Quantum Cryptography

A secretive journey from Math to Physics

Ever wondered how to make an unbreakable code, a code that no one can decrypt? Well, if it is yes then you are at the right place and with this blog post you will get to know what it takes to make an unbreakable code!

We all have read in physics about quantum mechanics and how it is different from classical mechanics. But never in our imagination have we thought of applying laws of quantum mechanics in the field of cryptography. Sounds strange? Well, it is in fact true that this new generation of code makers are turning from math to physics these days. These Cryptologists, experts in atoms and other particles, want to exploit the laws of quantum mechanics to send messages that are provably unhackable.

Quantum cryptography draws its strength from the weirdness of reality at small scales. The particles making up our universe are inherently uncertain creatures, able to simultaneously exist in more than one place or more than one state of being. They choose how to behave only when they bump into something else or when we measure their properties.

Seth Lloyd, a Researcher at MIT, has demonstrated that by exploiting the quirks of quantum physics, it is possible to build an encryption machine that is truly unbreakable. "The funny thing about quantum mechanics is when you measure something, you mess it up," Lloyd tells Popular Science. Lloyd's theoretical quantum cryptography machine works like this:- When an eavesdropper tries to make a measurement that would help him or her crack the code, the act of making the measurement disrupts what he or she is trying to measure. Tricky, right?

Photons are used in Quantum Cryptography to transmit a key. Once the key is transmitted, coding and encoding using the normal secret-key method can take place. But how can we attach information to a photon's spin and how can a photon be made a 'key'? And this is where we have our eyes preyed on the **Binary Code**.

Each type of a photon's spin represents one unique piece of information - usually a 0 or a 1, for binary code. This code uses strings of 1s and 0s to create a coherent message. Let's say, for example 1100101011 can correspond with a h-e-l-l-o. In this way we can assign a binary number to each photon. Like - a photon that has a **vertical spin (|)** can be assigned a 0. We can send photons through randomly chosen filters and record the polarization of each photon and we will then know what photon polarizations the recipients should receive.

But despite of all the security quantum cryptography offers, it has flaws too. Chief among these flaws is- the length under which the system will work and It’s too short. The original quantum cryptography system, built in 1989 by Charles Bennett, Gilles Brassard and John Smolin, sent a key over a distance of 36 centimeters [source: Scientific American]. Since then, newer models have reached a distance of 150 kilometers (about 93 miles). But this is still far short of the distance requirements needed to transmit information with modern computers and telecommunication systems.

The future of cryptography is entangled between the code makers and the code breakers and it is where the new ideas and imaginations take flight with the hope of providing better security systems.