LNMIIT
The LNM Institute of Information Technology

# The LNM Institute of Information Technology

Department of Computer Science & Engineering

**Cryptograhic Algorithms (CSE3112)**
**End-term Examination**

Time: 3 hours(11.30.00-2.30PM) Date:30/04/2019 Maximum Marks: 50

1. Suppose Alice signs on a $m$ using **DSA** and sends the signed message to Bob over a public network. Let the adversary Eve sets $\theta = (\text{SHA-I}(m))^{-1} \bmod q$, $\gamma = y^{\theta} \bmod p$. Suppose the she can find $r, \mu \in \mathbb{Z}_p^*$, such that

$$((\alpha\gamma^{r})y^{\mu^{-1} \bmod q}) \bmod p \bmod q = r$$

Define $s = \mu$ SHA-I$(m)$ mod $q$. Prove that she can mount a potential attack in this setting. [7]

**HINTS:** $(r, s)$ is valid signature on message $m$.

2. Let the message $m_0$ is being signed using **ECDSA** scheme. Where the message $m_0 \in \{0,1\}^*$ is a bit string such that SHA-II$(m_0) =$ $00\ldots0$, *i.e* SHA-II$(m_0) \equiv 0 \bmod$ ~~q~~ n in **ECDSA**. Prove that it is possible to forge the signature which would be a `Total break`. [7]

3. Write **Schnorr Signature Scheme** and prove that signature verification works. $[3\frac{1}{2} + 3\frac{1}{2}]$

4. Suppose that Alice signs on a message $m$ using **ElGamal Signature Scheme**. In order to save time in generating the random numbers $k$ that are used to sign messages, Alice chooses tan initial value $k_0$, and then signs the $i^{th}$ message say $m_i$ using $k_i = k_0 + 2i \bmod p$, therefor $k_i = k_{i-1} + 2 \bmod p$ for all $i \geq 1$. Suppose Bob observes two consecutive signed messages, say $(m_i, sig(m_i)$ and $(m_{i+1}, sig(m_{i+1}))$. Describe how Bob can easily compute Alice's private key $a$ given this information, without solving an instance of Discrete Logarithm Problem. [7]

5. (a) Write **RSA Encryption scheme** and its proof of correctness. [4]

   (b) Prove that it satisfies multiplicative property. [4]

6. Let Bob intercepts a ciphertext intended for Alice while communicating over a public network and encrypted with Alice's public key $e$. Bob wants to obtains original message $m = c^d \bmod n$. Bob chooses a random value $r$ less than $n$ and computes

$$Z = r^e \bmod n$$
$$X = Zc \bmod n$$
$$t = r^{-1} \bmod n$$

Next Bob gets Alice to authenticate $X$ ~~it to sign on X using his own private key~~ with her private key thereby decrypting $X$. Alice returns $Y = X^d \bmod n$. Show that Bob can use the information now available to him to determine $m$. [7]

7. Write **ElGamal Signature Scheme** and justify that the randomly chosen $k$, $1 \leq k \leq p-2$ would be co-prime with $p-1$ in `Signing algorithm`. [7]

******END*****