Teach the Teachers, a Tutorial on Quantum Key Distribution (Why and How)

Ronald I. Frank
School of Computer Science and Information Systems
Pace University
861 Bedford Road
Pleasantville, NY 10570, USA

Quantum Key Distribution (QKD) is the use of quantum phenomena to create and distribute secure random symmetric private one-time keys (random bit strings) used for encrypting and decrypting messages. The encryption using these keys is known to be unbreakable even classically. QKD encryption is also called Quantum Encryption (QE). There are products on the market doing this today. DARPA is funding the use of QKD to replace IPSEC on the internet. QKD overcomes the only weakness of classical unbreakable one-time pads - the secure distribution of the pads themselves. Encryption is used for transmitting data securely. In previous papers I have proposed an IS course module covering QE, and I have discussed where it would fit into the IS curriculum. I have analyzed and presented an outline on the prerequisites for such an IS course module and provided an advanced tutorial for faculty or graduate students. This paper is my suggestion, in some detail, for such a module for undergraduate students. I simplify the presentation so that undergraduate IS students ought to be able to follow the discussion. They need only some remembrance of high school algebra. The relevant physics is presented in a purely descriptive form. Appendices contain the QKD (QE) algorithm in UML-like diagrams. This module should be teachable in two one-hour lectures. Due to space limitations, I have left out appendices on the Vernam one-time-pad, and a typical simulation run output which should be part of the module.

keywords: quantum encryption, quantum cryptography, quantum key distribution, IS curriculum