Prelims Exam Topics

POST-QUANTUM CRYPTOGRAPHY (PQC)

Context

A DST task force under the National Quantum Mission recommended phased adoption of post-quantum cryptography (PQC) across India's critical sectors such as defence, banking, telecom and power.

Key recommendations of the Task Force

- **Critical Sector Migration:** Government, defence, telecom, banking, power and transport sectors placed on accelerated PQC transition timeline.
    - Critical infrastructure sectors targeted for complete PQC adoption by 2029.
- **Sandbox Testing:** Recommended pilot testing of PQC and hybrid encryption systems by 2027–28.
- **Sector-Specific Rules:** Suggested ministries and regulators frame dedicated PQC regulations.
- **National Testing Programme:** Proposed National PQC Testing and Certification Programme with testing labs by 2026.
- **Assume-Breach Principle:** Warned against "harvest now, decrypt later" cyberattacks where encrypted data is stolen today for future decryption.
- **Q-Day Concern:** Report warned that quantum computers capable of breaking current cryptography may emerge within a few years.
- **QKD Backbone:** Recommended long-term integration of **Quantum Key Distribution (QKD) networks.**

About Post-Quantum Cryptography (PQC)

- **Post-Quantum Cryptography (PQC):** New generation encryption algorithms designed to resist attacks from quantum computers.
- **Purpose:** Protects digital systems such as banking, defence communication and government data from future quantum attacks.
- **Need for PQC:** Quantum computers may break current public-key cryptography using advanced computational power.
- **How PQC Protects from Quantum Computers**
    - **Quantum-Resistant Algorithms:** Uses mathematical problems that quantum computers cannot easily solve.

- **Replaces Vulnerable Systems:** Designed to replace current public-key cryptography vulnerable to quantum attacks.
- **Secure on Classical Systems:** Works on existing computers and networks without requiring quantum hardware.
- **Future-Proof Security:** Protects sensitive data from "harvest now, decrypt later" cyberattacks.

Quantum Key Distribution (QKD)

- **Definition:** Quantum cryptography technique for secure sharing of encryption keys.
  - It is a hardware-based secure communication method using quantum properties of light.
- **Quantum Principle:** Any eavesdropping attempt alters quantum state and becomes detectable.
- **Application:** Used for ultra-secure communication networks.

LONG-TAILED DUSKHAWKER

Context

- A rare dragonfly species was rediscovered in Arunachal Pradesh's Namdapha National Park after nearly 110 years.

About the Discovered Dragonfly

- **Scientific Name:** *Gynacantha khasiaca*.
- **Group:** Belongs to Odonata order that includes dragonflies and damselflies.
- **Behaviour and Features:** Exhibits crepuscular behaviour(active primarily during the twilight period:) and possesses compound eyes enabling near-360° vision.
- **Habitat:** Found in freshwater and forest ecosystems.
- **Rediscovery Site:** Recorded from Namdapha National Park and Tiger Reserve in Arunachal Pradesh.
- **Distribution:** Found in Bangladesh, Myanmar, Nepal and parts of India including Arunachal Pradesh and Assam.
- **IUCN Status:** Not Evaluated (NE).

- **Genus Diversity:** *Gynacantha* genus has around 92 species globally and about 10 species in India.

HUMBOLDTIA NAIRIANA

Context

- Researchers from Jawaharlal Nehru Tropical Botanic Garden and Research Institute (JNTBGRI) discovered a new evergreen tree species, *Humboldtia nairiana*,

About the Tree

- **Scientific Name:** *Humboldtia nairiana*; named after G. M. Nair, former Director of JNTBGRI.
- **Type and Features:** Medium-sized evergreen tree (5–8 m) with pale brown warty bark and elliptic-oblong fruits.
- **Habitat and Distribution:** Found in riparian forests of the Agasthyamala Biosphere Reserve in the southern Western Ghats; strictly endemic to Kerala.
- **Conservation Status:** Known from less than 2 sq. km area with fewer than 10 mature trees; classified as Data Deficient (DD) under IUCN criteria.

