A "Teach the Teachers" Tutorial on Quantum Key Distribution (QKD) for Encryption

© Ron Frank Pace University

This is an outline of a tutorial session on Quantum Key Distribution for IS educators.

The take-aways are:

1. A basic understanding of the uses and needs for QKD.
2. A review of the current market status of QKD products.
3. An outline for a two hour lecture class module in QKD for an undergraduate (or graduate) IS course (based on this presentation).
4. Course materials for the two hour lecture module.
    - A slide set and a QKD Java simulator [bring your Java laptops]
5. An idea of where this module fits in the IS curriculum.

The prerequisite for this tutorial and the target IS course module are:

- A very basic background in high school algebra and an open mind.

The ideas that get discussed or introduced in this tutorial and the target IS course module are:

1. A review of he current state of data transmission / network transmission encryption.
2. The need for more robust data encryption.
3. A review of the definition and statement of the facts about one-time-pads (unbreakable).
4. A definition and statement about the symmetric key distribution problem in information assurance (open to attack).
5. Brief elementary introduction to the math/physics background of QKD
    - A definition and statement of the frequency definition of discrete probability.
    - The definition of cos(θ), especially for θ = 45°.
    - The definition of a vector basis in the 2-dimensional X, Y plane.
    - The definition of the components of a 45° vector in the X, Y plane.
    - The basic facts of polarized sun glasses (polarization of light).
        - I use a $17 kit from the American Optical Society or old sun glasses.
6. The QKD process itself and its 5-step algorithm
    - Introduction of the idea of a state vector, pure and mixed states.
    - A discussion of the measurement process in basic quantum mechanics.
    - A statement of the "No Cloning" theorem from quantum mechanics.
    - The basic five step QKD algorithm.
    - The robustness against eavesdropping
7. We discuss how the algorithm or other variants are used in current products and how they solve the key distribution problem in a robust (unbreakable) way.
8. We use a QKD algorithm simulator to try various bit string lengths to experiment with and see the effects of probability on the algorithm this exhibiting its strength for long keys and the weakness of short keys.
9. Finally, we discuss how to use this outline in an IS course module and where to put the course module in the IS curriculum
    - Based on the slide set and augmented by the simulator used in this lecture.
10. There will be an open discussion at the end.