Neil Gupta
10445674.

HomeWork 10

A1) In private key cryptography there is only one private key involved between sender and receiver to encrypt and decrypt the data. It is also symmetric key encryption. It is comparitevly faster. In public key cryptograph there are 2 keys involved public key which is used to encrypt the data and private key which used to decrypt it. It is lot safer than private key cryptography.

A2). Quantum cryptography also called quantum encryption, applies principles of quantum mechanics to encrypt messages in such a way that it is never read by anyone outside of the intended recipient.

A3). Polarizing filter is used to create plocarized photons By passing a normal beam of light through a filter with specific angle of polarization. It restricts the vibration of electric field in a single direction. Photons can be polarized in one of the two bases rectilinear or diagonal.

A4). The two polarized modes are rectlinear. and the other is horizontal. In rectilinear only photons with horizontal and vertical filters pass through.

In diagonal mode, photons with angle of $+45^\circ$ and -45° can pass through.

Rectilinear	0°	—
	90°	|
Diagonal	$+45^\circ$	/
	-45°	\

A5) Quantum key distribution is a secure communication method which implements a cryptographic ~~tec~~ protocol involving components of quantum mechanics.

A6) QKD provides security which is future proofed, it means that even if a cryptographic system is broken at some unspecified future time previous message sent through it remain secure. It is a good method for producing long random keys. QKD session key is independent of all previously used keys.

A7) The bit string corresponding to the photons received by the receiver is called the raw key.
While sifted key is the key which remains after discarding falsely measured photons

Neil Gupta
10445674
pg 6

Homework 10

A8) Alice Bits: 1 1 1 1 0 1 0 1 0 1 1 0

Alice Base: ⊗ ⊗ ⊕ ⊗ ⊕ ⊗ ⊕ ⊗ ⊕ ⊕ ⊕ ⊗

Alice Polarization: \ \ | \ - \ - \ - | | /

Bobs Bases: ⊗ ⊗ ⊗ ⊗ ⊗ ⊕ ⊕ ⊗ ⊗ ⊗ ⊕ ⊕

Bobs Polarization: \ \ \ \ / | - \ / \ | -

Raw key Bobs Bits: 1 1 1 0 1 1

Sifted key.

The secret key is → 1 1 1 0 1 1