

# **mus**e<sup>®</sup>

MARCH 2018



The  
**Heroes**  
& **Villains**  
of Computer  
Security



From Cricket Media

## FEATURES

**10**

### Alice and Bob Are on the Case

Protecting your  
digital privacy

by Mary Alexandra Agner

**18**

### Be a Hacker

... without going  
to jail.

by David J. Bianco and Gina  
DeAngelis

**26**

### Think Your Password

Devices that measure brain-  
waves make it possible.

by Kathryn Hulick

**32**

### I Like the Way You Move!

Gait biometrics could help  
keep the world secure.

by Rebecca E. F. Barone

**42**

### Bitcoin

The invisible money in  
your virtual wallet

by Alice Andre-Clark

# CONTENTS

**DIRECTOR OF EDITORIAL** James M. "Exploit" O'Connor  
**EDITOR** Johanna "Software Worm" Arnone  
**CONTRIBUTING EDITOR** Ka thryn "Clickjacking" Hulick  
**COPYEDITOR/PROOFREADER** Meg "Privilege Escalation" Moss  
**ASSISTANT EDITOR** Maria "Phishing" Hlohowskyj  
**ART DIRECTOR** Nicole "Spoofing" Welch  
**DESIGNER** Kevin L. "Keylogger" Cuasay  
**CARTOONIST** Caanan "Eavesdropping" Grall  
**RIGHTS & PERMISSIONS** David "DDoS" Stockdale

## BOARD OF ADVISORS

**ONTARIO INSTITUTE FOR STUDIES IN EDUCATION,  
UNIVERSITY OF TORONTO**  
Carl Bereiter

**ORIENTAL INSTITUTE, UNIVERSITY OF CHICAGO**  
John A. Brinkman

**NATIONAL CREATIVITY NETWORK**  
Dennis W. Cheek

**COOPERATIVE CHILDREN'S BOOK CENTER, A LIBRARY  
OF THE SCHOOL OF EDUCATION, UNIVERSITY OF  
WISCONSIN-MADISON**  
K. T. Horning

**FREUDENTIAL INSTITUTE**  
Jan de Lange

**FERMILAB**  
Leon Lederman

**UNIVERSITY OF CAMBRIDGE**  
Sheilagh C. Ogilvie

**WILLIAMS COLLEGE**  
Jay M. Pasachoff

**UNIVERSITY OF CHICAGO**  
Paul Sereno

MUSE magazine (ISSN 1090-0381) is published 9 times a year, monthly except for combined May/June, July/August, and November/December issues, by Cricket Media, 70 East Lake Street, Suite 800, Chicago, IL 60601. Additional Editorial Office located at 1751 Pinnacle Drive, Suite 600, McLean, VA 22102. Periodicals postage paid at McLean, VA, and at additional mailing office. One-year subscription (9 issues) \$33.95. Canadian and other foreign subscribers must add \$15.00 per year and prepay in U.S. dollars. GST Registration Number 128950334. For address changes, back issues, subscriptions, customer service, or to renew, please visit [shop.cricketmedia.com](http://shop.cricketmedia.com), email [cricketmedia@cdsfulfillment.com](mailto:cricketmedia@cdsfulfillment.com), write to MUSE at Cricket Media, PO Box 6395, Harlan, IA 51593, or call 1-800-821-0115. Postmaster: Please send address changes to MUSE, Cricket Media, PO Box 6395, Harlan, IA 51593.

Editorial office c/o 70 E. Lake Street, Suite 800, Chicago, IL 60601. March 2018, Volume 22, Number 03, © 2018. Carus Publishing dba Cricket Media. All rights reserved, including right of reproduction in whole or in part, in any form. For information regarding our privacy policy and compliance with the Children's Online Privacy Protection Act, please visit our website at [cricketmedia.com](http://cricketmedia.com) or write to us at CMG COPPA, 70 East Lake Street, Suite 800, Chicago, IL 60601.

