CS60065: Cryptography and Network Security Total: 50 *points*

Assignment 4

Instructor: *Monosij Maitra* Due: *11.59 pm, Nov 07, 2024*

Note: The basic policies are stated in the course page. Using GPT (or similar tools) to solve problems from the assignment is **strictly prohibited**. Use of any other (possibly online) source(s) **must** be clearly stated in the solution. **Any dishonesty, if caught, will yield zero credits for the entire assignment.**

A. [RSA and Primality Tests : $10 + 5 + 5 = 20$ points.]

1. For $n = pq$, where p and q are distinct odd primes, define $\lambda(n) = \frac{\phi(n)}{\gcd(p-1,q-1)}$. Suppose that we modify the RSA encryption scheme by requiring that $ed \equiv 1 \pmod{\lambda(n)}$. Prove that encryption and decryption are still inverse operations in this modified scheme.

2. Define the set $G(n) = \left\{ \mathsf{a}\colon a \in \mathbb{Z}_n^*, \quad \left(\frac{a}{n}\right) \equiv a^{(n-1)/2} \pmod{n} \right\}$.
   (a) Prove that $|G(n)| \leq \frac{n-1}{2}$.
   (b) Suppose $n = p^k q$, where p and q are odd, $p \in \mathbb{P}, k \geq 2$, and $\gcd(p, q) = 1$. Let $a = 1 + p^{k-1}q$. Prove that $\left(\frac{a}{n}\right) \not\equiv a^{(n-1)/2} \pmod{n}$.

B. [ElGamal Encryption and Diffie-Hellman Problems: $10 + 10 = 20$ points.]

1. Recall the ElGamal encryption scheme discussed in class. Show that reusing the ephemeral secret during encryption for just two ciphertexts can break secrecy of messages.

2. Recall the Diffie-Hellman problems discussed in class. Let $\mathbb{G}$ be a finite, multiplicative, cyclic group of prime order p with two generators $g, h \in \mathbb{G}$ sampled randomly from $\mathbb{G}$. Next, for each $i \in [\ell]$, let $s_i, t_i \leftarrow \mathbb{Z}_p$ denote two randomly sampled integers and define $h_i = g^{s_i} \cdot h^{t_i}, \forall i \in [\ell]$. Consider a vector $\vec{\mathbf{y}} = (y_1, \ldots, y_\ell) \in \mathbb{Z}_p^\ell$. Define a secret key associated to the vector $\vec{\mathbf{y}}$ as

$$\mathsf{SK}_{\vec{\mathbf{y}}} := (s_{\vec{\mathbf{y}}}, t_{\vec{\mathbf{y}}}) = \left(\sum_{i=1}^{\ell} s_i \cdot y_i \pmod{p}, \sum_{i=1}^{\ell} t_i \cdot y_i \pmod{p} \right).$$

   Consider a vector $\vec{\mathbf{x}} = (x_1, \ldots, x_\ell) \in \mathbb{Z}_p^\ell$ describing a "message". The following steps are executed to encrypt the message vector $\vec{\mathbf{x}}$: Sample a uniformly random integer $r \leftarrow \mathbb{Z}_p$ and compute

$$C := g^r \pmod{p}, \quad D := h^r \pmod{p}, \quad \{E_1 := g^{x_1} \cdot h_1^r \pmod{p}, \ldots, E_\ell := g^{x_\ell} \cdot h_\ell^r \pmod{p}\}$$

   The final ciphertext encrypting the vector $\vec{\mathbf{x}}$ is defined as $\mathsf{CT} = \left(C, D, \{E_i\}_{i \in \{1,2,3,\ldots,\ell\}}\right)$. Show how to decrypt CT with secret key $\mathsf{SK}_{\vec{\mathbf{y}}}$ such that decryption yields $g^{\langle \vec{\mathbf{x}}, \vec{\mathbf{y}} \rangle \pmod{p}}$.
   [**Hint**: Recall how decryption algorithm works in the ElGamal encryption scheme.]

C. [Elliptic Curves: $5 + 5 = 10$ points.]

1. Compute discriminant for the elliptic curve $y^2 \equiv x^3 + 2x + 2$ over $\mathbb{Z}_{17}$. What is the sum of points $P = (13, 7)$ and $Q = (6, 3)$ in the Abelian group for the above curve? **[2 + 3 = 5]**

2. Let $E : y^2 = x^3 + 3x + 2$ be an elliptic curve defined over $\mathbb{Z}_7$. Compute all the points on E over $\mathbb{Z}_7$. What is the order of the group? Given the element $\alpha = (0, 3)$, determine the order of α. Does α generate the group? **[1 + 1 + 3 = 5]**