CSE5014: Cryptography and Network Security
2023 Spring Semester Written Assignment #1
Due: Mar. 21st, 2023, please submit at the beginning of class

Q.1 The following is an encryption of English text using a shift cipher. Find the key and decrypt the ciphertext.

"gighsqv wg o dipzwq ibwjsfgwhm tcibrsr wb hvs zigv vwzzg ct bobgvob rwghfwqh gvsbnvsb wh wg kcfywbu hckofrg psqcawbu o kcfzr qzogg ibwjsfgwhm slqszzwbu wb wbhsfrwgqwdzwbofm fsgsofqv bifhifwbu wbbcjohwjs hozsbhg obr rszwjsfwbu bsk ybckzsrus hc hvs kcfzr"

Q.2 Prove that the two definitions (Definition 1.6 and Definition 1.7) on slides (Lecture 02) are *equivalent*.

Q.3 Let $M = 6$, and let $\mathbb{Z}_M$ denote the set $\{0, 1, \ldots, M-1\}$. Let $x \bmod M$ denote the remainder obtained when dividing x by M.

(1) Consider the symmetric encryption scheme in which the encryption of message $m \in \mathbb{Z}_M$ under key $k \in \mathbb{Z}_M$ is $(m + k) \bmod M$. Is this encryption scheme *perfectly secure*? Why or why not?

(2) Consider the symmetric encryption scheme in which the encrption of message $m \in \mathbb{Z}_M$ under key $k \in \mathbb{Z}_M$ is $(m + 2k) \bmod M$. Is this encryption scheme perfectly secure? Why or why not?

Q.4 An encryption scheme (Gen, Enc, Dec) with message space $\mathcal{M}$ is perfectly secure if and only if

$$\Pr[Enc_K(m) = c] = \Pr[Enc_K(m') = c]$$

holds for every two $m, m' \in \mathcal{M}$ and every $c \in \mathcal{C}$.

Q.5 For an encryption scheme (Gen, Enc, Dec), consider the following game:

- Eve chooses $m_1, m_2, m_3 \in \{0,1\}^\ell$.
- Alice selects $k \leftarrow_R \{0,1\}^n$, $i \leftarrow_R \{1,2,3\}$ and gives Eve $c = E_k(m_i)$.
- Eve sends a number $j \in \{1,2,3\}$.

Eve *succeeds* if $i = j$. Prove that (Gen, Enc, Dec) is perfectly secure, if and only if Eve can guess i with probability at most $1/3$.

Q.6 Prove that the *statistical distance* $\Delta(X, Y)$ defined in Definition 2.1 of Lecture 3 is a **metric**.

Q.7 Let $\{X_n\}$, $\{Y_n\}$ be sequences of distributions with X_n and Y_n ranging over $\{0,1\}^{p(n)}$ for some polynomial $p(n)$ in n. $\{X_n\}$ and $\{Y_n\}$ are *computationally indistinguishable* ($X_n \approx Y_n$) if for every polynomial-time algorithm A, there is a negligible function ϵ such that

$$|\Pr[A(X_n) = 1] - \Pr[A(Y_n) = 1]| \leq \epsilon(n).$$

Prove that the *computational indistinguishability* $\approx$ defined above is an **equivalence relation**.