공개키 암호

(Public Key Cryptography)

- RSA의 개인키의 크기를 줄이시오.

Proof. Recall that RSA-CRT algorithm : Suppose we have a system of k linear congruences:

$$x \equiv a_1 \pmod{n_1}\ x \qquad\qquad \equiv a_2 \pmod{n_2} \vdots\ x \qquad\qquad \equiv a_k \pmod{n_k}$$

where $n_1, n_2, \ldots, n_k$ are pairwise coprime. Let $N = n_1 n_2 \cdots n_k$. Then, for each $i = 1, 2, \ldots, k$, let $N_i = N/n_i$ and let d_i be the inverse of N_i modulo n_i, i.e., $d_i N_i \equiv 1 \pmod{n_i}$. Then the unique solution of the system of congruences is given by:

$$x = \sum_{i=1}^{k} a_i N_i d_i \pmod{N}$$

To prove this, first note that for each i, the condition $n_i \mid (x - a_i)$ implies that $n_i \mid (x - a_j)$ for all $j \neq i$. Therefore, if y is any integer that satisfies the system of congruences, then we have $y \equiv x \pmod{n_i}$ for all i. In particular, $y - x$ is divisible by each n_i, so $N \mid (y - x)$. Thus, any two solutions of the system of congruences differ by a multiple of N.

Now, we need to show that x is a solution to the system of congruences. For each i, we have:

$$x \equiv \sum_{j=1}^{k} a_j N_j d_j \pmod{n_i} \qquad = a_i N_i d_i + \sum_{j \neq i} a_j N_j d_j \pmod{n_i} \equiv a_i N_i d_i \pmod{n_i}$$

since n_i divides N_j for all $j \neq i$. Thus, x satisfies the i-th congruence. Therefore, x is a solution to the system of congruences.

Finally, we need to show that x is the unique solution modulo N. Suppose y is another solution. Then $y \equiv x \pmod{n_i}$ for all i, so $y - x$ is divisible by each n_i, and hence by N. Therefore, $y \equiv x \pmod{N}$. Thus, any two solutions of the system of congruences are congruent modulo N, so x is the unique solution modulo N. □

Instructions:

a. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec pulvinar mauris in nisi fringilla, eu dictum mi laoreet. Vestibulum et lobortis libero.

b. Suspendisse eget massa in augue eleifend egestas. Nam pulvinar euismod enim ac tristique.

c. Proin auctor, arcu sit amet venenatis hendrerit, nisi quam maximus justo, nec tincidunt mauris nibh nec risus. Vivamus commodo sed mauris vel dapibus.

Questions:

1. **Brightness (X points)** - Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec pulvinar mauris in nisi fringilla, eu dictum mi laoreet. Vestibulum et lobortis libero.

2. **Color (X points)** - Suspendisse eget massa in augue eleifend egestas. Nam pulvinar euismod enim ac tristique.

3. **Contrast (X points)** - Proin auctor, arcu sit amet venenatis hendrerit, nisi quam maximus justo, nec tincidunt mauris nibh nec risus. Vivamus commodo sed mauris vel dapibus.

4. **Motion (X points)** - Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec pulvinar mauris in nisi fringilla, eu dictum mi laoreet. Vestibulum et lobortis libero.
5. **Depth (X points)** - Suspendisse eget massa in augue eleifend egestas. Nam pulvinar euismod enim ac tristique.

Submission instructions: Submit your completed assignment by emailing it to `example@email.com` by the due date.