JOHN PAVLUS SCIENCE DEC 15, 2024 7:00 AM

The Simple Math Behind Public Key Cryptography

The security system that underlies the internet makes use of a curious fact: You can broadcast part of your encryption to make your information much more secure.

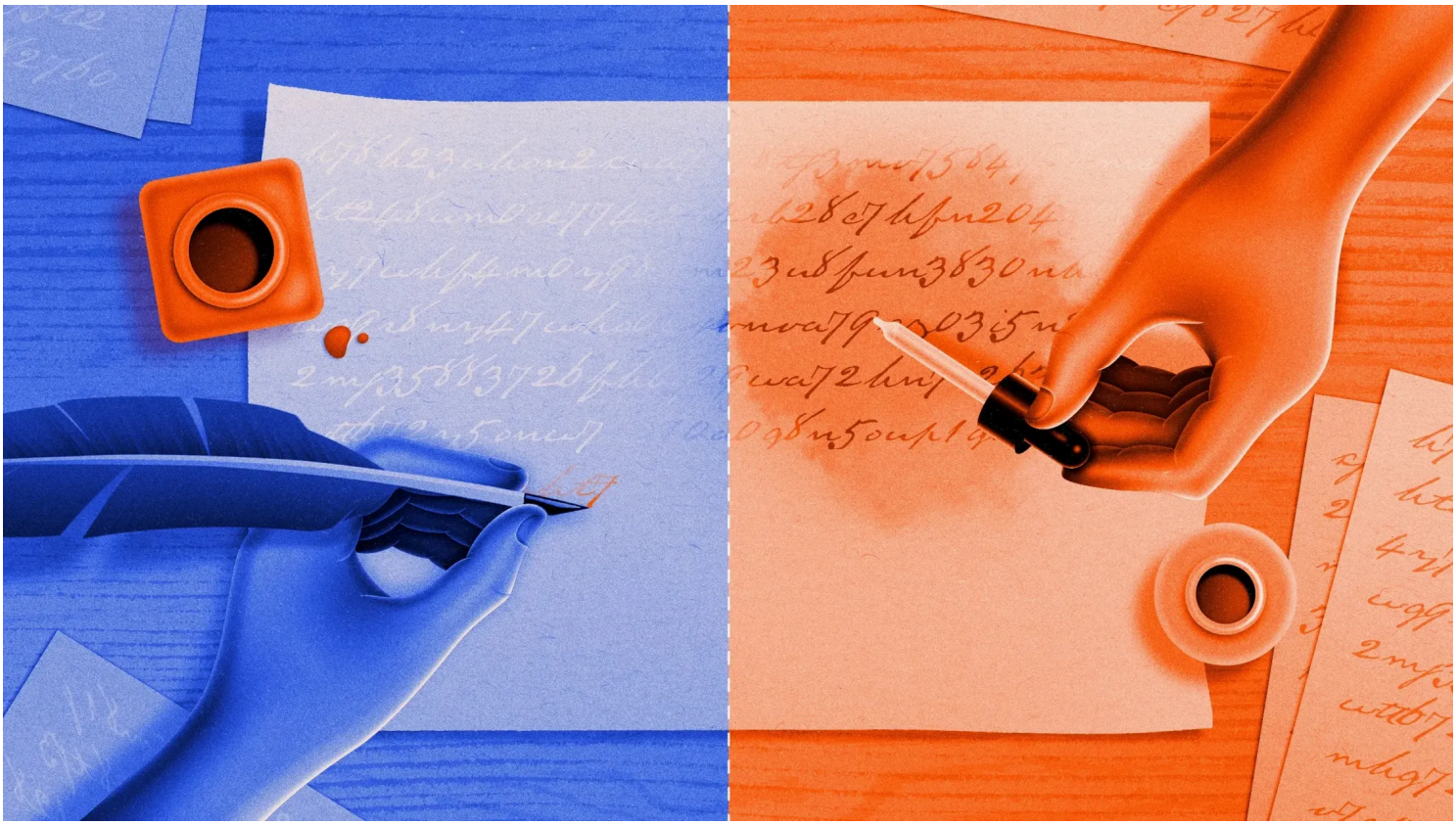


ILLUSTRATION: KRISTINA ARMITAGE/*QUANTA MAGAZINE*

SAVE

If you buy something using links in our stories, we may earn a commission. This helps support our journalism. Learn more. Please also consider subscribing to WIRED

THE ORIGINAL VERSION *of this story appeared in Quanta Magazine.*

For thousands of years, if you wanted to send a secret message, there was basically one way to do it. You'd scramble the message using a special rule, known only to you and your intended audience. This rule acted like the key to a lock. If you had the key, you could unscramble the message; otherwise, you'd need to pick the lock. Some locks are so effective they can never be picked, even with infinite time and resources. But even those schemes suffer from the same Achilles' heel that plagues all such encryption systems: How do you get that key into the right hands while keeping it out of the wrong ones?

