RAJASTHAN PUBLIC SERVICE COMMISSION, AJMER

SYLLABUS OF COMPETITIVE EXAMINATION FOR THE POST OF SENIOR SCIENTIFIC OFFICER CYBER FORENSIC DIVISION STATE FORENSIC SCIENCE LABORATORY (HOME DEPARTMENT)

1. Computer Fundamentals

Computer Organization and Architecture (COA): Definition, history, types of computers, block-diagram, processor and its types; I/O devices: input devices, output devices, storage media and its types; Operating System: definition, architecture types of OS, scheduling algorithms, boot process, Master Boot Record (MBR), Volume Boot Record (VBR), boot loaders, process management, memory management, kernel, and system level APIs; File Systems: definition, role of file system in electronic devices, structure, types of file systems, File Allocation Table (FAT), New Technology File System (NTFS), Extended File System (EXT), Apple File System (APFS), Yet Another Flash File System (YAFFS) and other File systems.

2. Networking concepts

Definition; types: Local Area Network (LAN), Metropolitan Area Network (MAN), Wide Area Network (WAN), Campus Area Network (CAN) and others; Architecture: client-server, peer-to-peer and others; Topology: Bus, Star, Ring, Mesh and others; Network Interface Controller (NIC); Types of media: Co-axial, Twisted Pair, Fiber Optic and others; Open Systems Interconnection (OSI) Reference Model and its layers; TCP/IP Protocol Suite; wired v/s wireless networks; Communication devices: switch, router, gateway and others; Internet: definition, history, Internet Service Provider (ISP), Domain Names, Secure transmission, Proxy, Virtual Private Network (VPN); mailing protocols and file transfer protocols.

3. Database Management Systems (DBMS)

Definition of data; data v/s information; structured v/s unstructured data; definition of DBMS and Relational DBMS (RDBMS); records; tuples; fields; tables; procedures; schemas; types of DBMS/RDBMS; Exiting tools and packages: Oracle MySql, PostgreSQL, SQL Server and others; Structured Query Language (SQL) and NoSQL: Data Definition and Data Manipulation Languages (DDL and DML); Basics SQL Commands; Procedures; Remote Procedure Calls (RPC); No SQL packages; indexing; sorting and searching; Database Administration (DBA): DBMS/RDBMS configurations; backup & restore; logging; recovering corrupted/crashed tables or databases; user rights management; security measures for effective data handling and storage.

4. Software Engineering and Programming Concepts

Software engineering: process; types of software development models; stages of software development and engineering; Types of applications: desktop, mobile, web and others; Software Licenses; Fundamentals of Programming Languages: Procedure Oriented V/S Object Oriented Programming, software testing, packaging, reverse engineering and re-engineering, debugging, deployment, maintenance, secure source code techniques, patch management.

5. Emerging Technologies

AI/ML/DL: Definition of Artificial Intelligence, Machine Learning and Deep Learning, history of AI, types of machine learning, various algorithms of ML/DL, Artificial Neural Network (ANN), Deep Neural Network (DNN), Convolutional Neural Network (CNN), Generative Adversarial Networks (GANs), Computer Vision, Natural Language Processing, Large Language Models (LLMs) and risks related to AI; Internet of Things (IoT): definition, IoT ecosystem, applications of IoT, architecture/layers of IoT, components of IoT, networking protocols in IoT, security concerns and challenges; Blockchain: definition, blockchain concept and decentralized approach, types of blockchain implementation, regulatory challenges and security concerns in blockchain implementation, cryptocurrencies and wallets: AR/VR and Metaverse: Augmented Reality (AR), Virtual Reality (VR), Mixed Reality(MR), Metaverse implementation, challenges and regulatory concerns related to metaverse.

6. Information Security

Information Security: Confidentiality, Integrity and Availability (CIA) Triad, Authentication, Authorization, Non-repudiation; Cryptography & Steganography: Cryptography, Symmetric and Asymmetric algorithms, Hashing Algorithms, Cryptanalysis, Digital Signature, Digital Certificate, Certifying Authorities (CAs), definition of steganography, types and algorithms of steganography, steganalysis and its challenges; Vulnerability Assessment and Penetration Testing (VAPT): definition, vulnerability v/s weakness, types of vulnerabilities, Common Vulnerabilities and Exposures (CVEs), Common Vulnerability Scoring System (CVSS), vulnerability assessment tools and techniques, penetration testing and its methods/tools.

7. Cyber Crimes and Cyber Forensics

Cyber Crimes: definition of cyber/computer crime, types of cyber crimes, known cybercrimes, emerging cyber crimes; Cyber Forensics: definition, branches of cyber forensics, cyber forensic process, definition of electronic evidence, types of electronic evidences, principle of exchange (Locard's exchange principle), search & seizure of electronic evidences, evidence preservation, evidence integrity (chain-of-custody, hashing, etc.), standard operating procedures (SOPs) and best practices in electronic evidence handling and cyber forensics; Malware: definition, types of malware, malware analysis techniques, sandboxing, honeypot, malware samples and challenges involved in malware analysis.

