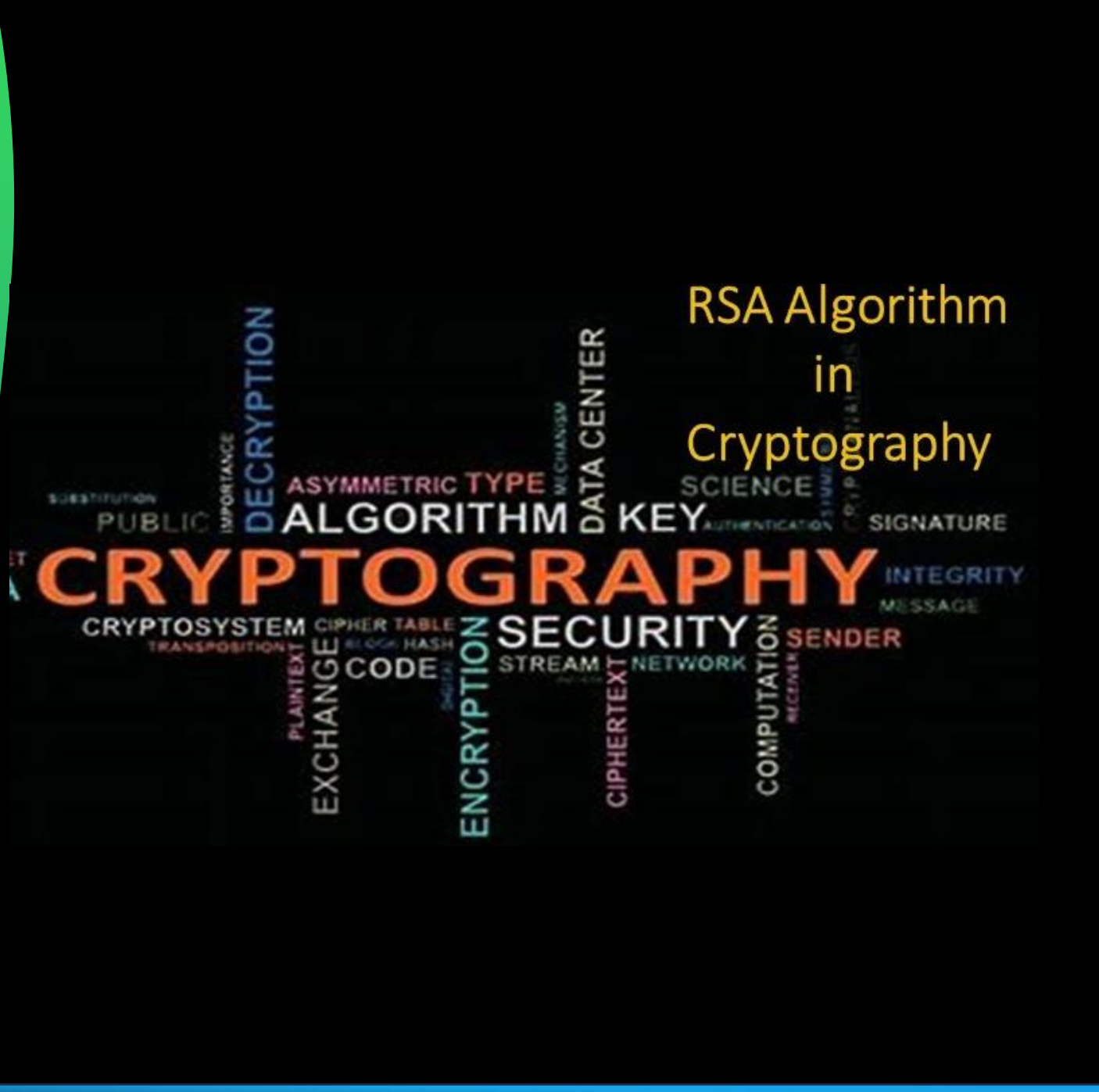
The Quantum Disruption:
How Quantum Computing Will Redefine Cybersecurity

How Do We Protect Our Data?

