LNMIIT
The LNM Institute of Information Technology

# The LNM Institute of Information Technology

Department of Computer Science & Engineering

**Computer Security (CSE329)**
**End-term Examination**

Ujjawal Kumar
17UCS171.

Time: 3 hours(12:00-03:00PM) Date:06/12/2019 Maximum Marks: 50

**Instructions:** Attempt all the seven (07) questions in sequential order. Start each question from the new page. Solve the question using standard method/techniques. Tweaking the parameters are not allowed particularly for numerical problems.

1. Answer the following in maximum 5 lines:

   (a) User "vivaan" owns a directory, "stuff," containing a text file called "ourstuff.txt" that he shares with users belonging to the group "staff." Those users may read and change this file, but not delete it. They may not add other files to the directory. Others may neither read, write, nor execute anything in "stuff." What would appropriate ownerships and permissions for both the directory "stuff" and the file "ourstuff.txt" look like? (Write your answers in the form of "long listing" output.) [3]

   (b) Suppose a web client and web server for a popular shopping web site have performed a key exchange so that they are now sharing a secret session key. Describe a secure method for the web client to then navigate around various pages of the shopping site, optionally placing things into a shopping cart. Your solution is allowed to use one-way hash functions and pseudo-random number generators, but it cannot use HTTPS, so it does not need to achieve confidentiality. In any case, your solution should be resistant to HTTP session hijacking even from someone who can sniff all the packets. [3]

2. For the DAC model, an alternative representation of the protection state is a directed graph. Each subject and each object in the protection state is represented by a node (a single node is used for an entity that is both subject and object). A directed line from a subject to an object indicates an access right, and the label on the link defines the access right. [8]

   (a) Draw a directed graph that corresponds to the given access matrix.

   (b) Is there a one-to-one correspondence between the directed graph representation and the access matrix representation? Explain in maximum 5 lines.

| | File 1 | File 2 | File 3 | File 4 |
|---|---|---|---|---|
| User A | Own<br>Read<br>Write | | Own<br>Read<br>Write | |
| User B | Read | Own<br>Read<br>Write | Write | Read |
| User C | Read<br>Write | Read | | Own<br>Read<br>Write |

3. An organization *XYZ* wants to implement a technique for secure communication between host and application server. Design a protocol that can facilitate authentication mechanism between the host and the server. Note

that there should not be any credentials/key exchange over the public network. However, the protocol can make use of a trusted third-party server. [8]

4. There are two communication parties Alice and Bob sharing some secret information using MIME protocol. There is a chance that an adversary can intercept the communication. Modify the protocol and illustrate the modifications on both the sides of the communicating parties with diagram to prevent such attacks. [8]

5. Let $H : \{0,1\}^{2n} \rightarrow \{0,1\}^n$ be a collision resistant hash function. Let $k \in \{0,1\}^n$ be the key and $\alpha$ be a random $n$-bit key string. Consider the following symmetric key cryptosystem. Let the message is encrypted by using the the given scheme.

$$E_k(m) = \alpha \| (H(\alpha) \oplus m \oplus k)$$

Prove that, it is not a **CPA** secure encryption scheme.
(**CPA** -Chosen Plain text Attack). [6]

6. Let's consider the encryption scheme $E_k : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$. Where the symmetric key $k \in \{0,1\}^n$. The scheme works as block cipher that encrypt the message of block size $n$ with the following rule

$$E_{H_{i-1}}(m_i) = H_i$$

Where $m = m_1 \| m_2 \ldots m_\alpha$, $H_0 = IV$, $IV$ denotes initialization vector and $h(m) = H_\alpha$. This also defines the hash function $h : \{0,1\}^* \rightarrow \{0,1\}^n$.
Prove that the adversary can find a collision in $h$ [7]

7. Consider the following rule to construct tag $T = S_k(m)$ to authenticate a message $m = m_1 \| \ldots m_\alpha$ with $m_i \in \{0,1\}^n$

$$S_k(m) = \{f_k(m_1) \oplus k\} \oplus \ldots \oplus \{f_k(m_\alpha) \oplus k\}$$

Where $f : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$ is a pseudo random function.
Prove that the construction of tag $T$ *i.e* **MAC** is not secure. [7]

**Hints**: Consider an adversary say $\mathcal{A}$ submits the queries on a message $m = 0^{(\alpha-2)n} \| 1^n$ for an even $\alpha$.

****END***