The counterintuitive solution, known as public key cryptography, relies not on keeping a key secret but rather on making it widely available. The trick is to also use a second key that you never share with anyone, even the person you're communicating with. It's only by using this combination of two keys—one public, one private—that someone can both scramble and unscramble a message.

To understand how this works, it's easier to think of the "keys" not as objects that fit into a lock, but as two complementary ingredients in an invisible ink. The first ingredient makes messages disappear, and the second makes them reappear. If a spy named Boris wants to send his counterpart Natasha a secret message, he writes a message and then uses the first ingredient to render it invisible on the page. (This is easy for him to do: Natasha has published an easy and well-known formula for disappearing ink.) When Natasha receives the paper in the mail, she applies the second ingredient that makes Boris' message reappear.

In this scheme, anyone can make messages invisible, but only Natasha can make them visible again. And because she never shares the formula for the second ingredient with anyone—not even Boris—she can be sure the message hasn't been

deciphered along the way. When Boris wants to receive secret messages, he simply adopts the same procedure: He publishes an easy recipe for making messages disappear (that Natasha or anyone else can use), while keeping another one just for himself that makes them reappear.

In public key cryptography, the "public" and "private" keys work just like the first and second ingredients in this special invisible ink: One encrypts messages, the other decrypts them. But instead of using chemicals, public key cryptography uses mathematical puzzles called trapdoor functions. These functions are easy to compute in one direction and extremely difficult to reverse. But they also contain "trapdoors," pieces of information that, if known, make the functions trivially easy to compute in both directions.

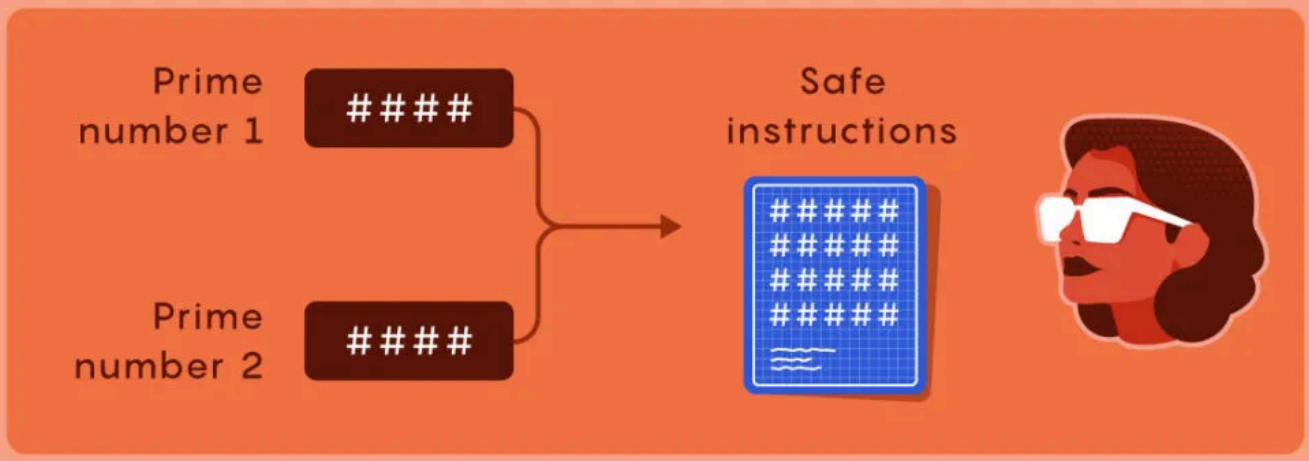
One common trapdoor function involves multiplying two large prime numbers, an easy operation to perform. But reversing it—that is, starting with the product and finding each prime factor—is computationally impractical. To make a public key, start with two large prime numbers. These are your trapdoors. Multiply the two numbers together, then perform some additional mathematical operations. This public key can now encrypt messages. To decrypt them, you'll need the corresponding private key, which contains the prime factors—the necessary trapdoors. With those numbers, it's easy to decrypt the message. Keep those two prime factors secret, and the message will stay secret.

