End Semester Examination

Principles of Information Security
IIIT Hyderabad

May 1, 2025

There are 10 questions, 10 marks each. Maximum Marks: 100. Time: 180 min

---

1. Let F be a block cipher with 128-bit input length. Prove that neither of the following encryption schemes are CPA-secure: $5 + 5 = 10$

   - Scheme A: choose a random 128-bit r and let $c = \langle r, F_r(k) \oplus m \rangle$, m is of 128 bits.
   - Scheme B: For 256-bit messages: to encrypt message $m_1 m_2$ using key k (where $|m_1| = |m_2| = 128$), choose random 128-bit r and compute the ciphertext $\langle r, F_k(r) \oplus m1, F_k(m_1) \oplus m_2 \rangle$.

2. Prove that no perfect Byzantine agreement protocol exists for 3 parties with any one among them being faulty (the setting is a completely connected synchronous P2P network). Assuming digital signatures exist, design an authenticated byzantine agreement protocol (for the aforementioned setting). Show the equivalence Byzantine agreement and the broadcast problem in the above setting. $5 + 3 + 2 = 10$

3. Design a protocol for securely simulating a TTP in each of the following settings: $3 + 4 + 3 = 10$

   1. Three unbounded parties one among them is passively corrupt.
   2. Two computationally bounded parties, one is passively corrupt.
   3. Four unbounded parties, one among them is actively corrupt.

4. Using quantum mechanics, show how to achieve the following: $3 + 2 + 5 = 10$

   1. Establishing a secret-key between two parties using the BB84 protocol.
   2. Establishing a secret-key among n parties, using a n-qubit state like

   $$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|00\ldots0\rangle + |11\ldots1\rangle\right)$$

   3. Breaking RSA using Shor's algorithm.

5. For each of the following historical ciphers, either show how to break them or prove their unbreakabilty by using Shannon's perfect secrecy: $2 \times 5 = 10$

   1. Caesar Cipher
   2. Shift Cipher
   3. Mono-Alphabetic Substitution Cipher
   4. Vegenere Cipher

5. Vernam Cipher (one-time pad)

6. Formally define the concept of negligible functions. Give an example or prove the non-existence of an operation $\circ$ on functions for each of the following: $2 \times 5 = 10$

   1. Negligible functions are closed under $\circ$ and non-negligible functions are closed under $\circ$.
   2. Negligible functions are closed under $\circ$ and non-negligible functions are not closed under $\circ$.
   3. Negligible functions are not closed under $\circ$ and non-negligible functions are closed under $\circ$.
   4. Negligible functions are not closed under $\circ$ and non-negligible functions are not closed under $\circ$.
   5. If f is negligible and g is non-negligible then $f(n) \circ g(n)$ is neither always negligible nor always non-negligible.

7. Design a new MAC scheme that is provably secure (and prove it under CDH/DDH/DLP-assumption) — specifically, construct a fixed length collision resistant hash function using DLP, followed by the Merkle-Damgard transform and subsequently a HMAC-like design. Compare/contrast your design with the CBCMAC, and which of the two is likely to have a smaller block-size? $3+2+2+2+1 = 10$

8. Describe a *zero knowledge proof* (ZKP) for GRAPH-3-COLORING (G3C). Prove the completeness, soundness and the zero-knowledgness of your protocol/proof. Why are digital signatures a special case of zero-knowledge proofs? Can you imagine a new kind of interactive authentication protocol based on the the hardness of GRAPH-3-COLORING and your ZKP for it? $3+3+1+3 = 10$

9. Answer the following regarding Shamir's secret sharing: $3+2+2+3 = 10$

   1. Explain why Shamir's secret-sharing scheme has zero reconstruction error, then design a modification that allows $\epsilon > 0$ reconstruction error but reduces expected share size. Analyze the trade-off.
   2. Over the field $\mathbb{F}_{19}$, generate a $(3, 5)$ secret sharing scheme for the secret $s = 7$. Publish all five shares. Then show step-by-step how any three specific shares reconstruct s using Lagrange interpolation.
   3. Suppose one participant forges their share during reconstruction in a (t, n) scheme. Give an algorithm that detects cheating when an authenticated channel is available only between the dealer and each participant (not between participants). Prove correctness.
   4. Design and analyze a weighted-threshold version of Shamir's scheme in which each player i has weight w_i and the secret is recoverable iff the total weight of cooperating players $\geq T$. Show how to assign each player an appropriate number of shares without increasing total share size asymptotically.

10. Write in detail about any *two* of the following: $2 \times 5 = 10$

    1. Perfectly secure 1-out-of-2 OT is impossible
    2. Kerckhoff's Principle
    3. Shannon's Theory of Perfect Secrecy
    4. Fiat-Shamir Heuristic for Designing Non-interative ZKP
    5. Details of any two Public-key Cryptosystems (other than RSA and El Gamal)
    6. 1-out-of-n OT using $O(\log n)$ instances of 1-out-of-2 OT
    7. Blockchains

BEST OF LUCK