Paras Garg 16UCS122

The LNM Institute of Information Technology

(Deemed-to-be University)

QUIZ-II

Cryptographic Algorithms(CRYALO)

Duration:1 Hrs **10 Marks**
8.00 PM-9.00AM 11^{th} April 2019

Answer all Questions

1. Suppose E is an elliptic curve defined over $\mathbb{Z}_p$, where $p > 3$ is prime. Suppose that the number of points $\#E$ is prime, P be an element in $E(\mathbb{Z}_p)$ and $P \neq \mathcal{O}$, where $\mathcal{O}$ is point at infinity (identity element). Prove that the discrete logarithm $log_P(-P) = \#E - 1$.

   HINT: Discrete logarithm - Let an element $P \in E(\mathbb{Z}_p)$ of order n. An element Q is in the cyclic group generated by P. Find an unique integer d, $0 \leq d \leq n-1$ such that $d \cdot P = Q$. This can be written as $d = log_P Q$. [3]

2. Prove the following in **ElGammal Signature Scheme** and **DSA**
   A signature in the **ElGammal Signature Scheme** or **DSA** is not allowed to have $s = 0$. Show that if a message were signaled with a "signature" in which $s = 0$, then it would be easy for an adversary to compute the private key a. [2]

3. Write **Elliptic Curve Digital Signature Algorithm(ECDSA)** and justify that the security of this scheme relies on Discrete Logarithm Problem(ECDLP). [3]

4. Suppose Alice and Bob communicating over a public network. To preserve data integrity, Alice modifies the **ElGammal Signature Scheme** as

$$r = \alpha^k \bmod p$$
$$s = (H(m) - kr)a^{-1} \bmod (p-1)$$

   and signs on message m. Construction of keys remains same. She chooses a generator $\alpha \in \mathbb{Z}_p^*$, where $\mathbb{Z}_p^*$ is the multiplicative group. Also selects a random integer a, $1 \leq a \leq p-2$, $gcd(a, p-1) = 1$ and construct both the public and private keys by computing $y = \alpha^a \bmod p$. The keys are (p, α, y) and a.
   How the signature (r, s) would be verified by Bob using the following verification equation

$$v_1 = v_2$$

   Where $v_1 = y^s \cdot r^r \bmod p$ and $v_2 = \alpha^{H(m)} \bmod p$ [2]

End