# Data Privacy Homework 3

严禁抄袭，可以使用Latex、word或手写拍照等方式，最终请提交pdf文件至bb系统。

Plagiarism is strictly prohibited, and methods such as Latex, Word, or handwritten photography can be used. Finally, please submit a PDF file to BlackBoard.

## 1. Permutation Cipher(10')

**(a) 5'** Consider the permutation $\pi$ on the set $1, 2, \ldots, 8$ defined as follows. Find the inverse permutation $\pi^{-1}$.

| $x$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| $\pi(x)$ | 4 | 1 | 6 | 2 | 7 | 3 | 8 | 5 |

**(b) 5'** Decrypt the following ciphertext encrypted using a permutation cipher with the key being the permutation $\pi$ from part (a).

$$TGEEMNELNNTDROEOAAHDOETCSHAEIRLM$$

## 2. Perfect Secrecy(20')

**(a) 10'** Let $n$ be a positive integer. An $n$-th order Latin square is an $n \times n$ matrix $L$ such that each of the $n$ integers $1, 2, \ldots, n$ appears exactly once in each row and each column of $L$. The following is an example of a Latin square of order 3:

| 1 | 2 | 3 |
| --- | --- | --- |
| 3 | 1 | 2 |
| 2 | 3 | 1 |

For any $n$-th order Latin square $L$, we can define a related encryption scheme. Let $\mathcal{M} = \mathcal{C} = \mathcal{K} = \{1, 2, \ldots, n\}$. For $1 \leq i \leq n$, the encryption rule $e_i$ is defined as $e_i(j) = L(i, j)$ (thus, each row provides an encryption rule). Prove that if the key is chosen uniformly at random, the Latin square cipher has perfect secrecy.

**(b) 10'** Prove that if a cipher has perfect secrecy and $|\mathcal{M}| = |\mathcal{C}| = |\mathcal{K}|$, then each ciphertext is equiprobable.

## 3. RSA(25')

Assuming that Bob uses RSA and selects two ”large” prime numbers $p = 101$ and $q = 113$:

**(a) 5'** How many possible public keys Bob can choose?

**(b) 10'** Assuming that Bob uses a public encryption key $e = 3533$. Alice sends Bob a message $M = 9726$. What will be the ciphertext received by Bob? Show the detailed procedure that Bob decrypts the received ciphertext.

**(c) 10'** Let $n = pq$ be a product of two distinct primes. Show that if $\phi(n)$ and $n$ are known, then it is possible to compute $p$ and $q$ in polynomial time. (Hint: Derive a quadratic equation (over the integers) in the unknown p.)

## 4. Multi-Party Computation(20')

**(a) 10' Paillier encryption**. Assuming Alice employs the Paillier encryption scheme with the prime numbers $p = 11$ and $q = 17$, along with a randomly chosen value of $r = 83$. Alice transmits a message $M = 175$ to Bob. What ciphertext will Bob receive? Additionally, please prove the Homomorphic addition property of Paillier : $\text{Decrypt}\big((c_1 \cdot c_2) \bmod n^2\big) = m_1 + m_2$

**(b) 10' Secret Sharing.** We define a 2-out-of-3 secret sharing scheme as follows. In order to share a bit $v$, the dealer chooses three random bits $x_1, x_2, x_3 \in \{0, 1\}$ under the constraint that $x_1 \oplus x_2 \oplus x_3 = 0$. Then:

- $P_1$ 's share is the pair $(x_1, a_1)$ where $a_1 = x_3 \oplus v$.
- $P_2$ 's share is the pair $(x_2, a_2)$ where $a_2 = x_1 \oplus v$.
- $P_3$ 's share is the pair $(x_3, a_3)$ and $a_3 = x_2 \oplus v$.

Let $(x_1, a_1), (x_2, a_2), (x_3, a_3)$ be a secret sharing of $v_1$, and let $(y_1, b_1), (y_2, b_2), (y_3, b_3)$ be a secret sharing of $v_2$. Try to explain that no communication is needed in order to compute a secret sharing of $v_1 \oplus v_2$. ($\oplus$ means XOR)

## 5. Computational Security(25')

**(a) 5'** Explain the difference between $Interchangeable$ and $Indistinguishable$

**(a) 10'** Which of the following are negligible functions in $\lambda$ ? Justify your answers.

$$\frac{1}{2^{\lambda/2}} \quad \frac{1}{2^{\log(\lambda^2)}} \quad \frac{1}{\lambda^{\log(\lambda)}} \quad \frac{1}{\lambda^2} \quad \frac{1}{2^{(\log \lambda)^2}} \quad \frac{1}{(\log \lambda)^2} \quad \frac{1}{\lambda^{1/\lambda}} \quad \frac{1}{\sqrt{\lambda}} \quad \frac{1}{2^{\sqrt{\lambda}}}$$

**(b) 10'** Suppose $f$ and $g$ are negligible.
(1) Show that $f + g$ is negligible.
(2) Show that $f \cdot g$ is negligible.
(3) Give an example $f$ and $g$ which are both negligible, but where $f(\lambda)/g(\lambda)$ is not negligible.