ujiyari

UPSC & STATE PCS CURRENT AFFAIRS · UJIYARI.COM

EDITORIAL ANALYSIS

Quantum-Safe Thinking: India's Post-Quantum Cryptography Roadmap and the Harvest-Now-Decrypt-Later Risk

THE HINDU

29 May 2026 · SCIENCE & TECH · SECURITY & DEFENCE · GS3

CURATED & WRITTEN BY

Bharat Choudhary

UPSC Educator & Content Creator

linkedin.com/in/epicbharat

ALSO FROM THE CREATOR

BharatNotes

Free UPSC notes, MCQs, PYQ analysis. **100% Free.**

bharatnotes.com →

ADVERTISE

Advertise with Ujiyari

Reach thousands of UPSC aspirants daily.

epicbharat@gmail.com

Quantum-Safe Thinking: India's Post-Quantum Cryptography Roadmap and the Harvest-Now-Decrypt-Later Risk

The Hindu 29 May 2026 GS3

TH The Hindu | 3 tags ▾

INTERVIEW ANGLE

"If quantum computers powerful enough to break current RSA encryption are still 5-15 years away, but adversaries are already harvesting encrypted data to decrypt later — what should India's migration timeline to post-quantum cryptography be, and is the DST Task Force's roadmap aggressive enough?"

THE HINDU

| Editorial | May 29, 2026

The

DEPARTMENT OF SCIENCE AND TECHNOLOGY (DST) TASK FORCE ON POST-QUANTUM CRYPTOGRAPHY (PQC)

released its roadmap recently, providing India's **first comprehensive migration plan** away from classical asymmetric cryptography that quantum computers will eventually break. The Hindu welcomes the move but warns that **India's critical digital infrastructure — banking, Aadhaar, defence communications, digital governance** — remains exposed to **"harvest-now-decrypt-later"** attacks. **Adversaries are already collecting encrypted data today** to decrypt once quantum hardware matures. The editorial urges accelerated migration timelines and indigenous capacity in quantum-resistant standards.

THE ARGUMENT IN ONE LINE

The cryptographic threat from quantum computing is not "future" — it is **present and accumulating**, because data encrypted today with broken algorithms is being stockpiled for future decryption; India's PQC migration must therefore be measured in **months, not decades**.

WHAT IS "HARVEST-NOW-DECRYPT-LATER" (HNDL)?

PHASE	ACTION	THREAT
Phase 1 (today)	Adversary intercepts encrypted traffic — bank transactions, government communications, defence data, citizen records	Data is unreadable but stored
Phase 2 (5-15 years)	Cryptographically Relevant Quantum Computer (CRQC) becomes available	Stored encrypted data is decrypted retrospectively
Impact	Banking, identity, defence, intellectual property compromised — even if encryption was current at time of capture	Strategic intelligence gain

This is why **the threat is present**, not future: data sensitive **20+ years from now** (defence plans, citizen biometrics, M&A deals, deep IP) must be encrypted **today** with PQC algorithms.

WHY CLASSICAL ENCRYPTION WILL BREAK

ALGORITHM	USED IN	QUANTUM
RSA (Rivest-Shamir-Adleman)	Banking, HTTPS, digital signatures	**Shor's Algorithm** breaks it in polynomial time on a CRQC
ECC (Elliptic Curve Cryptography)	Modern HTTPS, blockchain, mobile	Also breakable by Shor's
Diffie-Hellman key exchange	TLS, VPNs	Breakable
AES-128 / AES-256 (symmetric)	Stored data, file encryption	**Grover's Algorithm** halves effective key length — AES-256 still safe, AES-128 weakened
SHA-256 (hash)	Blockchain, digital signatures	Grover's reduces security but practical resistance survives

The catch: **classical symmetric encryption (AES) is largely safe** with longer keys. The **asymmetric (RSA, ECC) layer is broken** — and that layer is what makes the internet work (key exchange, certificate authorities, digital signatures).

WHAT IS POST-QUANTUM CRYPTOGRAPHY (PQC)?