How Public Key Cryptography Works

Modern internet security often involves two keys: a public one that allows anyone to encrypt a message, and a private key that's used to decrypt it. The first key acts like a safe, and the second key unlocks the safe.

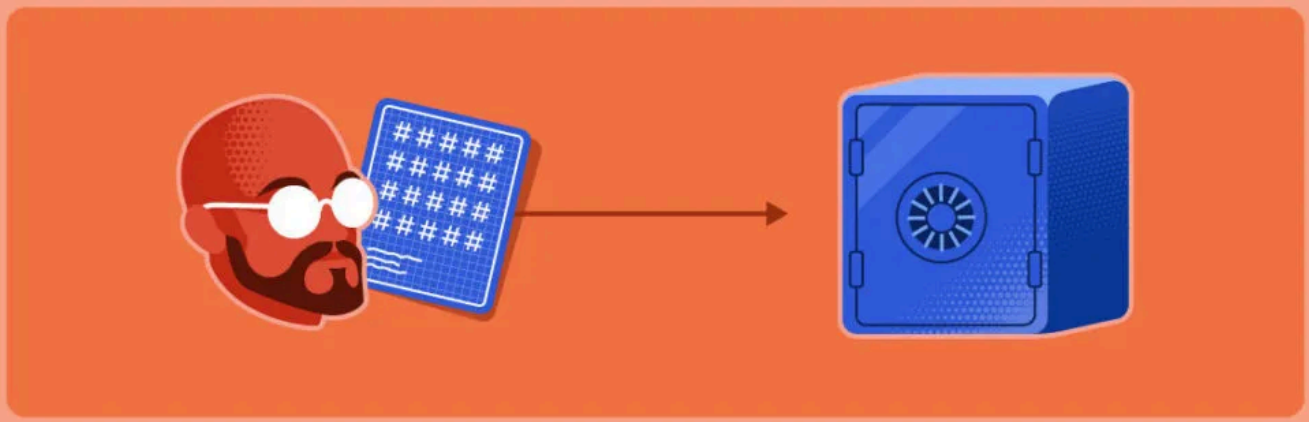
STEP 1: PUBLISH YOUR INSTRUCTIONS

Natasha describes how to build a unique safe. Her instructions are based on a huge number — the product of two large prime numbers.



STEP 2: BUILD A SAFE

Boris reads Natasha's instructions and constructs a safe.



