RSA Encryption and Quantum Computing

How quantum computers will affect our entire internet

By Samuel Wan (id: 900142126)

What RSA is used for

1. RSA is in HTTPS
    a. What is HTTPS?
        i. HTTPS stands for Hypertext Transfer Protocol Secure, a combination of the Hypertext Transfer Protocol, and the Secure Socket Layer (SSL) protocol
        ii. HTTPS is used by around 79% of websites and uses SSL cryptographic protocol, which uses the RSA algorithm.
        iii. Basically, HTTPS uses the RSA algorithm to encrypt your browsing data/activity.
2. RSA is used in iMessage
    a. iMessage uses RSA-OAEP (Optimal Asymmetric Encryption Padding) to encrypt your messages. This ensures that even if an observer reads your traffic, they will not be able to read the contents of your message.
3. RSA is used in SQL database encryption
    a. What are SQL databases?
        i. SQL databases are a collection of tables that store a specific set of structured data.
        ii. SQL stands for Structured Query Language, which is used to manipulate databases.
    b. Companies use RSA encryption to encrypt the data in SQL databases
        i. Major companies that use SQL databases are
            1. Microsoft
            2. Dell
            3. Stack Overflow
            4. Adobe
            5. Facebook
            6. LinkedIn

Basic overview of how the RSA algorithm works

The server generates two or more large prime numbers and multiplies them together. This is called the "public key". This key is made available to any client which wishes to transmit data securely to the server. The client uses this "public key" to encrypt the data it wishes to send. Now because this is an asymmetric algorithm, the public key *cannot* be used to decrypt the transmitted data, only to encrypt it. In order to decrypt, you need the original prime numbers, and only the server has these (the "private key"). On receiving the encrypted data, the server uses its private key to decrypt the transmission.

Why Quantum Computers Matter

The RSA algorithm is fundamentally based on the difficulty to perform prime factorization.

a. Currently, the best attempt at a prime factorization of a large number was done by a group headed by Greg Childres at CSU Fullerton. This number has 320 digits and took about 340 CPU years. If you had 340 CPUs, it would take you about a year to complete this.
b. RSA-600, a common RSA protocol, uses 193 decimal digits, so for even a large organization, it would take an impractical amount of time to break RSA.

Shor’s Algorithm

a. What is Shor’s algorithm?
    i. Shor’s algorithm takes a bad guess at a prime factor and then turns that guess into a much better guess at a prime factor.
    ii. Even though this sounds simple, the “turning a bad guess into a good guess takes” step a very long time on a normal computer.

How Shor’s Algorithm Works Pt. 1

Using:

Public Key N

Guess g

Euclid’s Algorithm

And Lemma : for any two integers A and B with no common factors, there is always some integer p and m, where $A^p = m * B + 1$.

How Shor’s Algorithm Works Pt. 2

Writing equation as $(g^p) - 1 = m * N$, then $(g^{p/2} + 1)(g^{p/2} - 1) = m * N$,

We have (some number) times (some number) = (some number) * N

Simplified: $g^{p/2} \mp 1$

Problems:

- If P is odd, p/2 is not whole
- If we get a multiple of N, then the other factor would be m, and the whole algorithm falls apart
- We don't know what P is

How to find our power P

- Using quantum superposition, you can calculate a ton of possible answers for single input, and then have each wrong answer quantumly interfere with each other so they cancel out.
- Plus using this mathematical observation

$$g^x = m_1 * N + r$$
$$g^{(x+p)} = m_2 * N + r$$

- P gains a “repeating property”

Using Fourier Transform

Oversimplifying, you can use superpositions to create sin waves, and the quantum Fourier Transform to find our 1/p. If p is even and we can plug this p into our original equation, use Euclid's algorithm to find the shared factors, and now we can use these factors to decrypt our data.

<https://en.wikipedia.org/wiki/Quantum_Fourier_transform>

Conclusion

Quantum computers will break the internet as it is today

But luckily, there is already a plan to prevent that from happening:

<https://en.wikipedia.org/wiki/Post-quantum_cryptography>