CS60065: Cryptography and Network Security Total: 40 *points*

Assignment 2

Instructor: *Monosij Maitra* Due: *11.59 pm, Aug 20, 2024*

Note: The basic policies are stated in the course page. Using GPT (or similar tools) to solve problems from the assignment is **strictly prohibited**. Use of any other (possibly online) source(s) **must** be clearly stated in the solution. **Any dishonesty, if caught, will yield zero credits for the entire assignment.**

A. [Perfect Secrecy : $4 \times 4 = 16$ points.]

1. Consider an encryption scheme $(\mathbf{M}, \mathbf{C}, \mathbf{K}, \mathbf{E}, \mathbf{D})$ with the usual notations introduced in class. Let $\mathbf{M}_R$ and $\mathbf{C}_R$ be discrete random variables representing the message and ciphertext distributions on $\mathbf{M}$ and $\mathbf{C}$ respectively. Perfect secrecy is achieved when

$$\Pr[\mathbf{C}_R = \mathsf{C} \mid \mathbf{M}_R = \mathsf{M}_1] = \Pr[\mathbf{C}_R = \mathsf{C} \mid \mathbf{M}_R = \mathsf{M}_2], \quad \forall \mathsf{M}_1, \mathsf{M}_2 \in \mathbf{M}, \mathsf{C} \in \mathbf{C}.$$

   Prove or refute if the following condition also implies perfect secrecy or not.

$$\Pr[\mathbf{M}_R = \mathsf{M}_1 \mid \mathbf{C}_R = \mathsf{C}] = \Pr[\mathbf{M}_R = \mathsf{M}_2 \mid \mathbf{C}_R = \mathsf{C}], \quad \forall \mathsf{M}_1, \mathsf{M}_2 \in \mathbf{M}, \mathsf{C} \in \mathbf{C}.$$

2. Prove that in a perfectly secure encryption scheme $(\mathbf{M}, \mathbf{C}, \mathbf{K}, \mathbf{E}, \mathbf{D})$ with $|\mathbf{K}| = |\mathbf{C}| = |\mathbf{M}|$, every ciphertext is equally probable.
3. Recall the Affine cipher defined on $\mathbb{Z}_{26}$. Prove that this encryption scheme achieves perfect secrecy when the keys are sampled uniformly at random.
4. Recall the one-time pad encryption scheme with $\mathbf{M}, \mathbf{K}, \mathbf{C} = \{0,1\}^n$ ($n \in \mathbb{N}$) we discussed in class. Using the key $\mathsf{K} = 0^n$ we have $\mathsf{E}_\mathsf{K}(\mathsf{M}) = \mathsf{K} \oplus \mathsf{M} = \mathsf{M}$, i.e., the message is sent in the clear! One suggestion is to modify this scheme to encrypt only with nonzero keys $\mathsf{K} \neq 0^n$ (i.e., to have the key generation algorithm choose a uniform random key $\mathsf{K} \neq 0^n$ from the set $\{0,1\}^n$. Prove or disprove formally if this modified scheme is perfectly secure or not.

B. [Entropy : $4 + (4 \times 2) + (4 \times 2) + (3 + 1) = 24$ points.]

Let $H(\mathbf{Z})$ denotes the Shannon entropy of a random variable $\mathbf{Z}$ defined on some set Z.

1. Let $(\mathbf{M}, \mathbf{C}, \mathbf{K}, \mathbf{E}, \mathbf{D})$ be any secret-key encryption scheme with $\mathbf{M}_R$, $\mathbf{C}_R$ and $\mathbf{K}_R$ as the discrete random variables associated to $\mathbf{M}$, $\mathbf{C}$ and $\mathbf{K}$ respectively. Prove that $H(\mathbf{K}_R|\mathbf{C}_R) \geq H(\mathbf{M}_R|\mathbf{C}_R)$.
2. Compute $H(\mathbf{K}_R|\mathbf{C}_R)$ and $H(\mathbf{K}_R|\mathbf{M}_R, \mathbf{C}_R)$ for the Affine cipher over $\mathbb{Z}_{26}$ assuming messages and keys used are equiprobable.
3. Let $\mathbf{D}$ and $\mathbf{R}$ be discrete random variables defined on finite sets D and R respectively. Define a function $f : D \to R$. Compute the relationship between $H(\mathbf{D})$ and $H(\mathbf{R})$ if:
   - $f(x) = 7^x$ for all $x \in D$.
   - $f(x) = \sin x$ for all $x \in D$.
4. Recall the definition of min-entropy we discussed in class: $H_\infty(\mathbf{Z}) = -\log_2 \left(\max_{z \in Z} \Pr[\mathbf{Z} = z] \right)$. Show that $0 \leq H_\infty(\mathbf{Z}) \leq H(\mathbf{Z})$. When is $H_\infty(\mathbf{Z}) = H(\mathbf{Z})$?