PQC = **cryptographic algorithms that run on classical computers but resist quantum attacks**. They use mathematical problems that are hard even for quantum computers:

FAMILY	APPROACH	STATUS
Lattice-based	Shortest Vector Problem (SVP), Learning with Errors (LWE)	**NIST winners: ML-KEM (Kyber), ML-DSA (Dilithium)**
Hash-based	One-time signature trees	**SLH-DSA (SPHINCS+)** standardised
Code-based	Error-correcting codes	Classic McEliece — large keys
Multivariate	Solving multivariate equations	Falcon-style
Isogeny-based	Elliptic curve isogenies	SIKE broken (2022); approach now under review

In **August 2024**, the **US NIST** published the **first three PQC standards**:

- **FIPS 203** — ML-KEM (key encapsulation)
- **FIPS 204** — ML-DSA (digital signatures)
- **FIPS 205** — SLH-DSA (stateless hash-based signatures)

This kicked off the global PQC migration era.

THE DST TASK FORCE — INDIA'S PLAN

ELEMENT	DETAIL
Parent ministry	Department of Science and Technology (DST)
Coordinating bodies	DST + MeitY + NSCS (National Security Council Secretariat) + RBI + CERT-In
Task Force composition	Cryptographers from IISc, IIT Madras, IIT Bombay, ISI Kolkata + DRDO scientists + RBI/SEBI representatives + industry experts
Roadmap horizon	**2026-2035** (10-year migration plan)
Phases	Inventory → Pilots → Hybrid deployment → Full migration
Standards adoption	**NIST PQC standards** (ML-KEM, ML-DSA, SLH-DSA) recommended as baseline
Indigenous standards	Encouraged for sovereign use cases — defence, election systems
Critical sectors flagged	Banking, Aadhaar/UIDAI, defence communications, electricity grid, telecom, healthcare

WHY SPEED MATTERS

INDICATOR	WHAT IT IMPLIES
CRQC arrival estimate	**2030-2040** (NIST, NSA, GCHQ converge on this range)
Sensitive-data shelf life	25-50 years (Aadhaar, defence plans, IP)
PQC migration time	**5-10 years** for large institutions
Math	If CRQC arrives 2035 and migration takes 7 years, we should start by **2028** at the latest — but data captured today is already at risk

Conclusion: Migration must begin **now**, not when the quantum threat materialises.

INDIA'S SPECIFIC VULNERABILITIES

SECTOR	SPECIFIC RISK
Aadhaar (UIDAI)	130+ crore biometric records under classical encryption — irreplaceable if compromised
Banking + UPI	All inter-bank communications, KYC, transaction signatures
Defence	Strategic communications, command-and-control, ISR data
Election systems	EVM-VVPAT communication, voter database integrity
Telecom	All voice/data infrastructure key management
Health (ABDM)	EHR (electronic health records) — long shelf life
Diplomatic	MEA cable encryption, sensitive treaty negotiations
Critical Infrastructure	Power grid, water utilities, oil/gas SCADA

INDIA'S QUANTUM STACK — A RECAP

INITIATIVE	YEAR	OUTLAY	FOCUS
National Mission on Quantum Technologies and Applications (NM-QTA)	2020 (announced)	₹8,000 crore over 5 years	Quantum computing + comms + materials + sensing
National Quantum Mission (NQM)	**April 2023** (Cabinet)	**₹6,003 crore** (revised)	4 Thematic Hubs — Computing, Comms, Sensing & Metrology, Materials & Devices
DRDO Quantum Key Distribution (QKD)	2022 onwards	—	Defence-grade QKD demonstrations
ISRO Quantum Communication	2023 onwards	—	Satellite-based QKD
DST PQC Task Force	2026	—	Migration roadmap

WHAT COULD GO WRONG

RISK	SUBSTANCE
Delay	Migration phases stretch beyond CRQC arrival
Skill gap	India has <500 trained PQC engineers (estimated); needs 10,000+
Standards lag	Reliance only on NIST may not capture India-specific use cases
Hybrid pitfalls	Classical-PQC hybrid systems can fail in unexpected ways
Foreign dependence	Hardware Security Modules (HSMs), root certificates often from foreign vendors
Quantum-readiness audit fatigue	Institutions may treat audit as compliance, not security

THE INTERNATIONAL PICTURE

COUNTRY	STATUS
USA	NSA's CNSA 2.0 (2022) mandates PQC migration; NIST standards 2024
EU	ENISA PQC guidance; EU Cybersecurity Act framework
China	Indigenous SM2/SM9 PQC variants; aggressive deployment
UK	NCSC guidance; mid-decade migration
Singapore	National Quantum Strategy 2024
India	DST PQC Roadmap 2026

WIDER SIGNIFICANCE

- **Sovereign cyber capacity** — quantum-safe cryptography is the new digital sovereignty layer.
- **Strategic stability** — cryptographic compromise can shift military balances overnight.
- **Economic competitiveness** — Indian financial sector cannot afford to be quantum-vulnerable.
- **Standards leadership** — India can lead Global South PQC adoption through capacity-sharing.
- **Defensive doctrine** — Information Operations doctrines must integrate quantum-cyber threats.

