexts together. Observe what happens when an encrypted space is XORed with an encrypted letter (a-z or A-Z).

hint 2: something is unusual about the second to last ciphertext: use that to your advantage

Note: feel free to use a search engine or other tool to look up the titles and authors of texts once you have recovered partial plaintexts. if i were you, i wouldn't worry too much if you don't get the second to last ciphertext
; it is a tricky one

Optional Feedback [5 points]. Please answer the following questions to help design future problem sets. You are not required to answer these questions (the points are free), and if you would prefer to answer anonymously, please use the anonymous feedback form. However, we do encourage you to provide feedback on how to improve the course experience.

(a) Roughly how long did you spend on this problem set?

(b) What was your favorite problem on this problem set?

(c) What was your least favorite problem on this problem set?

(d) Any other feedback for this problem set? Was it too easy/difficult?

(e) Any other feedback on the course so far?