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

Sample Solutions

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"

Solution:

The key is 14 and the decrypted text is:

SUSTech is a public university founded in the lush hills of Nanshan District Shenzhen It is working towards becoming a world class university excelling in interdisciplinary research nurturing innovative talents and delivering new knowledge to the world.

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

Solution: We now prove that for every pair of plaintexts x, x', $E_{U_n}(x) \equiv E_{U_n}(x')$ **iff** the probability that Eve guesses x_b after seeing the ciphertext $c = E_k(x_b)$ is at most $1/2$.

If $E_{U_n}(x) \equiv E_{U_n}(x')$, then Eve gets no information on b, and can win with probability at most $1/2$.

For the "if" part, we prove by contrapositive. W.l.o.g., there exist x_1, x_2 such that $E_{U_n}(x_1)$ is not the same distribution as $E_{U_n}(x_2)$. This means that there is a string y_0 such that $\Pr[Y_{x_1} = y_0] > \Pr[Y_{x_2} = y_0]$. Thus, Eve can do the following: given ciphertext y and x_1, x_2, outputs 1 if $y = y_0$, else outputs a random number in $\{1, 2\}$ otherwise. Then Eve will succeed with probability larger than $1/2$.

□

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?

Solution:

(1) This encryption scheme is *perfectly secure*. We use a table, whose entry is $E_k(m)$ to describe the encryption scheme as follows:

$k =$ / $m =$

	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

We claim that $\Pr[E_k(m) = c] = 1/6$ for every $m \in \mathbb{Z}_M$ and $c \in \mathbb{Z}_M$, where the probability is over a random choice of k from $\mathbb{Z}_M$. This implies that the scheme is *perfectly secure*. For each pair of m and c, the probability that $E_k(m) = c$ is the number of times c occurs in column m of the table divided by the number of choices for k. But c occurs exactly once in this column and the number of possible rows is 6. Thus, the probability is 1/6. More formally, we compute

$$\Pr[E_k(m) = c] = \frac{|\{k \in \mathbb{Z}_M : k + m \bmod M = c\}|}{|\mathbb{Z}_M|} = \frac{1}{6}.$$

(2) This encryption scheme is *not* perfectly secure. We use a similar table, whose entry is $E_k(m)$ to describe the encryption scheme as follows:

$m =$

$k =$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	2	3	4	5	0	1
2	4	5	0	1	2	3
3	0	1	2	3	4	5
4	2	3	4	5	0	1
5	4	5	0	1	2	3

Let $c = 4$, $m_1 = 0$, and $m_2 = 1$. Then we have

$$\begin{aligned} \Pr[E_k(m_1) = c] &= \frac{2}{6} = \frac{1}{3} \\ \Pr[E_k(m_2) = c] &= \frac{0}{6} = 0. \end{aligned}$$

Since we have found m_1, m_2, c such that

$$\Pr[E_k(m_1) = c] \neq \Pr[E_k(m_2) = c],$$

the scheme is *not* perfectly secure.

□

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 $c \in \mathcal{C}$.

Solution:

"Only if" part: Suppose that (Gen, Enc, Dec) is perfectly secure. Fix two messages m, m' and a ciphertext c that occurs with nonzero probability, and consider the uniform distribution over $\{m, m'\}$. Perfect secrecy implies that $\Pr[M = m|C = c] = 1/2 = \Pr[M = m'|C = c]$. But

$$\begin{aligned} \frac{1}{2} = \Pr[M = m|C = c] &= \frac{\Pr[C = c|M = m] \cdot \Pr[M = m]}{\Pr[C = c]} \\ &= \frac{\frac{1}{2}\Pr[C = c|M = m]}{\Pr[C = c]}, \end{aligned}$$

and so $\Pr[C = c|M = m] = \Pr[Enc_k(m) = c] = \Pr[C = c]$. Since an analogous calculation holds for m' as well, we conclude that $\Pr[Enc_k(m) = c] = \Pr[Enc_k(m') = c]$.

"If" part: see Proof of Lemma 2.4 in the textbook.

□

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 $1/3$.

Solution: "Only if" part: if the encryption scheme (Gen, Enc, Dec) is *perfectly secure*, Eve gets the same output no matter what i was. So, she gets no information on i, and the success probability is at most $1/3$.

"if" part: the proof is similar to that of *Two to Many Theorem*. We prove that if the scheme (Gen, Enc, Dec) is *not* perfectly secure, i.e., there is some set M and some strategy for Eve to guess a plaintext chosen from M with probability larger than $1/|M|$, then there is also some set M' of size 3 and a strategy Eve' for Eve to guess a plaintext chosen from M' with probability larger than $1/3$.