About Shendurney Wildlife Sanctuary

- **Location:** Situated in Kollam district of Kerala and forms part of the Agasthyamala Biosphere Reserve in the Western Ghats.
- **Vegetation:** Dominated by evergreen, semi-evergreen and moist deciduous forests.
- **Biodiversity:** Rich in endemic species including lion-tailed macaque, Nilgiri langur, king cobra and rare medicinal plants.
- **Name Origin:** Named after "Chenkurinji" (*Gluta travancorica*), an endemic tree species of the region.

SARTHAK-PDS SCHEME

Context

The **Cabinet Committee on Economic Affairs (CCEA)**, chaired by Prime Minister Narendra Modi, has approved the continuation and integration of public distribution programs into an umbrella scheme called **SARTHAK-PDS.**

About SARTHAK Public Distribution System (PDS) Scheme

- SARTHAK PDS (Scheme for Assistance in Ration Transport and Handling-Income with Automation in PDS) is conceived as an umbrella scheme that integrates two ongoing initiatives

- Assistance to State Agencies for intra-State movement of foodgrains and FPS dealers' margin under NFSA
- Scheme for Modernization and Reforms through Technology in Public Distribution System (SMART PDS)"
- **Aim:** The government aims to create a single administrative structure for improving foodgrain distribution and strengthening implementation of the National Food Security Act, 2013.
- It will run until March 2031.

Key Features

- **Financial Structural Assistance:** Revises and streamlines Central financial assistance to meet the real-world operational expenditures incurred by States and Union Territories for intra-state grain handling, storage, and transport.
- **Enhanced FPS Dealer Economics:** Guarantees higher and standardized dealer commissions linked with mandatory automation frameworks to promote ease of doing business and sustain local ration shops.
- **Advanced Technological Core:** Optimizes daily PDS operations by actively embedding new-age technologies, including:
- **Artificial Intelligence (AI) & Machine Learning (ML):** Used for predictive supply-chain tracking, identifying systemic diversions, and driving algorithmic fraud detection.
- **Natural Language Processing (NLP):** Powers multi-lingual, automated interactive voice responses and grievance registration systems for beneficiaries.
- **Blockchain Technology:** Deployed to construct unalterable ledger entries tracking grain allocations from central warehouses to individual plates, guaranteeing extreme security.
    - It will have three major AI enabled modules named NIRMAL, ASHA and SAKSHAM.
- **Unified Data Architecture:** Mandates a standardized, interoperable database infrastructure spanning all 36 States and UTs. It integrates existing tracking platforms like IM-PDS, Mera Ration, Anna Mitra, and Anna Sahayata.
- **State Command Control Centres:** Establishes centralized control hubs at the state level to give administrators data-driven, real-time oversight over supply chain drops, inventory levels, and operational e-PoS (Electronic Point of Sale) devices.
- **ISO-CertifiedProcess Quality:** Enforces standardized operational guidelines across all supply depots to ensure process transparency, material safety, and institutional accountability.

ONLINE GAMING

Context

The **Supreme Court has upheld the levy of 28% GST** on the full face value of online gaming bets, validating state laws banning online betting and gambling, with the gaming industry facing a potential **tax liability of around Rs. 2.5 lakh crore.**

About Organised Online Gaming

- Online gaming refers to the playing of digital games over the internet, often involving real money stakes.
- Organised online gaming typically includes:
    - **Fantasy Sports:** Platforms like Dream11, where users create virtual teams based on real players.
    - **Real Money Games (RMG):** Card games like Rummy and Poker played for monetary stakes.
    - **Casino-Style Games:** Online versions of traditional casino games.
    - **Skill-Based Games:** Games requiring strategic decision-making, often played for cash prizes.
    - **Esports and Casual Gaming:** Competitive video gaming with prize pools.

Distinction Between Game of Skill and Game of Chance

- **Games of Skill:** Where outcomes depend predominantly on the player's mental ability, knowledge, and judgement (e.g., Rummy, Poker, Fantasy Sports).
- **Games of Chance:** Where outcomes depend largely on luck or random factors (e.g., lotteries, dice games).
    - While games of pure chance have traditionally been regulated as gambling, games of skill have enjoyed legal protection under court rulings.