WHAT THE EDITORIAL DEMANDS

DEMAND	SUBSTANCE
Aggressive migration timeline — target full PQC by **2030**, not 2035	
Skilling mission — 10,000 PQC engineers by 2028	
National HSM mission — indigenous hardware security modules	
Quantum-readiness audit of all critical infrastructure	
Standards diplomacy — push for India-favourable standards in ISO/ITU	
R&D funding — PQC research at IITs, IISc, ISI Kolkata	
CERT-In PQC division — dedicated incident response capability	

WAY FORWARD

- **Crypto-agility** — system architectures that can swap algorithms easily.
- **Inventory mandate** — every critical institution to publish cryptographic inventory by 2027.
- **Hybrid deployment** — classical + PQC in parallel for 5-7 years.
- **Procurement standards** — government and BFSI to specify PQC-readiness in new procurements from 2027.
- **Quantum cyber doctrine** — NCIIPC + NSCS to issue protocols.
- **Indigenous testing labs** — STQC + CDAC + IIT Bombay to certify PQC implementations.

UPSC RELEVANCE

GS Paper 3 — Science & Technology / Security:

- Awareness in the fields of IT, computers, robotics, AI, nano-tech, bio-tech.
- Achievements of Indians in science & technology; indigenization of technology.
- Basics of cybersecurity; data and information security.

Analytical hooks for Mains:

- Quantum threats to existing cryptographic architecture.
- Post-quantum migration as digital sovereignty.
- India's National Quantum Mission and the PQC adjacent challenge.

FACTS CORNER

DST PQC Task Force roadmap released May 2026.

CRQC (Cryptographically Relevant Quantum Computer) estimated arrival: 2030-2040.

NIST PQC standards (Aug 2024): FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), FIPS 205 (SLH-DSA).

NIST PQC competition launched: 2016.

Shor's Algorithm breaks RSA, ECC, Diffie-Hellman in polynomial time on a CRQC.

Grover's Algorithm halves effective key length for symmetric encryption — AES-256 remains safe.

National Quantum Mission (NQM): ₹6,003 crore, April 2023 Cabinet approval; 4 Thematic Hubs.

CSE/NSA mandate (USA, CNSA 2.0): PQC by 2030 for national security systems.

HNDL (Harvest-Now-Decrypt-Later): adversaries collecting encrypted data today for future decryption.

Share as image

Editorial source: The Hindu, May 29, 2026 | Cross-link: Daily May 29 — Odisha-Intel-3DGS semiconductor MoU

Source: Quantum-Safe Thinking: India's Post-Quantum Cryptography Roadmap and the Harvest-Now-Decrypt-Later Risk — Ujiyari.com | Free UPSC & State PCS Editorial Analysis

PRACTICE TODAY'S QUIZ

Take the 29 May 2026 Quiz →

RELATED DAILY ARTICLES

29 May Current Affairs Today — May 29, 2026

29 May International Day of UN Peacekeepers — Two Indian...

29 May Odisha Signs Semiconductor Substrate MoU with Intel and...

29 May IAF-IIT Bombay Predictive Maintenance Pact for Su-30...

← NEWER EDITORIAL
S.Y. Quraishi on SIR: Electoral Rolls, Citizenship, and the...

OLDER EDITORIAL →
India's Water Stress: Heatwaves, Reservoir Crisis, and the...

CURATED & WRITTEN BY

Bharat Choudhary

UPSC Educator & Content Creator

linkedin.com/in/epicbharat

Read Full Article on Ujiyari →

https://ujiyari.com/editorials/2026/05/hindu-quantum-safe-thinking-dst-task-force-2026/

ALSO FROM THE CREATOR

BharatNotes

Free UPSC study platform — subject-wise notes across all 4 GS papers, Prelims MCQs, Mains answer frameworks, PYQ analysis & progress tracking. **100% Free • No Login Required.**

Start Preparing → bharatnotes.com

OPPORTUNITY

Advertise with Ujiyari

Reach **thousands of serious UPSC & State PCS aspirants** daily through our PDFs, website, and social channels.

Ideal for: Coaching institutes • EdTech platforms • Book publishers • Exam prep apps

epicbharat@gmail.com

Write to us for rates & media kit