8. Computer Forensics

Disk Forensics: storage media, secondary storage devices, disk, volume, partition, slack space, carving, data recovery and file system restoration; Windows Forensics: Windows boot process, Windows file systems, Windows registry, event logs, prefetch files, shortcut/link files, Most Recently Used (MRU), Shell bags, page file, user accounts and authorization, Windows servers, web history and other important artefacts; Linux Forensics: Linux boot process Linux file systems, logging mechanism in Linux, user accounts and authorization, types of shells, Linux servers (including web servers), web history and other important artefacts; Virtual Machine Forensics: Virtualization, analyzing Virtual Machines (VMs), Windows Subsystem for Linux (WSL) and its investigation.

9. Mobile Forensics

Basics: Mobile and small computing devices, Mobile communications, resource constraints and challenges, types of acquisitions, rooting & jail-breaking; Android: Android OS architecture, android file system, app permissions, logging mechanism in android phone, types of artefacts, tools and technologies for android forensics, challenges & limitations of android forensics; iOS: iPhone OS (iOS) architecture, iOS file system, iOS app permissions, logging in iOS, tools & technologies for iOS forensics, challenges & limitations of iOS forensics; Miscellaneous: Forensic analysis of Pagers, Wearable devices and other smart gadgets, CDR (Call Detail Record) Analysis, handling hoax calls, voice over IP (VoIP) technology and calls.

10. Network Forensics

Crimes committed within or targeting computer networks; challenges involved in acquiring evidences from a computer network; analyzing logs from network devices; Internet Protocol Detail Record (IPDR) analysis; Network Packet Analysis; analysis of server logs; role of Security Information and Event Management (SIEM) and firewall in network forensics; Wireless communications: Wi-Fi, Bluetooth, Near Field Communication (NFC) and other methods of wireless communications; Cloud Forensics: definition of cloud, architecture and types of clouds, containers, dockers, virtualization, analyzing and investigating cloud logs.

11. Multimedia Forensics

Types of multimedia files; types of images; image structure and digital representation; image enhancement techniques; CCTV and DVR basics; analysis of CCTV footage; video files; image/video authentication techniques; differentiating real v/s deepfake audio/image/video; morphing techniques and detection; types of audio files; audio quality enhancement and speaker identification techniques; tools and technologies used for multimedia forensics; AI based CCTV and video analytics techniques.

12. Memory forensics

Live v/s dead forensics; Memory Management; memory structure; importance of RAM Forensics; virtual memory; segmentation; pages and demand paging; page fault; memory address translation; shared memory; types of memory access; processes and threads;

challenges involved in memory acquisition; tools and technologies to acquire and analyze memory dump; important artefacts which could be recovered from Windows/Linux/Android RAM; analyzing malware using memory forensics; event and timeline reconstruction; analyzing memory dumps, page file and hiberfil files.

13. Social Media Investigation and Open Source Intelligence (OSINT)

Information: Definition, type and sources; Investigating social media Platforms: X, Facebook, LinkedIn, Instagram, WhatsApp and others; challenges and limitations of social media platform investigation; tools and technologies available for social media investigation; Open Source Intelligence (OSINT): OSINT and its branches, resources available for OSINT, importance of OSINT in cyber crime investigation, tools and technologies available for OSINT.

14. Emerging trends and challenges in cyber forensics

Dark web: basics of dark web, accessing dark web using The Onion Router (TOR) and working of TOR, TOR nodes, relays and networking, analyzing TOR traffic and websites, limitations and challenges of TOR investigations; AI- Based Crimes: basic of AI-based crimes, deep fake, differentiating between AI-based and traditional crimes, challenges and limitations of investigating AI-based crimes; Drones: basic of Unmanned Aerial Vehicle (UAV), types of UAV, UAV communication protocols, investigating drones and other UAVs, challenges in UAV / Drones investigation.

15. Acts & Legal Frame work

The Information Technology Act, 2000 of India and its amendments; cyber space jurisdiction; important sections of the Bharatiya Nyaya Sanhita (BNS), the Bharatiya Nagarik Suraksha Sanhita (BNSS) and The Bharatiya Sakshya Adhiniyam(BSA) related to cybercrimes; Intellectual Property Rights (IPR) its infringement and legal provisions; Audit and Compliance of Computer and IT infrastructure.

* * * * *

Pattern of Question Papers:

1. Objective Type Paper
2. Maximum Marks: 150
3. Number of Questions: 150
4. Duration of Paper: 2.30 Hours
5. All Questions carry equal marks
6. There will be Negative Marking