

RSA Encryption: Definition, Architecture, Benefits & Use

RSA allows you to secure messages before you send them. And the technique also lets you certify your notes, so recipients know they haven't been adjusted or altered while in transit.

The RSA algorithm is one of the most widely used encryption tools in use today. If you've used computers made by Samsung, Toshiba, and LG, you've probably used a device with an embedded [RSA-enabled chip](#).

Some people use RSA explicitly, and they dig deep into the math before they send any kind of message via an insecure service (like email). But some use RSA unknowingly when they sign on to secured websites. Their computers do the work behind the scenes, and sometimes, that work happens without their permission too.

RSA was once considered the gold standard of encryption security. But some experts believe that it's become too easy to hack. Others say it's never implemented properly, and that inaccuracy is responsible for the hacking risks.

No matter how it's used or what you believe, it pays to know more about how RSA works, so you can be aware of the security risks you face.

What Is an RSA Algorithm?

Before the mid-1970s, exchanging secure messages required a lot of coordination. Senders and recipients needed to share a secret code (or key). Without it, encrypted notes couldn't be decrypted. RSA changed everything.

In 1977, [three MIT colleagues](#) began developing their own cryptographic system based on randomization, basic math, and prime numbers. It took the trio 42 tries to find a formula they considered unbreakable, and they named it by combining the first letters of their last names.

Like other cryptographic algorithms, RSA transforms basic, readable data into something scrambled and twisted. Only a key can reverse the process. And RSA relies on a key made, in part, from prime numbers.

In theory, a hacker could compute the value of a private key by analyzing the public version. But prime numbers are incredibly difficult to work with, especially if they're long.

For example, researchers have held "RSA Factoring Challenge" to encourage mathematicians to break the code. A similar team

complete it via thousands of machines all around the world. And that was considered a speed record.

How Does RSA Encryption Work?

RSA encryption relies on few basic assets and quite a bit of math.

These elements are required:

- A public key (e)
- A private key (d)
- Two prime numbers (P and Q), multiplied (N)

Security relies on the assumption that it's impossible to determine the value of d. The math that sits behind these calculations is complex, but it would be familiar to any student of algebra.

If you're interested in seeing the math at work, [use an online calculator](#) to create your keys.

While breaking the code is difficult, it's not impossible. Some developers make theft harder by adding random elements. This so-called **padding scheme** makes the message larger, so it's harder to compute with math. And the random information makes decryption less accurate. A less sophisticated hacker might come up with decrypted text that's nothing like the original note.

Where Are RSA Encryption Algorithms Used?

People hoping to send secure messages, gain access to secure websites, or prove the authenticity of messages might use RSA.

To **send a message** with RSA, you will:

1. **Create keys.** You'll follow the mathematical steps above (or use a program) to create both a public and a private version. You'll store that private key in a spot where it can't be seen, but the public version should be widely shared.
2. **Get your recipient's public key.** You must know this value to encrypt your note.
3. **Encrypt and send.** Using the public key and an agreed-upon padding scheme, you'll scramble your note and send it along.
4. **Use recipient decoding.** When the message arrives, the person will use a private key to undo the work and see what's inside.

You can use this same process to append a digital signature to a message. You will:

- **Choose a hash algorithm.** You'll apply it to your entire message.
- **Alert the recipient.** Use a phone call or another message to tell your recipient of the method you choose.
- **Append the hash.** Apply the value at the end of your note and send it.
- **Decode.** The recipient will use the hash value and your public key to reverse the process. If the contents are the same, the contents haven't been altered.

Your computer might also use RSA without your explicit knowledge. Some websites require a quick verification conversation before you can gain access. Information is traded, and it's typically encrypted with RSA.

Is an RSA Formula Safe?

When RSA was released in the 1970s, plenty of people assumed it could never be cracked. We now know that's not true.

Some hackers bypass RSA altogether with **brute force attacks**. They pound the algorithm with numbers, hoping that one combination will unlock the code and provide the key.

Making your keys longer and more complex is a simple defense. Experts recommend **keys that are at least 1024 bits**. Protect very

We use cookies to ensure you get the best experience on our website. By clicking "Got it", you're consenting to our use of cookies.

