Fundamentals of Cryptography: Problem Set 1

Due Wed Sep 17

Collaboration is permitted (and encouraged); however, you must write up your own solutions and acknowledge your collaborators.

If a problem has **0pt**, it will not be graded.

Problem 0 Read Section 1 and 2 of "Introduction to Modern Cryptography (2nd ed)" by Katz & Lindell.

Problem 1 (3pt) In the one-time pad encryption scheme, there is nothing special about the XOR operation. Let $(\mathcal{G}, \cdot)$ be a finite group[1]. Prove that the following encryption scheme is perfectly secure.

> $\mathcal{K} = \mathcal{M} = \mathcal{C} = \mathcal{G}$
> Gen samples a random element from $\mathcal{K}$
> $\mathsf{Enc}(k, m) = k \cdot m$ (here "$\cdot$" is the group operation of $\mathcal{G}$)
> $\mathsf{Dec}(k, c) =$ _____fill the blank_____

Problem 2 (0pt) For an encryption scheme $(\mathcal{K}, \mathcal{M}, \mathcal{C}, \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$, we consider two equivalent definitions of security.

Prefect secrecy: For any distribution over $\mathcal{M}$, let random variable M denote the message sampled from the distribution, let K denote the key sampled from Gen, let C denote the output of $\mathsf{Enc}(K, M)$, then

$$\forall m \in \mathcal{M}, \forall c \in \mathcal{C}, \Pr[M = m | C = c] = \Pr[M = m].$$

Prefect indistinguishability: For any $m_0, m_1 \in \mathcal{M}$, the distributions of $\mathsf{Enc}(K, m_0), \mathsf{Enc}(K, m_1)$ are identical, that is,

$$\forall c \in \mathcal{C}, \Pr[\mathsf{Enc}(K, m_0) \to c] = \Pr[\mathsf{Enc}(K, m_1) \to c].$$

Prove that the two definitions are equivalent.

Problem 3 (3pt) Let X, Y, Z be three random variables over finite set(s). Let P_{XYZ} denote the distribution of (X, Y, Z), that is, $\Pr[X = x, Y = y, Z = z] = P_{XYZ}(x, y, z)$. Similarly, we define $P_X, P_Y, P_Z, P_{XY}, P_{XZ}, P_{YZ}$.

Part A (0pt) The entropy of a random variable is defined as

$$H[X] := \sum_x P_X(x) \log \frac{1}{P_X(x)}, \qquad H[X, Y] := \sum_{x,y} P_{XY}(x, y) \log \frac{1}{P_{XY}(x, y)}.$$

[1] If you haven't learned "group" before, you only need to learn its definition.

The entropy conditional on an event A is defined as

$$H[X|A] := \sum_x \Pr[X = x|A] \log \frac{1}{\Pr[X = x|A]}.$$

The entropy conditional on another random variable is defined as

$$H[X|Y] := \sum_y P_Y(y) H[X|Y = y].$$

The mutual information between two random variable is defined as

$$I[X;Y] = H[X] - H[X|Y].$$

Prove that

$$I[X;Y] = H[X] + H[Y] - H[X,Y].$$

Prove that (hint: Jensen's inequality)

$$H[X] \geq 0, \qquad H[X|Y] \geq 0, \qquad I[X;Y] \geq 0.$$

Part B (0pt) The conditional mutual information is defined as

$$\begin{aligned} I[X;Y|A] &= H[X|A] + H[Y|A] - H[X,Y|A], \\ I[X;Y|Z] &= \sum_z P_Z(z) I[X;Y|Z = z]. \end{aligned}$$

The "three-way mutual information" is defined as

$$I[X;Y;Z] = H[X] + H[Y] + H[Z] - H[X,Y] - H[X,Z] - H[Y,Z] + H[X,Y,Z].$$

Prove that

$$I[X;Y;Z] = I[X;Y] - I[X;Y|Z].$$

Prove that

$$H[Z] \geq I[X;Y;Z] \geq -H[Z].$$

Find an example where $I[X;Y;Z] = H[Z] > 0$, and another example where $I[X;Y;Z] = -H[Z] < 0$.

Part C (3pt) Let $(\mathcal{K}, \mathcal{M}, \mathcal{C}, \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a perfectly secure encryption scheme. Let random variable K denote the key generated by Gen. Prove that $H[K] \geq \log(|\mathcal{M}|)$.

Problem 4 (6pt) The last problem gives an alternative proof that $|\mathcal{K}| \geq |\mathcal{M}|$ for any perfectly secure encryption scheme. We will consider whether smaller key suffices if we relax the requirements.

Part A We relax the security requirement (parameterized by a constant $\varepsilon < 1$): Suppose we only require for any distribution M, for any $m \in \mathcal{M}$ and for any $c \in \mathcal{C}$, let K be sampled from Gen and let $C = \mathsf{Enc}(K, M)$, then

$$\Big| \Pr[M = m|C = c] - \Pr[M = m] \Big| \leq \varepsilon.$$

Prove a lower bound of $|\mathcal{K}|/|\mathcal{M}|$ for any encryption scheme that meets this definition and the perfect correctness requirement.

Part B We relax the security requirement (parameterized by a constant $\varepsilon < 1$): Suppose we only require for any $m_0, m_1 \in \mathcal{M}$, for any distinguisher D, the distinguisher guesses correctly with probability at most

$$\Pr_{\substack{k \leftarrow \mathsf{Gen} \\ b \leftarrow \{0,1\}}}\left[\mathsf{D}(\mathsf{Enc}(K, m_b)) = b\right] \leq \frac{1}{2} \cdot (1 + \varepsilon).$$

Prove a lower bound of $|\mathcal{K}|/|\mathcal{M}|$ for any encryption scheme that meets this definition and the perfect correctness requirement.

Part C We relax the correctness requirement (parameterized by a constant $\varepsilon < 1$): Suppose we only require for any $m \in \mathcal{M}$

$$\Pr_{k \leftarrow \mathsf{Gen}}[\mathsf{Dec}(k, \mathsf{Enc}(k, m)) = m] \geq 1 - \varepsilon.$$

Prove a lower bound of $|\mathcal{K}|/|\mathcal{M}|$ for any encryption scheme that meets this definition and the perfect secrecy requirement. We assume both Enc and Dec are deterministic algorithms.