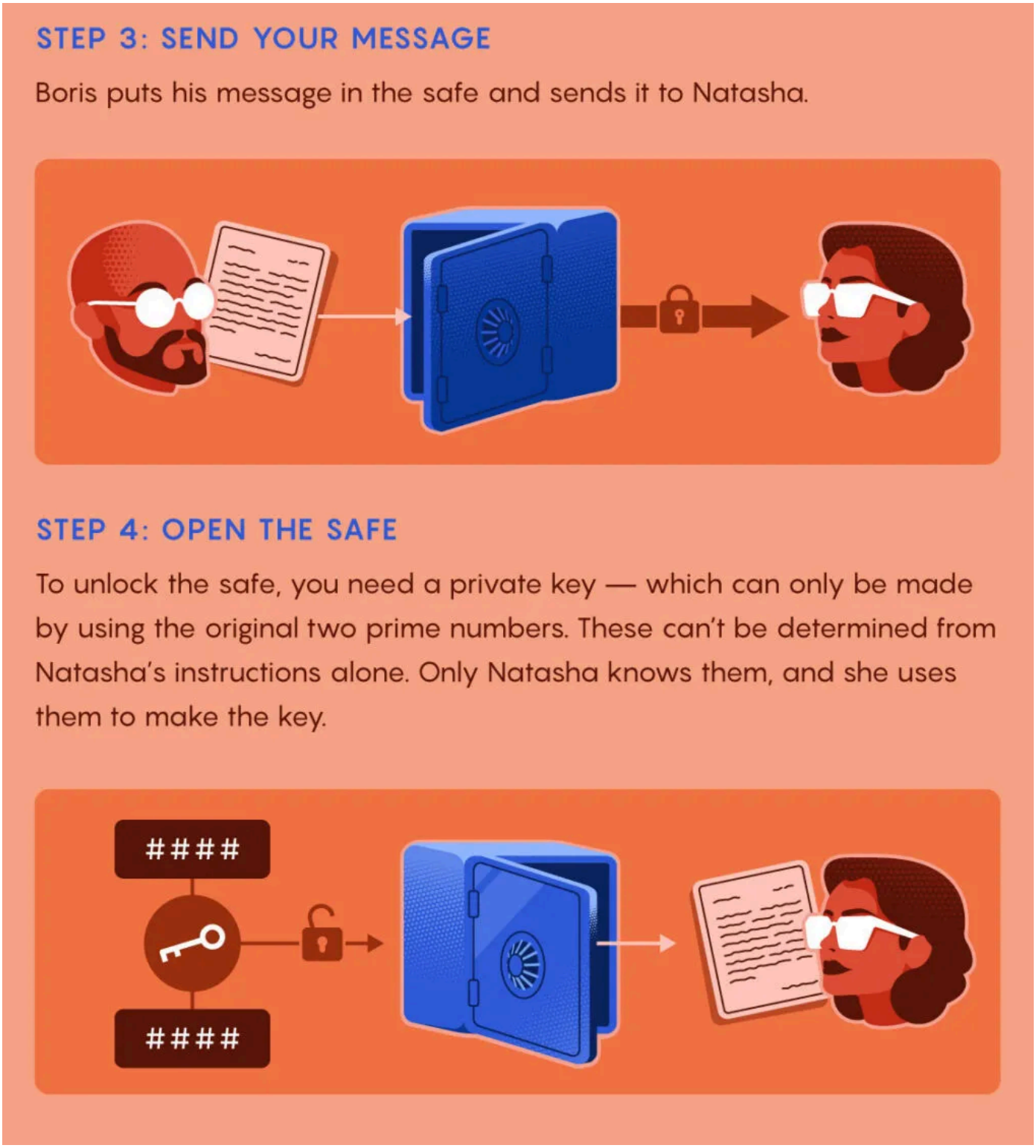


ILLUSTRATION: MARK BELAN/*QUANTA MAGAZINE*

The foundations for public key cryptography were first discovered between 1970 and 1974 by British mathematicians working for the U.K. Government Communications Headquarters, the same government agency that cracked the Nazi Enigma code during World War II. Their work (which remained classified until 1997) was shared with the US National Security Agency, but due to limited and expensive computing capacity, neither government implemented the system. In 1976, the

American researchers Whitfield Diffie and Martin Hellman discovered the first publicly known public key cryptography scheme, influenced by the cryptographer Ralph Merkle. Just a year later, the RSA algorithm, named after its inventors Ron Rivest, Adi Shamir and Leonard Adleman, established a practical way to use public key cryptography. It's still in wide use today, a fundamental building block of the modern internet, enabling everything from shopping to web-based email.

This two-key system also makes possible "digital signatures"—mathematical proof that a message was generated by the holder of a private key. This works because private keys can be used to encrypt messages too, not just decrypt them. Of course, this is useless for keeping messages secret: If you used your private key to scramble a message, anyone could just use the corresponding public key to unscramble it. But it does prove that you, and only you, created the message, since as the holder of the private key, only you could have encrypted the message. Cryptocurrencies like bitcoin couldn't exist without this idea.

If two cryptographic keys instead of one is so effective, why did it take millennia to discover? According to Russell Impagliazzo, a computer scientist and cryptography theorist at the University of California, San Diego, the concept of a trapdoor function just wasn't useful enough before the invention of computers.

"It's a matter of technology," he said. "A person in the 19th century thought of encryption as being between individual agents with military intelligence in the field —literally, in a field with guns firing. So if your first step is 'pick two 100-digit prime numbers to multiply together,' the battle is going to be over before you do that." If you reduce the problem to something a human can do quickly, it's not going to be terribly secure.

But while computers helped make public key cryptography possible, they've also created cracks in its armor. In 1994, the mathematician Peter Shor discovered a way for quantum computers to efficiently reverse the trapdoor functions that underlie most current public key cryptography systems, including prime factorization. This algorithm, if implemented, would act like an all-purpose "reappearing ink," capable of making any invisible message reappear. Goodbye, internet security.

Luckily, quantum computers themselves are "still in the ENIAC phase," Impagliazzo said, referring to the room-size machine built for the US Army in 1945. By the time

quantum computers become sophisticated enough to pose a real threat to public key cryptography, its original trapdoor functions could be replaced by "quantum-safe" versions called lattice problems. Of course, this new computational "ink" may also become susceptible to attack in the future. But that's the great thing about public key cryptography: As long as we can find new functions to use, we can just keep reinventing the wheel. Or in this case, the key.