History of Cryptography

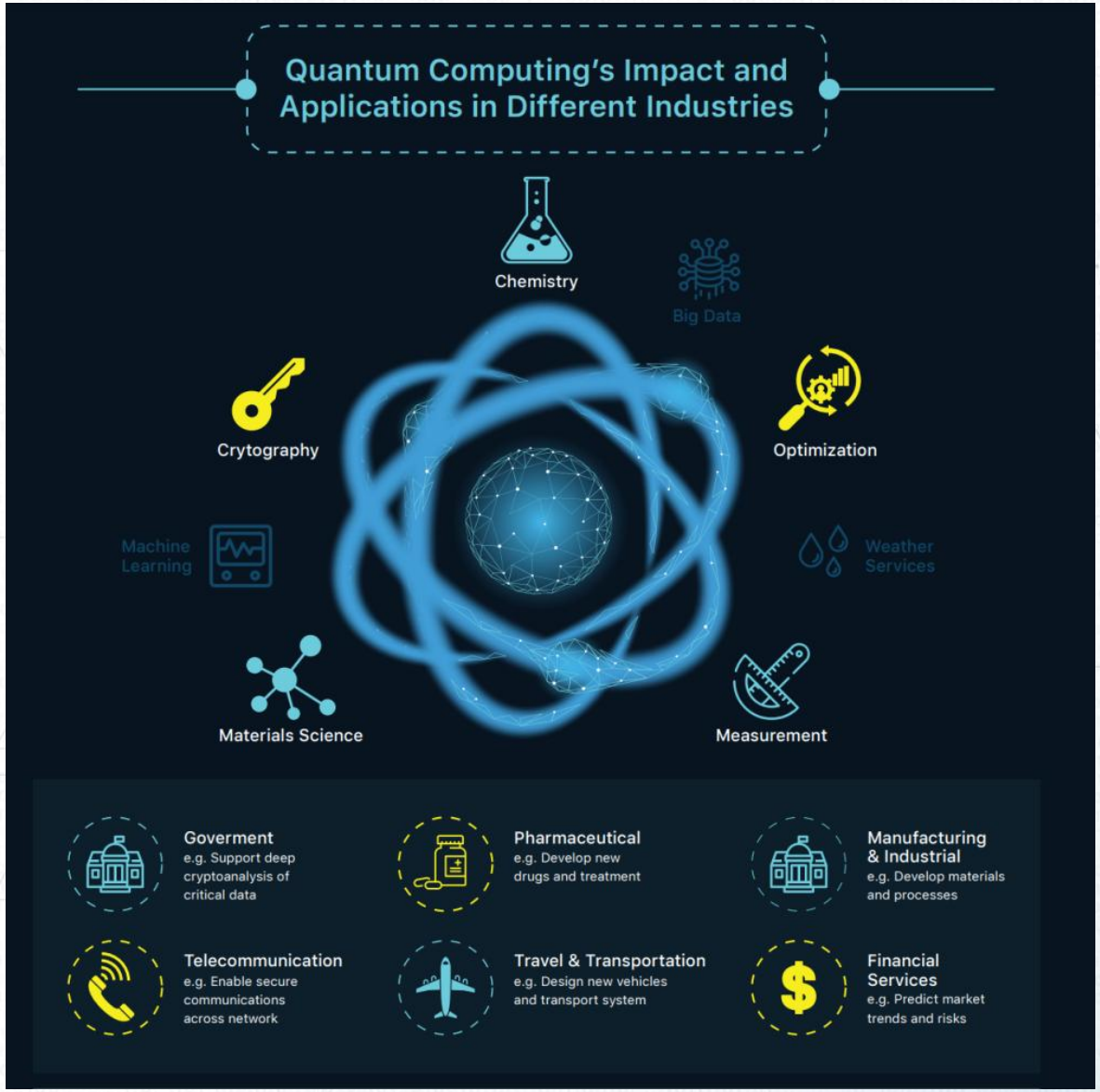
Current Cryptography



Quantum Computing: A New Era of Unthinkable Power

- What is Quantum Computing?
  - Uses quantum physics to process information fundamentally differently.
- Classical vs Quantum
  - Classical uses bits (0 or 1);
  - quantum uses qubits (0 and 1 at the same time).
- Why is Quantum Different?
  - Explores many outcomes in parallel instead of step-by-step.

Quantum Computing's Disruptive Potential



The Cryptographic Impact of Quantum Computing

Create Digital Distrust by breaking all Encryption and Authentication

- Broken Encryption – Quantum computers could break widely used encryption protocols (e.g., RSA, ECC), exposing sensitive financial data.
- Compromised Transactions – Digital signatures and secure payment systems may become vulnerable.
- Data Theft & Fraud – Hackers with quantum capabilities could access stored financial records if not protected by strong post quantum encryption
- Network Security Broken – All secure methods of communication within an institute or external can be intercepted if encryption is broken
- Application Security Compromised – When encryption is compromised by quantum computing, various banking applications become vulnerable, leading to operational disruptions, financial losses, and loss of trust.

