INDIAN STATISTICAL INSTITUTE
M. Tech. (CrS) II: 2025–2026
Cryptographic and Security Implementation
Semestral Examination

Date: 24. 11. 2025 | Marks: 100 | Time: 3 Hours

Answer any five questions.
Write the part answers of each question at the same place.

1. (a) Write down an efficient algorithm to calculate the Greatest Common Divisor (GCD) of two positive integers, each of size s bits.
   (b) What is the time complexity of your algorithm?
   (c) How this algorithm can be extended in obtaining b (inverse finding), given a, n, when $ab \equiv 1 \bmod n$, where a, b, n are on s bits each.
   (d) How the inverse finding algorithm can be implemented for large integers, in C language, with a suitable library of your choice?

   $[1 + 6 + 6 + 1 = 20]$

2. Different Processors (including Intel and AMD) support the AES-NI (AES New Instructions) extension.
   (a) List the main AES-NI instructions.
   (b) Explain how they correspond to the AES rounds and key expansion steps.
   (c) Discuss the advantage of using AES-NI over software-only AES implementations.

   $[6 + 6 + 8 = 20]$

3. Consider two machines are communicating securely over a public channel.
   (a) How the cipher suites are important in this context?
   (b) Clearly explain the cryptographic algorithms in the cipher suites considering one or more specific examples.
   (c) How can you design a software such that the cipher suite elements (cryptographic algorithms) can be listed on the screen at the time of secure communications?

   $[5 + 5 + 10 = 20]$

4. Describe the CRYSTALS-KYBER with set-up, encryption and decryption steps presenting relevant toy examples. $[8 + 6 + 6 = 20]$

5. Answer the following questions in the context of the Signal Protocol.
   (a) Define forward secrecy and post-compromise security in the context of the Signal Protocol.
   (b) Describe the purpose of the Double Ratchet Algorithm.
   (c) Explain the difference between the symmetric-key ratchet and the Diffie–Hellman ratchet.
   (d) Using a diagram or clear stepwise flow, show how new message keys are derived and updated between Alice and Bob.

(e) What is the role of the X3DH (Extended Triple Diffie Hellman) handshake in the Signal Protocol?

(f) How does Signal Protocol maintain asynchronous communication?

$[3 + 5 + 3 + 3 + 1 + 2 = 20]$

6. Answer the following questions in the context of Post Quantum scenario.

(a) Explain why classical public-key algorithms such as RSA and ECDH are considered insecure in the post-quantum era.

(b) Mention the quantum algorithms responsible for breaking them.

(c) Describe the architecture and key components of the PQXDH protocol. Your answer should identify the classical and post-quantum algorithms combined in the hybrid design, and briefly explain how these keys are generated and exchanged.

(d) Using the simplified lattice-based model $b = A \cdot s + e$, explain the role of the noise term "e" in ensuring post-quantum security. How does the legitimate receiver still manage to compute the shared secret accurately despite this noise?

$[1 + 3 + 8 + 5 = 20]$

7. (a) What is the primary difference between a Host Based Intrusion Detection and Network Based Intrusion Detection? What sort of data these intrusion detection systems work on?

(b) In today's world, most of the communication happens over Encrypted channel, relying mostly on the TLS protocol. If man-in-the-middle decryption is now allowed, then give one example of a technique through which malware implantation over encrypted channel can be detected. Shortly describe, how that technique works.

(c) Discuss the concept of password aging in Linux. How can system administrators configure and control password aging policies using tools like chage, or /etc/login.defs.

$[(1 + 3) + (3 + 1) + (3 + 3) = 20]$

8. (a) On a linux system, what we can achieve by firing the command

```
"iptables -A INPUT -s A.B.C.D -p tcp --dport 22 -j DROP"
```

What difference, one could expect if we replace the word DROP in the above command line by REJECT. If we want to REJECT all incoming SSH connections to a Linux System other than from IP A.B.C.D, then what are we required to do.

(b) Describe file access control mechanism in Linux and describe how file access permissions can be changed.

(c) What is the difference between logging and auditing in a Linux environment? Name one or two tools which are used for these purposes. $[(3 + 3 + 3) + (3 + 2) + (3 + 3) = 20]$