We fix $x_1 = 0^\ell$ and pick x_2 at random in M. Then it holds that for random key k and message $x_2 \in M$,

$$\Pr_{k \leftarrow \{0,1\}^n, x_2 \leftarrow M}[Eve(Enc_k(x_2)) = x_2] > 1/|M|.$$

On the other hand, for every choice of $k, x' = Eve(Enc_k(x_1))$ is a fixed string independent on the choice of x_1, and so if we pick x_2 at random in M, then the probability that $x_2 = x'$ is at most $1/|M|$, i.e.,

$$\Pr_{k \leftarrow \{0,1\}^n, x_2 \leftarrow M}[Eve(Enc_k(x_1)) = x_2] \leq 1/|M|.$$

Due to the linearity of expectation, there exists some x_2 satisfying

$$\Pr[Eve(Enc_k(x_2)) = x_2] > \Pr[Eve(Enc_k(x_1)) = x_2].$$

We now define a new attacker Eve' as:

$$Eve'(c) = \begin{cases} x_2, & \text{if } Eve(c) = x_2 \\ x_i, i \in \{1,2,3\} \text{ at random}, & \text{otherwise} \end{cases}$$

This means that the probability that $Eve'(Enc_k(x_2))$ is larger than $1/3$.

□

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

Solution: It suffices to prove that $\Delta(X,X) = 0$, $\Delta(X,Y) = \Delta(Y,X)$, and $\Delta(X,Y) + \Delta(Y,Z) \geq \Delta(X,Z)$. First, by definition, we have

$$\Delta(X,X) = \max_{T \subseteq \{0,1\}^n} |\Pr[X \in T] - \Pr[Y \in T]| = 0.$$

Second, we have

$$\begin{aligned} \Delta(X,Y) &= \max_{T \subseteq \{0,1\}^n} |\Pr[X \in T] - \Pr[Y \in T]| \\ &= \max_{T \subseteq \{0,1\}^n} |\Pr[Y \in T] - \Pr[X \in T]| \\ &= \Delta(Y,X). \end{aligned}$$

For the triangle inequality, by Lemma 2.3, we know that

$$\Delta(X,Y) = \frac{1}{2} \sum_{w \in Supp(X) \cup Supp(Y)} |\Pr[X = w] - \Pr[Y = w]|.$$

Thus, we have

$$\begin{aligned} &\Delta(X,Y) + \Delta(Y,Z) \\ &= \frac{1}{2} \sum_{w \in Supp(X) \cup Supp(Y)} |\Pr[X = w] - \Pr[Y = w]| + \frac{1}{2} \sum_{w \in Supp(Y) \cup Supp(Z)} |\Pr[Y = w] - \Pr[Z = w]| \\ &\geq \frac{1}{2} \sum_{w \in Supp(X) \cup Supp(Y) \cup Supp(Z)} |\Pr[X = w] - \Pr[Y = w] + \Pr[Y = w] - \Pr[Z = w]| \\ &= \frac{1}{2} \sum_{w \in Supp(X) \cup Supp(Y) \cup Supp(Z)} |\Pr[X = w] - \Pr[Z = w]| \\ &= \frac{1}{2} \sum_{w \in Supp(X) \cup Supp(Z)} |\Pr[X = w] - \Pr[Z = w]| \\ &= \Delta(X,Z). \end{aligned}$$

Hence, the *statistical distance* $\Delta(X, Y)$ 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**.

Solution: To prove that $\approx$ is an equivalence relation, we need to prove that $\approx$ is *reflexive*, *symmetric*, and *transitive*.

(1) reflexive: $X_n \approx Y_n$ means for every polynomial-time A and polynomially bounded ϵ, $|\Pr[A(X_n) = 1] - \Pr[A(Y_n) = 1]| \leq \epsilon(n)$. It is trivial that $X_n \approx X_n$.

(2) symmetric: If $X_n \approx Y_n$, since $|\Pr[A(X_n) = 1] - \Pr[A(Y_n) = 1]| = |\Pr[A(Y_n) = 1] - \Pr[A(X_n) = 1]|$, we have $Y_n \approx X_n$ by definition.

(3) transitive: if $X_n \approx Y_n$ and $Y_n \approx Z_n$, we have for every polynomial-time A and polynomially bounded ϵ, $|\Pr[A(X_n) = 1] - \Pr[A(Y_n) = 1]| \leq \epsilon(n)$ and $|\Pr[A(Y_n) = 1] - \Pr[A(Z_n) = 1]| \leq \epsilon(n)$. It follows that

$$\begin{aligned}
&|\Pr[A(X_n) = 1] - \Pr[A(Z_n) = 1]| \\
&\quad = |\Pr[A(X_n) = 1] - \Pr[A(Y_n) = 1] + \Pr[A(Y_n) = 1] - \Pr[A(Z_n) = 1]| \\
&\quad \leq |\Pr[A(X_n) = 1] - \Pr[A(Y_n) = 1]| + |\Pr[A(Y_n) = 1] - \Pr[A(Z_n) = 1]| \\
&\quad \leq 2\epsilon(n).
\end{aligned}$$

Thus, we have $X_n \approx Z_n$.

□