Photo credits: C - Olvind Hovland / IKON Images/Newscom, (LT) Sferdon/Shutterstock.com; 5 - Vluw/Shutterstock.com, Jojo Photos/Shutterstock.com; 6 - Eugene Berman/Shutterstock.com; 7 (TC), (BC) Courtesy Chris Danforth/UMM; 8 (RT) Yuzhen Yan, (C) Rawpixel.com/Shutterstock.com, (LT) Courtesy of Hervé Sauquet; 9 (RT) CSAIL/MIT, (RB) meec/Shutterstock.com, (RB-2) Evgeny Karandaev/Shutterstock.com; 12 (bkg) iunewind/Shutterstock.com; 18 (bkg) jivacore/Shutterstock.com; 19 (C) mei yanotai/Shutterstock.com; 20 (TC) REUTERS/Larry Downing, (RB) REUTERS/Lee Jae-Won; 21 (RT) Nir Alon / Alamy Stock Photo; 22-23 MICROSOFT-CYBERCRIME / REUTERS/Jason Redmond; 22 (LB) Peter Barreras/Invision for Netflix, Girl Scouts of the USA/AP Images; 23 (RT) Hero Images Inc. / Alamy Stock Photo; 24 (TC) Ivelin Radkov/Shutterstock.com, (TC-2) vrpotal/Shutterstock.com, (RB) Lorrie Faith Cranor; 25 (LB) Pictorial Press Ltd / Alamy Stock Photo; 26 (bkg) magic pictures/Shutterstock.com, (bkg-2) Preechar Bowonkitwanchai/Shutterstock.com; 27 (RB) Elena Pavlovich/Shutterstock.com; 28 (LT) VECTORWORKS\_ENTERPRISE/Shutterstock.com, (LB), (RB) Courtesy of InteraXon Media; 29 (RT), (C), (LB) Max Curran; 30 (C) kirill\_makarov/Shutterstock.com; 30 (RB), 31 (LT) Carnegie Mellon University CyLab; 32 - Vinay Darekar / Alamy Stock Photo; 33 (RT), 34 (LT), 35 (TC) Courtesy of Motion Analysis; 34 (LB) Lottie Hope / Stockimo / Stockimo / Alamy Stock Photo, (RB) Xinhua / Alamy Stock Photo; 36 (RT) Margaret Kepner; 37 (RT), (RB) Courtesy of John Sims; 38-39 ProStockStudio/Shutterstock.com; 40 (RB) Andrey\_Kuzmin/Shutterstock.com; 42 (C) sliplee/Shutterstock.com, (bkg) Anna\_Jeni/Shutterstock.com; 43 (TC) sliplee/Shutterstock.com; 44 (LT) PixieMe/Shutterstock.com, (LC) Dutoirdumonde Photography/Shutterstock.com, (LB) Casimiro PT/Shutterstock.com, (LB-2) rolandtopor/Shutterstock.com; 45 (RT) posteriori/Shutterstock.com, (RC) Reuters Graphics, (RB) REUTERS/Toru Hana; 46 - Petar Djordjevic/Shutterstock.com, Robert Dunn/Shutterstock.com; Back cover - BEST-BACKGROUNDS/Shutterstock.com.

Printed in the United States of America.

1st printing Quad/Graphics Midland, Michigan February 2018

From time to time, MUSE mails to its subscribers advertisements for other Cricket Media products or makes its subscriber list available to other reputable companies for their offering of products and services. If you prefer not to receive such mail, write to us at MUSE, P.O. Box 6395, Harlan, IA 51593-1895.



