Master of Computer Science and Engineering

First Year Second Semester Examination 2025

Subject: IoT Security

Time: 3 Hours | Full Marks: 100

Answer All Questions

1. (a) What are digital certificates? Describe how digital certificates can be used for the authentication of devices in the IoT.
   (b) Describe how the Diffie-Hellman key-exchange protocol can be used to establish a secret between two IoT devices that use an insecure communication protocol.
   (c) What are the challenges of using TLS in constrained IoT devices?
   (d) Why is IPsec rarely used in highly resource-constrained IoT environments?
   (e) What is proxy re-encryption? Describe one use case of proxy re-encryption in IoT.

   4+4+4+4+4=20

2. (a) What is Software Defined Networking (SDN)? How can SDN help improve security in IoT networks?
   (b) What is Network Functions Virtualization (NFV)? How does NFV enhance security in IoT networks?
   (c) What is Service Function Chaining (SFC) in NFV, and how does it help secure IoT traffic?
   (d) What are Virtualized Network Functions (VNFs) in NFV? How can VNFs be used to deploy firewalls or intrusion detection systems for IoT?
   (e) Describe how VNF migration can provide seamless movement of security services in mobile IoT environment?

   4+4+4+4+4=20

3. (a) What is DTLS? How is DTLS different from TLS? Why is DTLS suitable for IoT applications?
   (b) How does DTLS handle packet loss and reordering in UDP?
   (c) What is DTLS session resumption and why is it useful for IoT?
   (d) What are the necessity of the `epoch` and `sequence number` fields in the DTLS record protocol header?
   (e) What are `HelloVerifyRequest` and `Cookie` mechanisms in DTLS, and how do they improve security in UDP-based IoT communications?
   (f) How does DTLS differ from IPSec?

   4+3+3+4+4+2=20

4. (a) What is a Physical Unclonable Function (PUF)? What are Challenge-Response Pairs (CRPs) in a PUF?
   (b) Explain the following properties of PUF.
      i. Unclonable
      ii. Unpredictable
      iii. One-way

iv. Tamper-evident

(c) Describe how PUFs can be used for IoT device authentication.

(d) Describe how one can measure the performance of a PUF, based on the following criteria.

i. Uniqueness
ii. Uniformity
iii. Reliability
iv. Bit-aliasing

4+4+4+8=20

5. (a) Describe the structure of a blockchain. How does a blockchain ensure the immutability of the data stored in it?

(b) Discuss some applications of blockchain technologies in smart agriculture.

(c) What are the roles of consensus protocols in blockchain implementation? Describe the Proof-of-Work consensus protocol and discuss its suitability in IoT applications.

(d) What are smart contracts? Describe a use case for smart contracts in IoT applications.

(e) Discuss some challenges in integrating blockchain technologies in IoT.

4+4+5+4+3=20

6. (a) Discuss briefly about ZigBee network and application layer security.

(b) What are the roles of a trust center in a ZigBee network?

(c) What is a trust center link key? Describe the cases in which a trust center link key is used.

(d) Describe how a trust center periodically updates the network key.

(e) Under what circumstances a ZigBee device may have to rejoin a network? Describe the trust center rejoin process.

4+2+4+5+5=20

7. (a) What are CoAP proxies? Describe an example of a CoAP proxy use case. Describe security challenges with CoAP proxies?

(b) Describe the different modes in which CoAP can be secured.

(c) What is a request delay attack on CoAP? Give a suitable example.

(d) What are the different QoS levels in MQTT? Describe the connect flooding attack that exploits higher QoS levels.

(e) Describe the Last Will Testament (LWT) feature of MQTT. Describe how this feature can be exploited to launch a flooding attack on MQTT.

5+3+4+4+4=20