tcg crest

(Deemed to be University u/s 3 of UGC Act, 1956)

Distinct Category - Research

TCG CREST

School of Mathematics and Computer Sciences

Ph.D. Programme
Cryptology and Post-Quantum Cryptology

Academic Session: August 2026

Detailed Syllabus
for the Written Admission Test

Institute for Advancing Intelligence
TCG CREST

Syllabus

The written examination consists of two parts: Research Methodology and the Technical Section. Attempting the Research Methodology section is mandatory. The Technical Section will comprise three alternatives (A/B/C), of which candidates may attempt any one.

I. Research Methodology

The examination will include questions designed to assess the candidate's research aptitude, reasoning ability, divergent thinking, and general awareness of research methodology.

II. Technical Section

A. General Mathematics

1. **Basic Algebra:** Theory of Equations, Complex Numbers, Basic understanding of Group Theory, Polynomials.
2. **Elementary Linear Algebra:** Determinants and their properties, Cramer's Rule, Systems of linear equations, Rank, Matrices and matrix algebra, Eigen values and Eigen vectors, Orthogonal bases, Vector spaces, Inner products, Gram-Schmidt procedure.
3. **Basic Statistics:** Mean, Median, Mode, Standard deviation, Skewness and kurtosis, Moment, Correlation and Regression.
4. **Discrete Mathematics:** Basics of set theory, Functions and relations, Basic Combinatorics (Basic counting, Inclusion-exclusion principle, Pigeonhole principle), Permutation and Combination, Recurrence relations, Generating functions.
5. **Elementary Probability:** Basic definitions, Random variables, Distributions, Standard discrete distributions (uniform, binomial, Poisson, geometric, hypergeometric); Expectation, Variance and moments; Conditional probability and Bayes' theorem.
6. **Basic Number Theory:** Divisibility, GCD, Modular arithmetic, Chinese Remainder Theorem.
7. **Elementary High School Level Calculus:** Limit, Continuity, Differentiation and Integration.

B. Technical Topics in Computer Science

1. **Graph theory:** Paths and cycles, Connected components, Tree, Digraphs, Eulerian trails, Hamiltonian paths, Planar graphs, Graph coloring.
2. **Elements of computing:** Basics of programming (using pseudo-code), Procedure call and Parameter passing.
3. **Data Structures:** Array, Linked list, Stack, Queue, Heap, Binary tree, Heap, AVL tree.
4. **Design and Analysis of Algorithms:** Asymptotic notation, Searching, Sorting, Selection, Greedy Algorithms, Dynamic Programming, Graph algorithms: Breadth First Search, Depth First Search, Shortest Path.

5. **Circuits and systems:** Analysis of elementary high school level circuits involving resistance, Capacitance and Inductance; Analog electronic circuits involving transistors, Boolean algebra, Minimization of Boolean functions, Gates and logic circuits, Combinational and sequential circuits; Signals and systems, Convolution, Fourier transform, and z-transform.
6. **Formal Languages and Automata Theory:** Finite automata and regular languages. Push-down automata and context-free languages. Turing machines.

C. Quantum Computation and Quantum Information

1. **Introduction:** Quantum dynamics, quantum measurements and collapse hypothesis, density operators, single qubit and multi-qubit systems, pure and mixed states, quantum gates and circuits.
2. **Quantum Correlations:** Bell inequalities and entanglement, Schmidt decomposition, EPR paradox, quantum teleportation, theory of quantum entanglement, entanglement of pure bipartite states.
3. **Quantum Algorithms:** Introduction to quantum algorithms; Deutsch–Jozsa algorithm, Grover's search algorithm, Simon's algorithm, Shor's factorization algorithm.
4. **Quantum Information Theory:** Classical information theory, Shannon entropy, von Neumann entropy, no-cloning theorem; Quantum Key Distribution (BB84, Ekert, MDI-QKD).