Quantum Key Distribution

Why in News

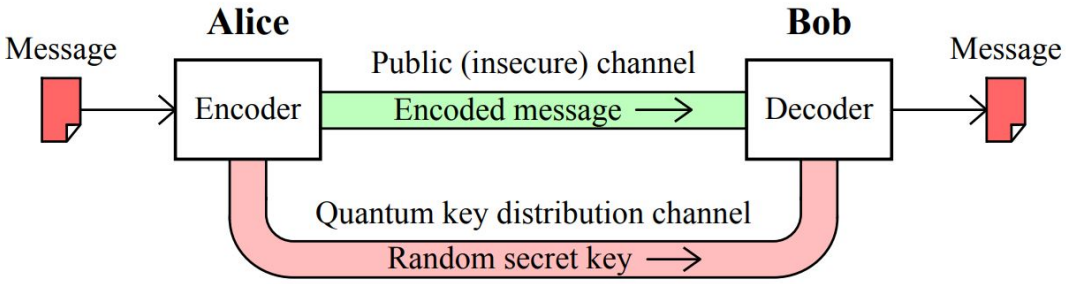
Recently, the government has inaugurated **C-DOT**'s (**Centre for Development of Telematics**) Quantum Communication Lab and unveiled the indigenously developed **Quantum Key Distribution (QKD) solution**.

> The government has also allocated **USD 1 billion for the National Mission on Quantum Technologies and Applications** spanning over a period of 8 years.

Key Points

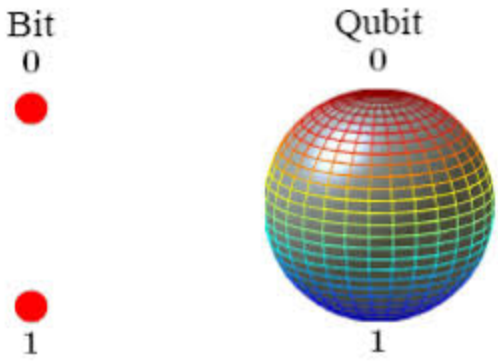
- **About:**
  - QKD, also called **Quantum Cryptography**, is a mechanism to develop secure communication.
  - It provides a way of **distributing and sharing secret keys** that are necessary for cryptographic protocols.
    - **Cryptography** is the **study of secure communications techniques** that 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.**

- **Mechanism:**
  - In the QKD, **encryption keys are sent as** '**qubits' (or quantum bits) in an optical fibre.**
    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.**



Qubits:

- **Conventional computers process information in 'bits' or 1s and 0s**, following classical physics under which our computers can process a '1' or a '0' at a time.
- Quantum computers compute in **qubits**. They exploit the properties of quantum mechanics, the science that governs how matter behaves on the atomic scale.
  - In this scheme of things, **processors can be a 1 and a 0 simultaneously,** a state called **quantum superposition**.
  - Because of quantum superposition, a quantum computer — if it works to plan — **can mimic several classical computers working in parallel**.



- **Need:**
  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.
- **Benefits:**
  - The technology would be useful in **enabling various start-ups and small and medium enterprises** in the domain of quantum information.
  - It is expected **to create a definition of standards and formulate crypto technology-related** policies.
- **Significance:**
  - **Detection of Leak:**
    It **allows the detection of data leak** or **hacking** because it can detect any such attempt.
  - **Predetermined Error Levels**:
    It also **allows the process of setting the error level** between the intercepted data.
  - **Unbreakable Encryption:**
    - 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.

Source: ET