Breaking RSA Encryption

Grant Haataja

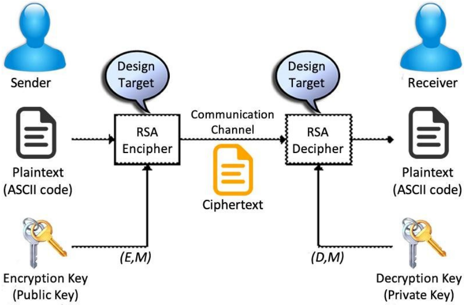
December 13, 2019

What is RSA encryption?

RSA encryption is a public-key cryptographic scheme which means the encryption key is not a secret, but individual users all have their own secret decryption key.

How does RSA work?

RSA encryption uses extremely large numbers and one-way functions to easily encipher messages in a way that is almost impossible to reverse without the specific, secret decryption key.

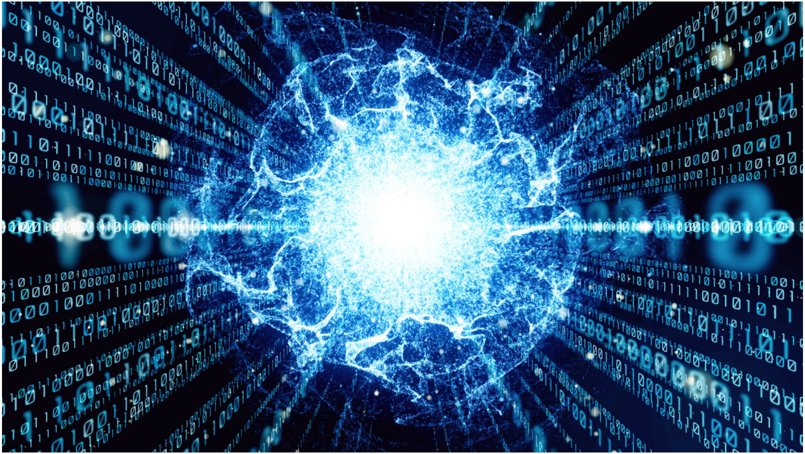


Brute force method

Trying to break RSA encryption using brute force method is virtually impossible.

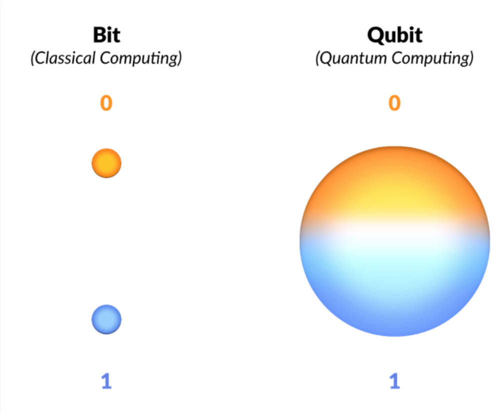
Quantum method

Although only theoretical currently, Quantum computing presents a relatively straightforward method to breaking RSA encryption.



Quantum Superposition

Quantum Superposition is the term used to refer to the ability of qubits to be in multiple states at the same time.



Shor's Algorithm

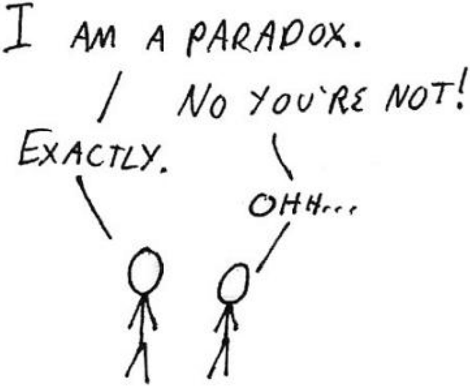
1. Find the gcd of N and m, where N, is the number you are trying to factor, and m is a random positive integer less than N. Most likely, $\gcd(N, m) = 1$, and the algorithm continues. If the gcd does not equal one, then you have found a factor of N and the work is complete.
2. Find the period of $m \pmod{N}$, $m^2 \pmod{N}$, and $m^3 \pmod{N}$. This is the only step that requires a quantum computer superior to traditional computers.
3. If the period P is even, continue with the algorithm. If it is odd, go back to step 1 and choose another random integer m.
4. Confirm that $m^{P/2} + 1 \neq 0 \pmod{N}$. If this is true, continue on to step 5. Otherwise, go back to step 1 and choose another random integer m.
5. Compute $\gcd(m^{P/2} - 1, N)$. The result will be a non-trivial prime factor of N, and will give you the key to break anything encrypted using RSA with the key N.

Conclusion

If quantum computing technology becomes powerful enough, it will render RSA encryption useless.

Paradox of Technology

If quantum technology can break RSA encryption, it will also allow for a new cryptological system of quantum key generation resistant to quantum attacks.



References

- https://www.thesslstore.com/blog/is-it-still-safe-to-use-rsa-encryption/
- https://www.theinquirer.net/inquirer/news/3078470/youtube-reinstates-pulled-cybersecurity-tutorial-videos
- https://www.engadget.com/2019/09/23/google-quantum-supremacy/
- https://medium.com/predict/quantum-computer-gateway-to-revolution-1028bedad17e
- https://medium.com/quantum-bits/break-rsa-encryption-with-this-one-weird-trick-d955e3394870
- https://easttenthgroup.com/modern-leadership-paradox-high-tech-vs-high-touch/
- https://usabilla.com/blog/the-paradox-of-technology-and-5-ways-to-avoid-it/