Quantum Key Distribution Technology

For Prelims: Quantum Key Distribution Technology, Quantum Technology and its applications, Qubits.

For Mains: Quantum Key Distribution Technology and its benefits and needs, applications of quantum technology.

Why in News?

Recently, a joint team of scientists from **Defence Research and Development Organisation (DRDO)** and **Indian Institute of Technology (IIT) Delhi**, for the **first time** in the country successfully **demonstrated Quantum Key Distribution link** between Prayagraj and Vindhyachal in Uttar Pradesh, a distance of more than 100 kilometres.

- With this success, the country has demonstrated indigenous technology of secure key transfer for bootstrapping military grade communication security key hierarchy.
- Earlie, **China's satellite Micius** had sent light particles to Earth to establish the world's most secure communication link.

What is Quantum Key Distribution Technology?

- QKD, also called **Quantum Cryptography,** is a mechanism to **develop secure communication.**
- It provides a way of **distributing and sharing secret keys** that are necessary for cryptographic protocols.
    - **Cryptography** is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents.
    - **Cryptographic algorithms** and protocols are necessary to keep a system secure, particularly when communicating through an untrusted network such as the Internet.
- The **conventional cryptosystems** used for data-encryption rely on the complexity of mathematical algorithms, whereas the security offered by quantum communication is based on the laws of Physics.

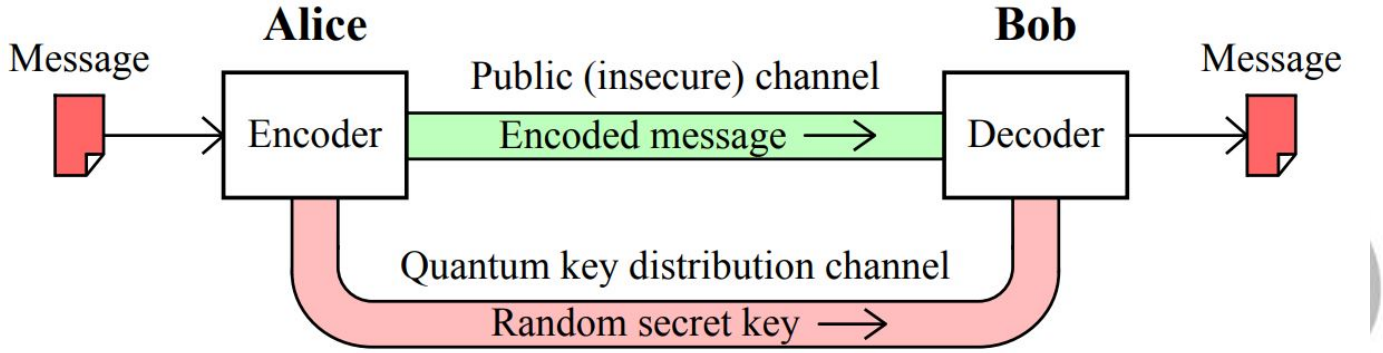
What are the Two Main Categories of QKD?

- **Prepare-and-Measure Protocols:**
    - It focuses on **measuring unknown quantum states**. This type of protocol can be **used to detect eavesdropping (spying)**, as well as how much data was potentially intercepted.
- **Entanglement-based Protocols:**
    - It focuses on **quantum states in which two objects are linked together,** forming a combined quantum state.
    - The concept of entanglement means that **measurement of one object thereby affects the other.** In this method, if an eavesdropper accesses a previously trusted node and changes something, the other involved parties will know.

How does the Quantum Key Distribution Work?

- In the QKD, encryption keys are sent as **'qubits' (or quantum bits)** in an **optical fibre.**
  - **Qubits** -- the **equivalent of bits in a binary system.**
  - **Optical fibers** are capable of transmitting more data over longer distances and faster than other mediums. It works on the **principle of total internal Reflections.**
- QKD implementation **requires interactions between the legitimate users**. These interactions need to be authenticated. This can be achieved through various cryptographic means.
  - QKD **allows two distant users,** who do not share a long secret key initially, to produce a common, random string of secret bits, called a secret key.
- The end-result is that **QKD can utilize an authenticated communication channel** and transform it into a secure communication channel.
- It is designed in a way that **if an illegitimate entity tries** to read the transmission, it will disturb the qubits – which are encoded on photons.
- This will **generate transmission errors,** leading to legitimate end-users being immediately informed.

//



Why is QKD Needed?

- QKD is **essential to address the threat** that rapid advancement in Quantum Computing poses to the security of the data being transported by various critical sectors through the current communication networks.
  - **Quantum Technologies** can broadly be divided into four verticals viz. Quantum Computing, Quantum Communications, Quantum Sensors and Quantum Materials.
- The technology would be useful in **enabling various** start-ups **and small and medium enterprises in the domain of quantum information.**
- It will enable security agencies to **plan a suitable quantum communication network** with indigenous technology backbone.
- The **encryption is unbreakable** and that's mainly because of the way data is carried via the photon.
  - A **photon cannot be perfectly copied** and any attempt to measure it will disturb it. This means that a person trying to intercept the data will leave a trace.

What are the Challenges associated with the QKD?

- **Integration of QKD Systems into Current Infrastructure:**
  - For now, it is **currently difficult to implement** an ideal infrastructure for QKD.
  - QKD is perfectly secure in theory, but in practice, **imperfections in tools like single photon detectors** create many **security vulnerabilities.**
- **Distance in which Photons Can Travel:**
  - **Modern fiber optic cables are typically limited** in how far they can carry a photon. Commonly, this range is seen to be upward of 100 km.
- **Use of QKD:**
  - QKD **relies on already having a classically authenticated channel** of communications

established.
        - This means that **one of the participating users** has probably already exchanged a symmetric key in the first place, creating a sufficient level of security.
        - A system can **already be made sufficiently secure without QKD** through using another advanced encryption standard.
    - However, as the **use of quantum computers becomes more frequent, the possibility that an attacker could utilize quantum computing's ability** to crack into current encryption methods rises -- making QKD more relevant.

Way Forward

- The power of **startups and Big Tech corporations** involved in developing quantum technology and applications must be harnessed.
- The **focus should be to develop an overarching strategy** for the next 10-15 years. The strategy must ensure that there is no misallocation of resources and that the efforts put in are concentrated in key areas that provide both economic and strategic benefits.

Source: PIB