RSA

Public key cryptography is currently the mainstream method of communicating securely over the internet. A system developed by Rivest, Shamir, and Adelman is in wide circulation, and is so called the RSA algorithm, after the surnames of its creators. Its use involves both a private key as well as a public key, which must be available to the intended recipients of messages.\(^1\)

A message is encrypted using RSA by first selecting two large (1024-bit) prime numbers, \(p\) and \(q\).\(^2\) These numbers are then multiplied together to come up with a product, \(n\). A combination of \(n\) and the results from mathematical manipulation of \(p\), \(q\), and \(n\) are what make up the private and public keys. While the public key is used to encrypt, the private key is used to decrypt the message.\(^1\)

Ensuring that \(p\) and \(q\) are very large prime numbers ensures the security of the system. Although multiplying large prime numbers is equivalent to multiplying any two large numbers, a trivial operation on a computer, its inverse is practically impossible. This operation is thus called a one-way function. This ensures that although one is given \(n\), the product of the two prime numbers, discovering \(p\) and \(q\) cannot be done. If it could, the keys could be discovered and the encryption would be lost.\(^3\)

Peter Shor

Finding prime divisors of a large number is infeasible using today's technology. This is the assumption that the RSA encryption scheme is built upon. This assumption may soon be false, however. Peter Shor, a mathematician who is currently a professor at MIT teaching theoretical computer science, devised a feasible algorithm which could break the RSA system.\(^4\) This algorithm, called “Shor’s Algorithm”, after its creator, was written by Shor while he was working at the AT&T Bell Laboratories in 1994.\(^5\)

For an algorithm to be feasible, its computation time must be bound by \(O((\log N)^k)\) for a finite \(k\). This allows \(N\), the problem size, to grow while the
problem remains feasible. Prior to Shor’s algorithm, no such factoring algorithm existed. This meant the problem soon became impossible as the size of the numbers grew. The best algorithm in existence had been the quadratic sieve, which had a running time of
\[ O\left(\exp\left(\left(\frac{64}{9}\right)^{1/3}N^{1/3}(\ln N)^{2/3}\right)\right) \]

Shor’s algorithm, on the other hand, can solve the problem in polynomial time, \( O(\log(N)^3) \).

The details of Shor’s algorithm are beyond the scope of this paper, but can be summarized by the following seven steps:

1. Pick a pseudo-random number \( a < N \)
2. Compute \( \gcd(a, N) \). This may be done using the Euclidean algorithm.
3. If \( \gcd(a, N) = 1 \), then it is a nontrivial factor of \( N \), so we are done.
4. Otherwise, use the period-finding subroutine (below) to find \( r \), the period of the following function:
\[ f(x) = a^x \mod N \]
5. If \( r \) is odd, go back to step 1.
6. If \( a^{r/2} - 1 \mod N \), go back to step 1.
7. The factors of \( N \) are \( \gcd(a^{r/2} \pm 1, N) \). We are done.

The complex part of the above procedure is the period-finding subroutine. It is implemented in two parts, the first of which turns the factoring problem into a question of the period of a function. The second actually finds this period. Although the first part may be implemented using a known algorithm, the second part uses the quantum Fourier transform and is responsible for the quantum speedup.

The quantum portion of the algorithm calls for the use of quantum registers and other references to quantum computing. Although still a mainly theoretical concept, quantum computers are becoming a possibility quicker than most may realize, which would inevitably lead to the breakdown of internet security.

Quantum Computers

Quantum computing was an idea first conceptualized by Paul Benioff. As opposed to a regular Turing Machine, which positions its head on an infinite tape to read zeros or ones, a quantum Turing Machine tape consists of zeros, ones, and the superposition of zeros and ones. The general idea of such a quantum system is the superposition principle, where symbols can be in either the zero state, the one state, in both states simultaneously, or in any state in between. Instead of being called bits, these symbols in a quantum computer are referred to as qubits (quantum
bits). The flexible state of these qubits implies that a quantum computer can be in multiple states at the same time.\(^7\)

This idea of superposition flows from the dual particle-wave behaviour first suggested by Louis de Boglie in the 1920's. This started with the concept of light behaving as a wave through Thomas Young's double-slit experiment, which evolved into electrons behaving as waves and eventually up to molecules themselves behaving as waves. As waves spread out through space, it was concluded that a particle exists in two places at once.\(^9\)

Suppose one has a register consisting of three regular bits. At any point in time, all of these three bits will have a value of either 0 or 1, and thus represent a decimal number between 0 and 7. If this were a register consisting of three qubits, each of the three qubits could have both the values 0 and 1 at the same time, and thus represent all decimal numbers between 0 and 7. A computer using such registers could then simultaneously utilize all possible values represented by the three qubits. This is referred to as quantum parallelization.\(^8\)

This creates a degree of parallelism never before seen and so quantum computers could have the ability to process data at millions of times quicker than current processors, according to physicist David Deutsch. One example given on howstuffworks.com is that of a 32-qubit quantum computer running at 10 teraflops, while the fastest supercomputer to date has a rating of 2 teraflops.\(^7\) However, the performance increase in using a quantum computer over a classical computer depends on the algorithm given to it. Classical algorithms will not run any quicker on a quantum computer, as they will be run in the same fashion. An algorithm must exploit the constructs of the quantum computer in order to use it to its full potential. Shor's algorithm as discussed earlier does so. Although his algorithm would take billions of years on a conventional computer, a quantum computer would solve the problem in a matter of seconds.\(^8\)

Construction of a quantum computer is at the atomic level. Each qubit is represented by one or more atoms, and its spin direction indicates its value. Since such computers are still in their very early stages, their building blocks have not yet been cut out, and different corporations are attempting different styles of construction. For example, Los Alamos–MIT in 1998 created a qubit which spread across three atoms, making it harder to corrupt its value.\(^7\)

One major problem with quantum computers is that a qubit’s value cannot be read without altering it in some way. The quantum mechanics aspect of entanglement states that if one atom has a force exerted on it, it will
become entangled with an adjacent atom, which will inherit the properties of the first.7

One successful implementation of a quantum computer utilizes Nuclear Magnetic Resonance. This is based on the concept of atoms having magnetic moments and aligning themselves with or against the magnetic field surrounding them. Since any atom has two distinct orientations, it can be used as a qubit. Additionally, the magnetic moment of one atom will affect the moments of adjacent atoms. Radiofrequency fields are used to control and change these moments, and thus control quantum computing. As the moments of the atoms change, the resulting radiofrequency fields generated by these oscillations are measured. In this sense, the actual qubits are not touched, but instead their side effects are observed to obtain useful data.9

Realistically, quantum computers would require at least 36 qubits to be able to solve any useful problems. To date, the largest quantum computer, built at the Los Alamos National Laboratory, used 7 qubits created in a drop of liquid. There is still much work to do and many problems to overcome before quantum computers of any use become feasible.7

“If computers that you build are quantum,
Then spies of all factions will want 'em.
Our codes will all fail,
And they'll read our email,
Till we've crypto that's quantum, and daunt 'em."  

Peter Shor10
Resources


