CERTIFICATE PROGRAMME IN PRACTICAL CRYPTOGRAPHY AND COMMUNICATION (CRYPTCOM) - 2026

26-31 May, 2026

The Centre for Development of Advanced Computing (C-DAC) Patna is organizing a 6-days Certificate Programme in Practical Cryptography and Communication (CryptCom)–2026 for government officials working in Indian R&D units, strategic organizations, and ministries. This compact program is designed to provide hands-on training along with the essential theories required for implementation and management of cryptography-powered communication systems.

Why train with us?

We don't just teach: we research, develop, innovate and impart the knowledge we acquire. The R&D team of C-DAC Patna has consistently tackled hard problems of cyberspace, leveraging broad expertise to strengthen the security posture across cybersecurity infrastructures. Having developed unique, proprietary security products trusted by premier government agencies, C-DAC Patna is now, for the first time, distilling its proprietary, years-long R&D insights into a comprehensive curriculum designed for the next generation of cyber defenders serving in various government agencies.

Features of CryptCom

- In-depth theory sessions
- Intensive laboratory-based technical training
- Dedicated daily doubt-clearing and mentoring sessions
- Professional certificate upon successful completion and assessment

Who Can Apply?

- Employees currently serving in Central or State governments only.

Prerequisites

- Any graduate / post-graduate / higher degree holder
- One year working experiance in cyber security will be given preference

Registration & Venue

Registration link: https://cdac.gov.in/cryptcom
Venue: C-DAC Patna

Programme Fee

₹ 60,000* /- + Applicable GST

Programme Coordinator (SPOC)

Dr. Kunal Abhishek, Scientist 'E' | Mobile No: **+91-9791006182** | Email: **akunal@cdac.in**

* *All modules are compulsory.*

Admission is strictly based on first-come, first-serve basis.

Syllabus & Schedule

Days	Topics
Module 1 - Module duration: 3 days	
DAY 1	**M1(A): Foundations of Cryptography** • Mathematics for Cryptography • Symmetric and Asymmetric Ciphers • Hash Functions • Random Number Generators • Lab Sessions
DAY 2	**M1(B): Core Cryptographic Mechanisms** • Key Management Techniques • Modern Encryptions • New Hash Functions • Lab Sessions
DAY 3	**M1(C): Post Quantum Cryptography (PQC)** • NIST Standard • Intricacies of New Cryptographic Schemes • Implications of PQC • Lab Sessions
Module 2 - Module duration: 2 days	
DAY 4	**M2(A): Networking and Secure Communication** • Modern Communication Protocols • PKI and TLS Applications • Lab Sessions
DAY 5	**M2(B): Secure Network Design** • Zero Trust Network • Operating System and Networking • Lab Sessions
Module 3 - Module duration : 1 day	
DAY 6	**M3: Cryptographic Practices: Case Studies** • Case study I: GHOST and Ganga Tools • Case study II: EYES Tool
	*Evaluation and Assessment of Candidates *Award and Certificate Distribution