Q’loQ

KryptoMagik

Q’loQ

A Public Key Encryption Algorithm

Based on RSA

- RSA encryption algorithm invented in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman
- RSA is the most popular public key encryption algorithm today
- RSA and Q’loQ encrypt and sign the same way

Q’loQ

- Invented in 2019
- Reference implementation in Python
- Based on the idea of the Klingon cloaking device

Governing Principles

- Base
- Cloak
- Key generation

Base

- First generate 2 primes of equal size and let them be P and Q and let them not be equal.
- Establish a totient with the product of P -1 and Q -1

Cloak

- Take the result of P modulo 2 and call it C. Then take the result of Q modulo 2 and call it K.

Establish a modulus N using the following formula

((((p + K) / (K+1)) * ((q+C) / (C+1)))) * ((p + (K+C+1))) % (K+C) * ((q / 2) + 1)

Public Key Generation

- Next find a number between 1 and the totient T where the number and T are coprime and call it PK. This becomes the public key.

Private Key Generation

- Find the multiplicative inverse of the public key PK and the totient T and call it SK, the secret key.

Encryption/Decryption

- Encryption is achieved by taking the plain text and raising it to the power of the public key modulo N
- Decryption is achieved by taking the cipher text and raising it to the power of the private key modulo N

Cryptanalysis

- One solves Q’loQ ciphers by finding P and Q, recontructing the totient and finding the inverse of the totient and the public key
- In RSA one can normally take the modulus modulo some number and when P or Q is encountered a zero should be the result. Q’loQ’s cloak defies this and P and Q against the modulus will result in an arbitrary number

Open Question/Problem

- How to identify P and Q?