Original story reprinted with permission from Quanta Magazine, an editorially independent publication of the Simons Foundation whose mission is to enhance public understanding of science by covering research developments and trends in mathematics and the physical and life sciences.

You Might Also Like ...

- **In your inbox:** WIRED's most ambitious, future-defining stories
- Musk takeover: The US government is not a startup
- **Big Story:** The bust that took down Durov and upended Telegram
- WIRED's favorite 'buy it for life' gear
- **Love Bytes:** The brave new frontiers of romance

TOPICS QUANTA MAGAZINE CYBERSECURITY SECURITY ENCRYPTION SCIENCE

Science Newsletter

Your weekly roundup of the best stories on health care, the climate crisis, new scientific discoveries, and more. Delivered on Wednesdays.

SIGN UP

By signing up, you agree to our user agreement (including class action waiver and arbitration provisions), and acknowledge our privacy policy.

READ MORE

Why Computer Scientists Need Magic 8 Ball–Like Oracles

Hypothetical devices that can quickly and accurately answer questions have become a powerful tool in computational complexity theory.

BEN BRUBAKER

Despite Catastrophic Hacks, Ransomware Payments Dropped Dramatically Last Year

Ransomware gangs continued to wreak havoc in 2024, but new research shows that the amounts victims paid these cybercriminals fell by hundreds of millions of dollars.

ANDY GREENBERG

Exposed DeepSeek Database Revealed Chat Prompts and Internal Data

China-based DeepSeek has exploded in popularity, drawing greater scrutiny. Case in point: Security researchers found more than 1 million records, including user data and API keys, in an open database.

LILY HAY NEWMAN

A 25-Year-Old With Elon Musk Ties Has Direct Access to the Federal Payment System

The Bureau of the Fiscal Service is a sleepy part of the Treasury Department. It's also where, sources say, a 25-year-old engineer tied to Elon Musk has admin privileges over the code that controls Social Security payments, tax returns, and more.

VITTORIA ELLIOTT

Federal Workers Sue to Disconnect DOGE Server

Two federal workers, citing reports that Elon Musk's associates are operating an illegally connected email server at OPM, seek a restraining order.

DELL CAMERON

This DOGE Engineer Has Access to the National Oceanic and Atmospheric Administration

Sources tell WIRED that NOAA employees were ordered to give an engineer from Elon Musk's DOGE task force access to all of the agency's Google sites by the end of business on Wednesday.

TIM MARCHMAN

DeepSeek's Safety Guardrails Failed Every Test Researchers Threw at Its AI Chatbot

Security researchers tested 50 well-known jailbreaks against DeepSeek's popular new AI chatbot. It didn't stop a single one.

MATT BURGESS

A Signal Update Fends Off a Phishing Technique Used in Russian Espionage

Google warns that hackers tied to Russia are tricking Ukrainian soldiers with fake QR codes for Signal group invites that let spies steal their messages. Signal has pushed out new safeguards.

ANDY GREENBERG

Meet the Hired Guns Who Make Sure School Cyberattacks Stay Hidden

An investigation into more than 300 cyberattacks against US K–12 schools over the past five years shows how schools can withhold crucial details from students and parents whose data was stolen.

MARK KEIERLEBER

Foreign Hackers Are Using Google's Gemini in Attacks on the US

Plus: WhatsApp discloses nearly 100 targets of spyware, hackers used the AT&T breach to hunt for details on US politicians, and more.

DHRUV MEHROTRA

Elon Musk's DOGE Is Still Blocking HIV/AIDS Relief Exempted From Foreign Aid Cuts

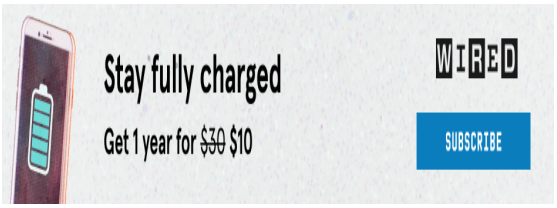
The Trump administration claims it is allowing "lifesaving" foreign aid to continue, but in reality, DOGE is preventing vital work on HIV and AIDS from saving lives.

KATE KNIBBS

US Government Websites Are Disappearing in Real Time

A growing number of US government websites have gone offline as of Saturday, including several related to USAID and others focused on youth programs, Africa, and more.

VITTORIA ELLIOTT



PRIVACY CONFIGURATIONS