Regulation of Online Gaming in India

- The regulatory landscape for online gaming in India has been complex and fragmented, involving both state and central laws.
- **Constitutional Framework**
    - **Entry 34 of the State List (Seventh Schedule)** gives states the power to legislate on "Betting and Gambling."
    - **Entry 62** of the State List allows states to impose taxes on betting and gambling.
- **Key Legislation**

- **Promotion and Regulation of Online Gaming Act, 2025:** A central law passed to ban online money games, currently pending notification after Presidential assent.
- **State-Specific Laws:** States like Tamil Nadu, Karnataka, Andhra Pradesh, and Telangana have passed laws banning online gaming with monetary stakes.
- **Information Technology Rules, 2023:** The Centre amended the IT Rules to regulate online gaming intermediaries, requiring self-regulatory bodies to certify "permissible online games."

SC UPHOLDS CONSTITUTIONAL VALIDITY OF SIR TO CONDUCT FREE AND FAIR ELECTIONS

Context

The Supreme Court upheld the constitutional validity of the Election Commission's Special Intensive Revision (SIR) of electoral rolls, recognising it as a mechanism to strengthen electoral integrity and uphold free and fair elections across India

What is SIR?

- **About**: The Special Intensive Revision (SIR) is an extensive voter verification and electoral roll purification exercise undertaken by the Election Commission of India. Its primary objective is to ensure that every eligible citizen is included in the voter list while preventing the inclusion of ineligible or duplicate entries.
- **Methods for updating electoral rolls:**
    - **Summary Revision (Regular Process):** This is a routine exercise carried out annually or before smaller elections. It mainly involves desk-based corrections such as enrolling citizens who have turned 18 and processing applications voluntarily submitted by voters, without conducting comprehensive field verification.
    - **Special Intensive Revision (SIR)**: Unlike routine revisions, the SIR is a large-scale and labour-intensive exercise involving physical verification. Under this process, Booth Level Officers (BLOs) are required to visit each household in the identified area to personally verify the identity and eligibility status of every registered voter.

Stages in the SIR Process

- **Pre-Enumeration**: The Election Commission prepares pre-filled Enumeration Forms (EFs) for all registered voters using existing electoral databases.

- **Door-to-Door Verification**: Booth Level Officers conduct multiple visits to households, distribute the Enumeration Forms, assist residents in linking their details with older electoral records, and record any necessary corrections or updates.
- **Data Collection and Identification**:During verification, BLOs identify voters falling under the "ASDD" category, namely Absent, Shifted, Dead, or Duplicate entries. At the same time, newly eligible citizens are provided Form 6 for fresh registration.
- **Draft Roll and Hearings:** After preliminary scrutiny, a revised Draft Electoral Roll is published. Individuals whose names are deleted or marked for verification are formally notified and given an opportunity to present supporting documents, such as Aadhaar, government identity proofs, or birth records, to establish their eligibility.
- **Publication of Final Electoral Roll:** Once all objections, claims, and appeals are resolved through the prescribed legal process under the supervision of District Magistrates, the final updated electoral roll is officially released.

Key Observations of the Supreme Court

- The Court observed that the SIR does not override the provisions of the Representation of the People Act (RPA), 1950, or the Registration of Electors Rules, 1960.
    - The Bench characterised Article 324 as a "continuous source of authority".
- The Supreme Court accepted the EC's justification for initiating an intensive revision after more than twenty years.
    - It pointed to factors such as rapid urban expansion, large-scale migration, unreported deaths, duplication of voter entries, and frequent modifications in electoral rolls.
- Electoral rolls are dynamic in nature and must be periodically updated to reflect changing demographic and residential realities.

RISING PUBLIC HEALTH EXPENDITURE IN INDIA

Context

India's public expenditure on healthcare has witnessed a substantial rise over the past decade, reflecting a gradual shift towards stronger public financing and improved access to healthcare services.