Cookie Settings

Got it

X

okta

Solutions

Products

Developers

Resources

Company

Try Okta

Contact Sales

And know that you have options. Some experts believe that [RSA is inherently flawed](#) and no one should use it. They recommend other methods that come with even more complex math. They may take longer to implement, but they could be more secure options.

Get Help From Okta

Parsing all of your options isn't easy. Implementing solutions can be even more complicated.

Work with Okta and get robust security solutions delivered by people who can explain your options clearly and carefully. Contact us to get started.

References

[The Encryption Many Major Companies Rely On Has a Serious Flaw](#). (October 2017). Engadget.

[Leonard Adleman](#). National Inventors Hall of Fame.

[New Record Set for Cryptographic Challenge](#). (March 2020). Phys.Org.

[Still Guarding Secrets After Years of Attacks, RSA Earns Accolades for Its Founders](#). (June 2003). *SIAM News*.

[Cryptographic Padding in RSA](#). (January 2009). Science Blogs.

[RSA Encryption: Keeping the Internet Secure](#). (March 2014). American Mathematical Society Graduate Student Blogs.

[Public-Key Encryption by RSA Algorithm](#). Steyerbrains.at.

[Understanding Public Key Cryptography and the History of RSA](#). (February 2012). SecurityWeek.

[Seriously, Stop Using RSA](#). (July 2019). Trail of Bits.

COMPANY

About Us

Careers

Pricing

Press Room

Support

Trust

Status

Customer Experience Center

RESOURCES

Blogs

Demos

Webinars

Whitepapers

Datasheets

Infographics

Zero Trust Assessment

ROI Calculator

Businesses @ Work

Identity 101

PLATFORM

Overview

Directories

Integrations

Insights

Identity Engine

Workflows

Devices

FEATURES

FastPass

Passwordless Authentication

Hooks

Admin Experience

End-User Experience

YouTube

Facebook

Twitter

LinkedIn



Oktane21

Explore the future of how people, technology, and identity intersect. April 6-8, 2021, virtual and free.

We use cookies to ensure you get the best experience on our website. By clicking "Got it", you're consenting to our use of cookies.

Cookie Settings

Got it

X

Get Help From Okta

Parsing all of your options isn't easy. Implementing solutions can be even more complicated.

Work with Okta and get robust security solutions delivered by people who can explain your options clearly and carefully. Contact us to get started.

References

[The Encryption Many Major Companies Rely On Has a Serious Flaw](#). (October 2017). Engadget.

[Leonard Adleman](#). National Inventors Hall of Fame.

[New Record Set for Cryptographic Challenge](#). (March 2020). Phys.Org.

[Still Guarding Secrets After Years of Attacks, RSA Earns Accolades for Its Founders](#). (June 2003). *SIAM News*.

[Cryptographic Padding in RSA](#). (January 2009). Science Blogs.

[RSA Encryption: Keeping the Internet Secure](#). (March 2014). American Mathematical Society Graduate Student Blogs.

[Public-Key Encryption by RSA Algorithm](#). Steyerbrains.at.

[Understanding Public Key Cryptography and the History of RSA](#). (February 2012). SecurityWeek.

[Seriously, Stop Using RSA](#). (July 2019). Trail of Bits.

COMPANY

About Us

Careers

Pricing

Press Room

Support

Trust

Status

Customer Experience Center

RESOURCES

Blogs

Demos

Webinars

Whitepapers

Datasheets

Infographics

Zero Trust Assessment

ROI Calculator

Businesses @ Work

Identity 101

PLATFORM

Overview

Directories

Integrations

Insights

Identity Engine

Workflows

Devices

FEATURES

FastPass

Passwordless Authentication

Hooks

Admin Experience

End-User Experience

YouTube

Facebook

Twitter

LinkedIn



Oktane21

Explore the future of how people, technology, and identity intersect. April 6-8, 2021, virtual and free.

Register now

We use cookies to ensure you get the best experience on our website. By clicking "Got it", you're consenting to our use of cookies.

Cookie Settings

Got it

X