RSA: The Elegant Code

by Harman Kour - Thursday, July 10, 2014

http://gonitsora.com/rsa-elegant-code/

The quest to share information securely and the curiosity to decipher the hidden meaning, has astounded the human mind since eternity. Whether it was the ancient art of steganography, or the development of ciphers from the Caesar Cipher to the Enigma Cipher Machine, the basic idea has been to protect information from falling into the wrong hands.

This science of cryptography took a very interesting turn during the 1970's with the development of the concept of asymmetric ciphers by exploiting the one-way functions. This was achieved by a trio of three brilliant cryptographers at Stanford University, namely Whitfield Diffie, Martin Hellman and Ralph Merkle. Together they solved one of the greatest mysteries of sharing messages secretly without having to share the key. For instance, if Alice wants to communicate privately to Bob she must encrypt the message using a key. Now for Bob to be able to decrypt the message he must know the key. This is an example of a symmetric cipher which uses the same key to encode and decode the message. This implied that the key distribution is an inevitable part of decipherment. It could be achieved by personally meeting and sharing the key or delivering it through a reliable source which is not only less secure but also inconvenient.

Adi Shamir, Ronald Rivest, and Leonard Adleman : When they were students at MIT. Image Credit : ams.org

Another trio of computer scientists at MIT namely Ron Rivest, Adi Shamir and Leonard Aldeman developed a mathematical function in 1977 (called the RSA Code, named after their initials) which was based on the revolutionary concept of asymmetric ciphers (which uses separate keys for encryption and decryption).

The RSA Code, a system of asymmetric cryptography is a form of Public Key cryptography. To understand the mystery of RSA Code, we again take the example of Alice and Bob, who want to share some private information with each other. Alice creates a public key (which is a one way function- that is it is impossible for anyone to reverse it to decode the message). This is available to everyone who wants to send her a message. So Bob encrypts the message using the public keys and sends it to Alice. Now Alice needs to decipher the message sent to her and for this she possess a private key (some extra piece of information) that allows only her to decode any message sent to her since no one else possess the private key for decryption.

Mathematically it goes like this:

- Alice takes two giant prime numbers, $latex p$ and $latex q$. Let's take $latex p=17$ and $latex q=11$ for simplicity. She multiplies $latex p$ and $latex q$ to get $latex N=187$. In practice the numbers $latex p$ and $latex q$ are quite large, so that $latex N$ cannot be easily found out even if computers are employed.
- She now picks up another number $latex e$ (say $latex 7$) such that $latex e$ is relatively prime

to $latex (p-1)(q-1)$ which in this case is $latex (17-1)(11-1)=160$. This is an outcome of Euler's Theorem which states that if we raise $latex a$ to the power Euler's Totient function of $latex n$ then we end up with $latex 1$ modulo $latex n$. That Is $latex a^{\phi(n)}\equiv 1\pmod n$, where $latex \phi(n)$ is the Euler's totient function.

- Alice now publishes $latex e$ and $latex N$ which are available to everyone as public keys for encryption.

- Bob wants to send her a message $latex M$ (say $latex 88$). He uses the encryption formula (one way function) along with the public keys issued by Alice to get the encryption key $latex C=M^e \pmod N$ such that in our example $latex C=11$, where $latex C$ is called the Cipher Text, which is what he sends Alice.

- Since modular functions are one way functions hence it is extremely difficult to work out $latex M$ from $latex C$ when larger primes are involved. So even if Eve (any third person or spy) catches hold of $latex C$ when Bob sends it to Alice, she can't decipher it back to trace $latex 88$.

- But Alice can decipher the message because she knows $latex p$ and $latex q$. She calculates a special number, $latex d$ her private key according to the formula $latex ed\equiv 1\pmod{(p-1)(q-1)}$. In our example $latex d=23$ which can be easily calculated using the technique of Euclid's algorithm.

- Once Alice has calculated her private key, she simply uses the decryption formula, $latex M\equiv C^d \pmod N$. Here in our example after simplification we shall get $latex M=88$.

Eureka! Alice is able to recover the original message sent by Bob. Thus this one-way function allows everyone to encrypt messages to a particular person by using the public keys ($latex N$ and $latex e$) but only the intended person can decrypt the message because the recipient is the only person who knows $latex p$ and $latex q$, and hence the only person who knows the private key $latex d$.

The fundamental logic involved is the difficulty in factorizing $latex N$ (to get $latex p$ and $latex q$). Nowadays, for important transactions $latex N$ is taken to be of the order of atleast $latex 10^{308}$ which would take all the computers in the world, put together, longer than the age of the universe to

factorize $latex N$.

As long as we do not come up with extremely efficient and faster ways of factorization, the RSA Code is here to stay in all its elegance, simplicity and beauty.

[This article has been written by Harman Kour, who is at present an intern with Gonit Sora.]
