Original sendmsg programme

Technology

This review discusses the need for extra security on the internet by use of more powerful cryptosystems than those in use today. The RSA cryptosystem is discussed and it's algorithm is also shown in detail. The emergence of Quantum Computers that would be able to work through the algorithm with ease are mentioned, illustrating that the security of RSA cryptosystems is only temporary.

Quantum cryptography, the new system which relies on Heisenburg's Uncertainty Princple for it's security rather than the difficulty to factorise the RSA algorithm is discussed as the replacement. How the system works is principly discussed followed by the established protocol for implementing it. However, quantum cryptography is not absolutely secure from attack. The problems arise when an attempt is made to implement all the theoretical ideas into practise. Some clever hacks, thought up by the very designers and engineers of quantum cryptography, reveal some weak spots which earlier were never dreamt of. These ideas and the fact that perhaps no network can be absolutely secure to the ideal level are discussed in depth.

Introduction

Since the first step towards the global internet taken by Ray Tomlinson's SENDMSG programme in 1971, the need for secure data transfer was essential. It is becoming even more so with the passage of time. Recently there has been a surge in attempts to obtain retail bank details from individuals by use of bogus emails. There is no shortage of people willing to spy into secure sites to obtain sensitive information. There is certainly a heightened security consciousness post September 11th, and a quest bordering on paranoia for absolute security.

A new method of securely transferring data is by use of lasers connected to computers via fibre optic cables. It is designed to make life much more difficult for internet spies. Instead of passing information digitally in the form of 0's and 1's as is conventionally done, photons are transmitted corresponding to 0's and 1's depending on their quantum state. This new method of data transfer is called Quantum Communication. Devices providing one-to-one links are currently available, used largely by military and intelligence agencies.

Now in the very lab in Cambridge, Massachussetts, where the original SENDMSG programme was first used and developed, an attempt is being made to create a Quantum network of computers dubbed Q-Net. This network will be able to handle everyday uses such as banking transactions and handling sensitive web pages, instead of the one-to-one quantum communication products currently in use.

Quantum Web Encryption promises an un-hackable method of data transfer guaranteed by the laws of quantum physics. These claims take advantage of Heisenberg's uncertainty principle, whereby any attempt to measure a quantum system disturbs its state, thereby rendering the information being transferred useless. The unavoidable noise created would therefore also alert the intended recipient of any attempted eavesdropping, hence providing a built in alarm system. This yields the possibility of creating a system whereby a secret and random string of bits, called a cryptographic key, can be established between a sender and receiver. Once this key has been established, it can be used to encrypt messages and send meaningful information between the sender and receiver in absolute secrecy.

Current Security

A system for using an encrypted data transfer is already used every time a secure transaction is carried out over the internet with addresses beginning with https://. One such example of the existing cryptosystems is the RSA algorithm cryptosystem, developed in 1977 and used extensively by many security conscious organisations. The RSA algorithm works by taking two large prime numbers, x and y, and computing their product, z = xy. A number, n (called the public exponent), is chosen less than z and is relatively primed to (x-1)(y-1). Hence n and (x-1)(y-1) have no common factors except 1. Another number, m (called the private exponent), is found such that (nm-1) is divisible by (x-1)(y-1). The public key is the pair z and n, and the private key is the pair z and m. The data sent to and from the sites beginning with https:// is encrypted with the public key, (z, n), and can only be deciphered by a recipient who has the private key, (z, m).

It is currently difficult to obtain the private key from the public key. The RSA cryptosystem works because it is assumed this process of factoring the large 512-bit public key value will take months to complete. The cryptosystem remains secure because the public key is simply changed every few weeks. If a method for finding a quick way of factoring were found then the RSA cryptosystem would no longer be secure.

The security provided by this cryptosystem is only temporary. A candidate to make RSA cryptography redundant is the emergence of 'Quantum Computers', using qubits instead of classical bits found in today's computers. A classical bit is a fundamental unit of data stored on a computer physically as a 0 or 1. A quantum computer works on the phenomenon of the qubit which can exist as a 0, a 1 or simultaneously as a superposition of both with a numerical value representing the probability of each of these states.

If for example a system of a few hundred qubits were arranged in a three dimensional space as an exponentially large matrix, classical computers would take exponentially longer time to perform calculations on each individual state, also represented as a matrix, than it would for quantum computers which would operate on all states simultaneously within the same period of the computers clock. Many experts believe this new generation of computers will be available in the next decade, and would therefore be able to factorise those large numbers with ease. This would certainly spell the end of the cryptosystem so extensively relied upon for years.