QUANTUM COMPUTING TO ACHIEVE UNBREAKABLE ENCODING TECHNOLOGY

1. **Objective** Development of Quantum cryptography viz, Quantum Key Distribution (QKD) Technique.

2. Description

Quantum computing could be a transformation technology for Defence. Quantum cryptography promises to revolutionise secure communications by providing security based on the fundamental laws of physics instead of the current state of mathematical algorithms/computing technology. The domain knowledge w.r.t. development related activities are available with various agencies, albeit in specialised domains. Further, this being a niche technology, readymade solutions/critical tools would be either proprietary or available only through very limited sources.

Traditional cryptography creates security protocols by using the principles of mathematics, computing science and electronics. This form of cryptography relies heavily on the complexity of factoring integers whereas QKD is bases on the fundamental laws of physics. (The Quantum cryptography technology is primarily based on Heisenberg's uncertainty principles wherein, measuring one variable necessarily affects the other). The technology facilitates secure key distribution even between non-speaking entities, which is not possible in conventional systems. The uniqueness of Quantum cryptography also lies in its ability of two communicating user to detect the presence of third party trying to gain knowledge of the key. The technology can solve the key distribution problem i.e, once key is securely received, it can be used to encrypt messages transmitted by conventional means.

Quantum computing uses properties of subatomic particles like superposition and entanglement to encode and manipulate data. The technology is envisaged to solve the secure key distribution problem i.e, once key is securely received, it can be used to encrypt messages transmitted by conventional means.

The quantum cryptography essentially means distributing secret keys over a public communication channel and not encrypting of qbits like in the classical cryptography. The main task of the QKD protocols is to achieve an absolute secure key exchange process on the quantum channel. The quantum algorithms are being used in space communication mostly to secure key exchange and the values of quantum bits are encoded by photon polarization. The free-space QKD was first introduced over an optical path of about 30 cm in 1991 and since, has been extended to line-of-site (LOS) and beyond ranges, by daylight as well as at night. The satellite based quantum key distribution scheme uses optical devices, improved spatial filtering and narrowband pass filter to control the transmitter lasers. The technology has been discussed as a theoretical possibility for decades and could be realised.

The envisaged advantages of Quantum Cryptography are as follow:-

(aa) Virtuanlly un-hackable.

(ab) Simplicity of operations

(ac) Lesser resources for maintenance.

(ad) Breaking the system is hard due to large numbers of possible keys. (for example, for a key 32 bits long, there could be 232 possibilities).

(ae) Can be used to detect eavesdropping in Quantum Key Distribution.