

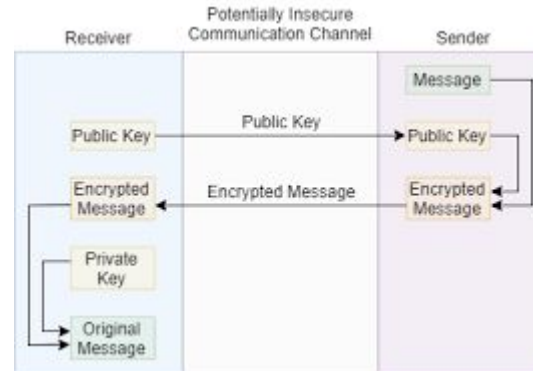
Shor's Algo





RSA Encryption

- Computer generates really large number with two prime factors
- Classical Computers have hard time guessing these numbers
- Basis of most encryption algorithms
- Quantum computing exponentially speeds up the guessing process



Quantum Computers Destroy Internet Security

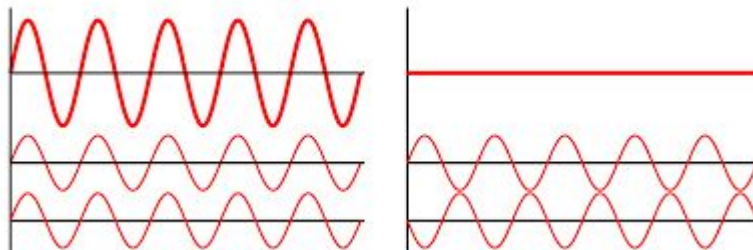


Minute Physics



TakeAways

- Classical computer must brute force prime factors for big numbers
- Using a special equation we can get that down to only one prime factor
- There is an equation where we can manipulate the power of the prime factor so that it has a repeating property correlated to the big number
- Quantum Computing uses interference patterns to narrow down the power
- Using the power, we can get the guess and with the guess.



Qubit Timeline Estimates



Note: Dates are speculative
ID: 374252

© 2018 Gartner, Inc.