Why Do you Care?

Critical Banking Assets Rely on Cryptography

- **Online Banking Platforms** – Encryption protects customer authentication and transaction security.
- **Payment Systems (SWIFT, VISA, Mastercard, etc.)** – Secured by cryptographic protocols to prevent fraud.
- **ATM Networks** – Secure PIN-based transactions rely on encryption to prevent unauthorized access.
- **Digital Identity Verification** – Uses cryptographic signatures for secure logins and fraud prevention.
- **Interbank Communication & Transfers** – Secure messaging (e.g., SWIFT) depends on cryptographic authentication.
- **Blockchain & Cryptocurrencies** – Public-private key cryptography secures digital assets and transactions.
- **Secure Email & Communication Systems** – Banking correspondence is encrypted to prevent eavesdropping.

What is the Urgency?

Q-Zero is getting closer (2030 or earlier)

Q-Zero: The Moment Quantum Computers Break Classical Encryption

Q-Zero refers to the point when quantum computers become powerful enough to **break classical encryption standards** (like RSA-2048, ECC, and AES-256), posing an immediate threat to banking security, financial transactions, and digital assets.

Indicators That Q-Zero is Approaching:

✅ Quantum computers achieve **1 million+ stable qubits**, overcoming error correction challenges.

✅ Shor's Algorithm runs efficiently on quantum hardware, making **RSA-2048 breakable in hours or days**.

✅ Government agencies and cybercriminals start using quantum decryption for financial espionage.

✅ Legacy cryptographic infrastructure begins to **fail under quantum attacks**.

✅ Mass migration to **post-quantum cryptography (PQC)** becomes a global financial priority.

What Should we do?

Roadmap to Quantum-Proof a Bank Before Q-Zero

1. **Quantum Education: Establish a Quantum Safe Program**
   a. Create awareness in Board and EXCO about Q-Zero and its potential impact to your institute
   b. Do Board and EXCO training demystifying Quantum computing and its risks
2. **Quantum Discovery: Create a Crypto bill of Material (CBOM)**
   a. Regulatory compliance. Regulations are being drafted across the globe regarding understanding where you use encryption within your firm. This will allow you to understand the extent of remediation that will be needed and help create a Quantum remediation roadmap
   b. Create a risk-based Quantum score to help prioritize remediation
   c. Write legal letters to all your 3rd party vendors who you are dependent on to become quantum safe demanding their timelines for becoming Quantum Safe
3. **Quantum Ready: Create remediation program**
   a. With the CBOM and risk-based analysis create a program to remediate all old/deprecated encryption in your environment

Staying safe with Quantum

Post-quantum (PQ) cryptographic algorithms have security based on mathematical problems that are widely believed to be difficult for a quantum adversary.
NIST announced the draft finalization of four algorithms:

- **CRYSTALS-Kyber** for general encryption (covered in FIPS 203)
- **CRYSTALS-Dilithium** for digital signatures (covered in FIPS 204)
- **SPHINCS+** for digital signatures (covered in FIPS 205)
- **FALCON** for digital signatures (expected to be covered in a FIPS draft in 2024)

Global Momentum

National Regulations for PQC Transition

- **United states**
  - Executive Order 14028
  - CISA PQC Initiative guides critical infrastructure toward post-quantum readiness.
- **European Union**
  - European Commission is working toward finalizing PQC mandates across the EU(ENISA)
- **Australia**
  - National roadmap targeting full PQC transition by 2030, led by the ACSC..
- **UAE**
  - Released the Cryptography Executive Regulation in 2023 — one of the first in the Middle East.
- **China**
  - Enforced the Cryptography Law, emphasizing sovereign control and PQC research.
- **United Kingdom**
  - NCSC has issued guidance encouraging early PQC adoption across public sector and critical infrastructure.

Conclusion

- Quantum computing represents a significant leap forward in computational power and efficiency.
- Its impact will be felt across multiple sectors, including cybersecurity, healthcare, and optimization problems.
- Key players in the field are driving the development of quantum technologies, making it a rapidly evolving area of study.
- Quantum readiness roadmap and plan is necessary for organizations to tackle the problem.

Are You Ready to Combat Quantum Threats with Chronos?

Connect with us for **Innovative Security Solutions**

noorim@doyencyber.com

THANK YOU

doλencyber