CS/ECE407 Cryptography – Homework 1
Perfect Secrecy and Information Theory

Due: Thursday, February 3, 3:30pm CT

Remember, you may collaborate with up to one classmate. See the course webpage for more details. You are expected to write out and submit your own solutions! Your collaboration is for discussing problems at a high level, not plagiarizing answers.

The non-coding portion of your homework should be typed or carefully handwritten. We provide a LaTeX template for this document, if you would like to use it as a starting point. **If we cannot read your handwritten answers, they will not receive credit.**

Typed solutions should be submitted through Gradescope (see course webpage). Hand-written solutions should be scanned and turned in through Gradescope.

Definition 1 (Perfect Cipher)**.** Let Enc, Dec be a cipher with message space $\mathcal{M}$, key space $\mathcal{K}$, and ciphertext space $\mathcal{C}$. The cipher is **correct** if for every message $m \in \mathcal{M}$ the following holds with probability 1:

$$\Pr\left[\, m' = m \;\middle|\; \begin{array}{l} k \leftarrow \mathcal{K} \\ c \leftarrow Enc(k, m) \\ m' \leftarrow Dec(k, c) \end{array} \right] = 1$$

The cipher achieves **perfect secrecy** if for every message $m \in \mathcal{M}$ the following distributions are identical:

$$\left\{\, c \;\middle|\; \begin{array}{l} k \leftarrow \mathcal{K} \\ c \leftarrow Enc(k, m) \end{array} \right\} \equiv \{\; c \;\mid\; c \leftarrow \mathcal{C} \;\}$$

Problem 1 (Breaking traditional schemes)**.**

1. **(1 point)** The following ciphertext was created using a Caesar Cipher, which is a specialization of a substitution cipher:

   ODKBFASDMBTKUEYADQEGNFXQFTMZUFYMKRUDEFMBBQMD

   What does the corresponding plaintext say? Hint: *The cipher operates only on the 26 capital letters of the English alphabet. We are just looking for the answer here, not the method by which you found it.*

Problem 2 (Perfect Secrecy, Part 1)**.** Recall the definition of perfect secrecy (Definition 1). Let's construct a cipher with integer message space $\{0, 1, ..., 7\}$ and integer key space $\{0, 1, ..., 7\}$. Here is a proposed cipher:

$Enc(k, x)$:	$Dec(k, c)$:
return $x + k$	return $c - k$

Here, '+' denotes integer addition.

1. **(2 points**) Is the scheme **correct**? If so, prove it; if not, show a key/message pair that does not correctly decrypt.
2. **(1 points**) This scheme does not satisfy perfect secrecy. Prove it.
3. **(2 points**) Propose a simple modification to the scheme such that it satisfies perfect secrecy. Prove that the modified scheme satisfies perfect secrecy.

Problem 3 (Perfect Secrecy, Part 2)**.** Consider the following attempt at an encryption scheme for n-bit strings:

$Enc(k, x)$:	$Dec(k, (c_0, c_1))$:
return $(k, x \oplus k)$	return $c_1 \oplus k$

Definition 2 (Negligible)**.** Let $\mu : \mathbb{N} \to \mathbb{R}$ denote a function. We say that μ is **negligible** if for every positive polynomial f, there exists some natural number x_0 such that for all $x > x_0$:

$$|\mu(x)| < \frac{1}{f(x)}$$

1. **(2 points)** Is the scheme **correct**? If so, prove it; if not, show a key/message pair that does not correctly decrypt.

2. **(2 points)** Does the scheme achieve **perfect secrecy**? Prove your claim.

Problem 4 (Perfect Secrecy, Part 3)**.** Alice and Bob need to communicate confidentially, and they decide to use a one-time-pad-based cipher. Alice and Bob understand that to safely encrypt this message and to achieve perfect secrecy, they need a key with (at least) n uniformly random bits. They plan to flip a fair coin n times to choose these bits. However, they fear that all n coin flips might come up tails! If this happens, their key will be the all zero key, and so when they use it as a one-time pad to encrypt their message m, they will be sending m in the clear!

Thus, Alice and Bob agree ahead of time on a contingency plan: if they happen to flip n tails, they will start over and flip the coin n more times. They will repeat this until they get some key that is not all zeros.

1. **(3 points)** Do Alice and Bob need to adopt this contingency plan? Why/why not?

Problem 5 (Negligible Functions)**.** Recall the definition of a negligible function (Definition 2).

1. **(2 points)** Which of the following are negligible (in x)?

   (a) $f_0(x) = 1/x^{100}$

   (b) $f_1(x) = 1/2^x$

   (c) $f_2(x) = \sin(x)$

   (d) $f_3(x) = x^2$

   (e) $f_4(x) = 2^x$

   (f) $f_5(x) = 1/x^{\log\log\log\log x}$

2. **(3 points)** One reason cryptographers like to work with negligible functions is that they nicely *compose*. Let f be a negligible function. Prove that $g(x) = c \cdot f(x)$ is also negligible, where $c > 0$ is a positive constant.

Feedback: Feel free to leave feedback with respect to this homework and the course! Did you find the homework too easy/too hard/just right? How is the pace of the course so far? Please add any feedback that would help improve the course.