Key Highlights of the National Health Accounts (NHA) Report

- **Government Health Expenditure:** Healthcare increased from nearly ₹1.3 lakh crore in 2013-14 to around ₹3.85 lakh crore in 2022-23.

- **Health Spending as Share of GDP:** Public health expenditure as a percentage of GDP rose from 1.15% in 2013-14 to 1.43% in 2022-23, reaching 1.48% under the revised GDP base year calculations.
- **Per Capita Health Spending:** Per capita government expenditure on healthcare increased almost 2.7 times, rising from ₹1,042 to ₹2,786 during the decade.
- **Pandemic-Driven Fiscal Push:** The COVID-19 pandemic accelerated public investment in healthcare, with government health expenditure touching 1.84% of GDP in 2021-22, the highest level recorded during the decade.
    - Eg: The increase in expenditure was supported by emergency response initiatives under ECRP-I and ECRP-II.
- **Financial Burden on Households**: The report recorded a substantial fall in Out-of-Pocket Expenditure (OOPE), which refers to direct household spending on healthcare services.
    - Eg: OOPE declined from 64.2% of Total Health Expenditure (THE) in 2013-14 to 43.4% in 2022-23.
- **Government Financing:** The contribution of government expenditure in Total Health Expenditure increased from 28.6% in 2013-14 to 43.7% in 2022-23.
- **Rise in Social Security Expenditure (SSE):** Social Security Expenditure on healthcare increased from 6% of Total Health Expenditure in 2013-14 to 9.9% in 2022-23.
- **Private Health Insurance**: Private health insurance expenditure also rose significantly, increasing from 3.4% to 9.2% of Total Health Expenditure over the decade.
- **Strengthening Primary Healthcare**: Government expenditure on primary healthcare more than doubled, increasing from ₹0.5 lakh crore in 2013-14 to ₹1.4 lakh crore in 2022-23.

Mains Exam Topics

THE BATTLE AGAINST AI MISINFORMATION

Context

Rapid advances in generative AI tools intensified concerns regarding deepfakes, synthetic propaganda, identity misuse and large-scale digital misinformation globally and in India.

How AI is Spreading Misinformation

- **Mass Production of False Content:** Generative AI drastically reduced the cost and effort required to create fake narratives at scale. (**E.g.** AI-generated news websites increased from ~600 in 2024 to over 2,089 in 2025 across 16 languages)
- **Hyper-Realistic Deepfakes:** AI can generate realistic images, videos and audio nearly indistinguishable from authentic content. (**E.g**. Deepfake attacks reportedly occurred every five minutes in 2024)
- **AI-Powered Propaganda Systems:** AI personas can mimic real users and manipulate public opinion through psychological targeting. (**E.g.** China-linked "GoLaxy" system allegedly used AI personas and "LLM grooming" to influence narratives)
- **Rapid Social Media Amplification:** Platforms prioritise engagement over authenticity, enabling misinformation to spread quickly. (**E.g.** AI-generated posts flooding Facebook, Instagram, LinkedIn and X)
- **Manipulation During Crises:** AI-generated fake visuals and videos increasingly used during conflicts and terror incidents. (**E.g.** After the 2025 Pahalgam terror attack, deepfake military videos and fake advisories circulated online)
- **Erosion of Trust ("Liar's Dividend"):** Rise of deepfakes allows even genuine evidence to be dismissed as fake. (Politicians or accused persons can deny authentic videos as AI-generated)
- **Identity Theft & Gendered Harms:** AI tools facilitate impersonation, voice cloning and non-consensual explicit content. (AI-generated fake sexualised images created using women's profile photos)
- **Academic & Institutional Manipulation:** AI can fabricate certificates, research papers and legal documents. (Fake mark sheets, journals and AI-generated legal citations)
- **Rising AI Error & Hallucination Rates:** AI systems themselves increasingly generate false information. (Chatbot falsehood rate reportedly rose from 18% in 2024 to 35% in 2025)

