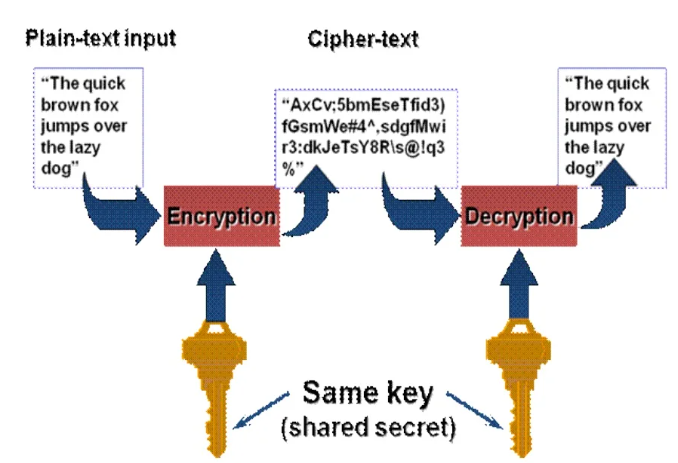
A Review on

‘ QUANTUM CRYPTOGRAPHY ’

Abstract :

In this slide, we review how the laws of Quantum Mechanics allow creating unconditionally secure protocols in cryptography, means, protocols where the security is done by physical laws .We first review the use of Quantum Mechanics to perform unconditionally secure secret key distribution, and we then extend the ideas to other cryptographic tasks including public-key cryptography, digital signatures, and fingerprinting ,data security. Quantum cryptography is one of the emerging topics in the field of computer industry. This paper focus on quantum cryptography and how this technology contributes value to a defense-in-depth strategy pertaining to completely secure .The scope of this paper covers the weaknesses of modern digital cryptosystems, the fundamental concepts of quantum cryptography, the real-world implementation of this technology along with its limitations, and finally the future direction in which the quantum cryptography.

INTRODUTION :

Quantum cryptography is a method of encryption that uses the properties of quantum mechanics to secure and transmit data so that it cannot be hacked or tracked by anyone who shouldn’t have its access. Quantum cryptography is different from traditional cryptographic systems in that it is based on physics, other than mathematics (based on binary digit 0 and 1) . In compare with mathematical encryption it is highly secured model which is based on transfer of photon which is called qubit. Charles H. Bennet and Gilles Brassard developed the concept of quantum cryptography in 1984 as part of a study between physics and information. 

* Quantum cryptography adapts quantum mechanical principles like Heisenberg Uncertainty principle and photon polarization principle to provide secure communication between two parties. The Heisenberg Uncertainty principle and quantum entanglement can be exploited in as system of secure communication often referred to as "quantum Cryptography".
* It is possible to encode information into quantum properties of a photon in such a way that any effort to monitor them disturbs them in some detectable way. This statement is known as the Heisenberg uncertainty principle.
* It works on the principle of polarisation of data in the form of waves in different states so that when anyone wants to compromise the data then user gets alert that the data is compromised by the states of waves.

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. In the QKD, encryption keys are sent as **‘qubits’ (or quantum bits)** in an optical fibre .  the**equivalent of bits in a binary system.** 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 cryptography obtains its security from the fact that each qubit is carried by single photon. Each photon will be altered as soon as it is read. Keys are shared using quantum channel and encrypted messages are sent using public channel. Both sender and receipient can discuss results and their use of basis over public channel to make the system more robust.

LIMITATIONS:

Since it is very secured but it also some drawbacks . Those are:

* **Maintaining A Quantum Communication Network:**

The cost of creating and maintaining a quantum communication network is a significant factor that needs to be addressed. Using existing legacy communication infrastructure is a less expensive approach.

* **Transferring Quantum States:**

Another significant challenge that faces quantum cryptography and quantum computing is an effective method to transfer quantum states from one place to another via a single photon channel at rates greater than 1 Gbit/s (1 Terabit per second). The most common type of light source used to create a single photon is the Alexandrite laser. The primary limitation of this light source is that it produces light of relatively low intensity and has a relatively low quantum yield.

* **A Means For Secure Encryption :**

The third challenge facing the implementation of quantum cryptography is the need to understand better how to utilize this emerging technology to meet all data security protection requirements.

* **Public Trust:**

A hurdle that all new technologies must overcome eventually is public adoption. The widespread implementation and use of quantum key distribution systems and other quantum protocols still face issues with trust, particularly from the public sector. Potential users and clients need assurance from government agencies that data encryption will be secure within the machines on which this new form of PKI (public key infrastructure) will reside.

* **Sharing Infrastructure:**

The final challenge in quantum cryptography is the need for shared infrastructure required for the communication between several applications. Quantum cryptographic standards, such as post-quantum cryptography and quantum-public key cryptosystems, utilize public-key encryption as part of a larger data security model in which multiple machines can securely share both encryption and decryption keys.

* **Changes in polarization and error rates:**

Photons may change polarization in transit, which potentially increases error rates.

* **Number of destinations:**

 It is not possible to send keys to two or more locations in a quantum channel.

ADVANTAGES:

**Benefits of quantum cryptography :**

Benefits that come with quantum cryptography include the following:

* **Provides secure communication:**

 Instead of difficult-to-crack numbers, quantum cryptography is based on the laws of physics, which is a more sophisticated and secure method of encryption.

* **Detects Spy:**

 If a third party attempts to read the encoded data, then the quantum state changes, modifying the expected outcome for the users.

* **Offers multiple methods for security:**

There are numerous quantum cryptography protocols used. Some, like QKD, for example, can combine with classical encryption methods to increase security. The performance of such cryptography systems is continuously improved. This results into its quick adoption in encrypting most valuable secrets of the government and industries.

CONCLUSION:

Quantum cryptography has become the first commercial application of the principles of quantum information. A best level of security has been made possible by using the very basic principles of quantum physics. Any spy, allowed to perform any possible attack, will be revealed. Even better, QKD allows one to quantify the maximum amount of information which might have leaked to the spy. The systems which are operative at the moment use either a fiber channel or a connection through free space to transmit weak light signals. Elongate laser pulses can be used, supported by additional protocol features, and allow the design of robust, cost-effective systems. High-speed point-to-point connections, very long connections over more than 100 m and networks in metropolitan areas have been developed and will be connected by satellite links, enabling global secure communication in the future.