Security of Communication and Quantum Technology

Gregory Paperin
Monash University, Australia

INTRODUCTION

In this article we aim to analyze some of the advances in security of communication since this discipline evolved and to pinpoint the main problems. We then introduce a modern attempt to solve some of these problems, in particular the key distribution problem, by using the theory of quantum mechanics to construct a communication system that automatically detects eavesdropping. We examine some of the implications of quantum mechanics relevant to this field and then introduce a selection of communication protocols based on them. Finally we examine how secure these protocols are and identify their potential weaknesses.

BACKGROUND

Traditional Cryptography and the Key Distribution Problem

Ever since people began to use remote communication systems, they have been concerned with the security of the messages they send. Two main problems were recognized thousands of years ago and still remain the main problems in the field of communication security:

- How do we make sure that only authorized recipients will read and understand a message?
- How do we verify the authenticity of a message—that is, how do we check that the sender is really the person he or she claims to be and that the message has not been altered on the way?

Since ancient times two types of approaches have attempted to solve these problems:

- make the communication channel so secure that the message cannot be interrupted before reaching the authorized recipient (secure channel); and
- encode the message in a way such that even if the message is intercepted, no unauthorized person can read and understand it (encryption).

A combination of these two methods is usually the most promising. But how can this be achieved?

Historians report tricks that ancient Romans used to encode their messages (e.g., Cesar Cipher) (ArticSoft, 2003; Singh, 1999)—for example the use of a table to substitute letters for other letters. Only someone possessing such a table could decipher the message.

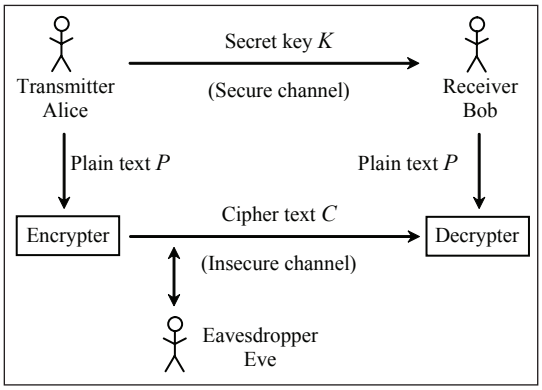
In 1466, Leon Battista Alberti invented and published the first poly-alphabetic cipher, which was not as liable to statistical analysis as simple substitution ciphers. This class of ciphers was not broken until the 1800s. The most famous cipher of this type is Vigenere, a variation of which is still today considered to be the only absolutely secure encoding method. Unfortunately it requires a key as long as the message, which can be used only once and is therefore hardly practical. Alberti also wrote extensively on the state of the art in ciphers, putting cryptography on a proper scientific foundation for the first time. (New Order, 2003).

These and similar approaches rely on the sender and the receiver having exclusive knowledge of the key used to encode and decode the message. If someone else were to get a hold of this information, he or she could interrupt and read the message or even forge one. This constitutes the key distribution problem: how can we securely let the authorized recipients (or senders) know the cipher key without allowing it to become public?

Usually, the encryption key needs only be communicated once. After that, many messages can be sent securely using that key. This lowers the probability of successful eavesdropping, but does not remove it.

During World War II the German army used an encryption device called Enigma. This electromechanical device consisted of a complicated system of rotors and included a plug board allowing the user of Enigma to swap any letter for any other letter. The use of this

Figure 1. A classical crypto-communication system: Alice, the sender, encrypts the plaintext P into the cipher text C using a secret key K, which she shares only with Bob, the authorized receiver, and sends C over an otherwise insecure channel, on which Eve is eavesdropping. Bob receives C and uses K to decrypt it to P. A secure channel is required for Alice and Bob to agree on K. (Lomonaco, 2002).



plug board increased the number of combinations of Enigma settings by a factor of 1015, which made a statistical analysis or a brute force attack (trying all possible keys) extremely hard. However, knowledge of the general encryption principle allowed British mathematicians, led by Alan Turing, eventually to crack the code.

Public Key Cryptography

With the appearance of modern communication technologies, the demand for secure communication increased. In the 1970s a new technique was devised to overcome some of the problems with key distribution. This new approach is known as Asymmetric-Key or Public-key cryptology.

The main idea of this approach is that there are now two keys: one to encrypt and another to decrypt the message. These keys are distinct, and it is infeasible to derive one from the other. The method constitutes a good attempt to solve the key distribution problem: for example, when a secret agent needs to send a message to his base, the base can broadcast the encryption key over a non-secure channel. Even if the enemy first interrupts the key and then the message sent back by the agent, the enemy will not be able to decrypt the message because the decryption key is kept secret.

An advantage of this system is that the algorithm used can be (and usually is) very well known to everyone—it does not provide any help in deciphering the text. Without the private decryption key, the message cannot be decoded.

However, how does the base know that the message was indeed sent by a trusted agent? To achieve such security the agent needs a second, private key, which is used to encrypt the message again. The problem of communicating that second key to the agent persists.

The algorithms used in modern public-key cryptotechnology are based on the RSA algorithm (named after its inventors Rivest, Shamir, & Adelman, 1978), which is based on the prime factorization problem: it is computationally very intensive to factorize a very large number, if its only factors are two very large primes.

In RSA, one of two very large primes p and q is used as the private key and p • q is used as a public key. When p and q are sufficiently large (a few hundred digits), it will take the most efficient algorithm known today, running on the fastest supercomputer, many years to factorize p • q. By then, the secret information will be of no use.

There are, however, two major problems with this approach:

- The message may remain sensitive for a longer period of time and the sender may not want it decoded by unauthorized people even after many years.
- Currently, there is no known efficient factorization algorithm. However, there is no mathematical proof that such an algorithm exists. If such an algorithm was developed, all modern RSA-based encryption algorithms would become useless overnight.

This situation is not satisfactory in the long term. In particular, recent advances in quantum computing encourage scientists to look for alternatives to common RSA, since there is a known algorithm for a quantum computer to factorize large numbers efficiently. Once such machine has been built; it will be the end of conventional RSA-based approaches to encryption.

Interestingly, the same theory that promises to break RSA offers the basis for the technology that is set to provide a new level of communications security in the future.