Implications

- **Threat to Democracy & Elections:** AI misinformation can distort electoral discourse and influence voter behaviour.
- **National Security Risks:** Synthetic propaganda can inflame communal tensions and manipulate conflict narratives. (Pahalgam attack misinformation campaign)
- **Damage to Institutional Credibility:** Public trust in journalism, academics, courts and governance may weaken.
- **Rise in Cybercrime & Fraud:** AI-driven phishing, impersonation and document forgery becoming more sophisticated. (Digital document forgery rose by 244% in one year)
- **Violation of Privacy & Personality Rights**: Unauthorised use of voice, likeness and personal data threatens dignity and privacy.
- **Psychological & Social Polarisation:** AI-driven content can deepen fear, outrage and communal divisions.

Government Measures

- **IT Rules, 2026:** Mandate disclosure labels for AI-generated or altered content to improve transparency and reduce deception.
    - introduced metadata tracing requirements for AI-generated content. (Aims to identify origin and modification history of synthetic media)
- **Rapid Takedown Mechanism:** Platforms must remove synthetic or manipulated content within three hours upon government or court orders. (Introduced after concerns over rapid spread of deepfakes during crises and elections)
- **User Grievance Redressal:** Social-media intermediaries required to resolve complaints related to harmful AI-generated content within 36 hours.
- **DPDP Act, 2023:** Strengthens accountability for misuse of personal data, voice and likeness by AI systems. (Important in cases involving AI-generated fake celebrity or individual images)
- **AI Governance Guidelines (2025):** MeitY proposed a risk-based AI governance framework for regulating high-risk AI applications.
- **MeitY Action Against Platforms**: Government increasingly seeking transparency from AI platforms regarding moderation and filtering systems. (MeitY issued notices to X after Grok-generated explicit deepfake images targeted an Indian user)
- **Safe Harbour Accountability Debate:** Government examining limits of intermediary immunity under Section 79 of IT Act for platforms embedding AI tools directly.

- **PIB Fact-Check & Crisis Monitoring:** PIB actively counters viral misinformation during sensitive events. (PIB identified multiple fake AI-generated narratives after the 2025 Pahalgam terror attack)

Way Forward

- **Build a Tiered Risk Classification Framework:** High-risk AI systems should face stricter regulation before deployment. (AI-generated content during communal tensions, elections or national-security crises should require mandatory compliance under MeitY's 2025 AI Governance Guidelines)
- **Reimagine Platform Liability**: Platforms embedding generative AI tools should face greater accountability instead of claiming intermediary immunity.
- **Crisis Disinformation Protocol:** During emergencies or communal crises, social-media platforms should rapidly detect and suppress verified synthetic misinformation. (Delayed response during the 2025 Pahalgam attack allowed fake military videos and advisories to spread widely)
- **Independent AI Safety Oversight**: AI Safety Institute proposed under India's AI Governance Guidelines can independently verify synthetic content instead of leaving decisions solely to governments or platforms.
- **Strengthen Digital & AI Literacy:** Citizens should be trained to critically verify online information before sharing. (Necessary to counter deepfakes, AI scams and manipulated narratives)
- **Global Cooperation on AI Governance**: Countries should develop common standards for deepfake regulation, AI transparency and platform accountability.

Global Best Practices to Tackle AI-Driven Misinformation

- **EU Digital Services Act (DSA):** Imposes strict accountability on large digital platforms for removing harmful and misleading AI-generated content.
- **U.K. AI Safety Institute**: Conducts independent testing and risk assessment of advanced AI systems and deepfake technologies.
- **Mandatory AI Labelling (Meta, YouTube, TikTok):** Platforms label AI-generated or altered images/videos to improve transparency.
- **Finland's Media Literacy Model:** Integrates misinformation detection and digital literacy into school education and public campaigns.
- **Election AI Disclosure Rules (U.S. & EU**): Require disclosure of AI-generated political advertisements and campaign material.
- **UNESCO & OECD AI Ethics Frameworks:** Promote global principles for trustworthy,

transparent and human-centric AI governance.