## DEPARTMENTS

**2 Parallel U: Like 2 Peas in a Paradox**  
by Caanan Grall

**7 Muse News**  
by Elizabeth Preston

**30 Science@Work: David Brumley**  
by Peg Lopata

**36 Do the Math: Color by Numbers**  
by Ivars Peterson

**47 Your Tech**  
by Kathryn Hulick

**48 Last Slice**  
by Nancy Kangas

## YOUR TURN

**4 Muse Mail**

**14 How to Shout a Secret**  
by Evelyn Lamb

**24 Hands-on: Open Sesame**  
by David J. Bianco & Gina DeAngelis

**38 Hands-on: Finding Your Uniqueness Factor**  
by Nick D'Alto

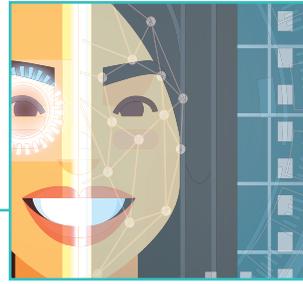
**41 Q&A**  
by Lizzie Wade

**46 Contest: Go Team**



## MS. ACORN

**STRONGLY RESEMBLES** Cate's mom  
**Issa Pine**  
**HEIGHT** 5'9"  
**AGE** N/A  
**FIRST POWERED UP** 1983  
**INTERESTS** Education, human knowledge, the Mnemosyne community, data storage, practical jokes  
**ONCE SAID** "Normally I would fix the gate myself, but this is a mechanical error, not computational. Being a hologram, I need some real hands for this one."



# "LIKE 2 PEAS IN A PARADOX"



WOOF! I CAN'T ANSWER ALL THESE!

← CAANAN (MAKES COMICS) (NEEDS SHOWER.)

I'LL HANDLE THAT ONE.

IT'S ADDRESSED TO ME ANYWAY.

I DO HAVE A BACKUP. DOES THAT COUNT?

I'M 14!

3. IS MS. ACORN REALLY CATE'S MOM? —Jonah B. / age 12 / California

4. How big is your fan mail pit?

I'M BASED ON HER APPEARANCE, NOT HER PERSONALITY, BUT I TREAT ALL MNEMOSYNE'S STUDENTS AS MY CHILDREN. I AM THEIR TEACHER AND PROTECTOR.

I have four questions to ask you:

1. Does Ms. Acorn have any brothers or sisters?
2. How old is Cate?

MS. ACORN (ADAPTIVE CENTRAL OBSERVATION & RESOURCE NETWORK)

CATE (TIMELESS)

Greetings Yorth dimension! I am Queen Khione of Behemothio, the dimension of dragons! We are an unfindable dimension, so don't try. My favorite *Muse* character is O because we both love animals and I think he is awesome, though I also like Ms. Acorn because she is my favorite color. O, is your personality as sunny as it seems? Why don't you want to be known as your full name? Did you know that we are technically the same age? (Just add a bunch of zeroes to 14!)

—Queen Khione of Behemothio / age 14 billion years

P.S. The creature you've dubbed the Leviathan? It came from the Behemothio dimension. Cool, right? She was kind of mysterious, though. I never had the pleasure of her acquaintance, just her presence.

WHEN I WAS LITTLE, I COULDN'T PRONOUNCE MY 'R'S SO I COULDN'T SAY ORION. ALSO, OH IS WHAT PEOPLE USED TO SAY WHEN THEY HEARD MY VOCABULARY AT 3 YEARS OLD.

AND THANKS FOR NOTICING I'M SUNNY! THIS PLEASURES ME. IT MAKES ME EVEN SUNNIER!

TOP LEVIATHAN THEORIES

ORION (DENSE TWEAR A BELT)

DEPRESSURIZATION IS IMMINENT!

Whatsi, can you get me some rocket boots too?! You are my favorite!

—Isaiah F. / age 11 / Minnesota

EVERYTHING IS SCANNED AND CATALOGUED SO IT DOESN'T MATTER HOW BIG THE PIT GETS.

(UNTIL IT STARTS THREATENING TOWNS THAT IS.)

CATE SAYS I DID...DO INVENT THEM, BUT I'M STILL WORKING ON IT.

ONCE I'M PAST THE TESTING STAGE, I'LL CALL YOU!

WHATSI (PIAT ROBOTS)

I have a question for Cate. How do you travel through time so fast?

—Zoey / age 9 / Illinois

FAST?!

SO BORED!

I WAIT 2 TO 4 SECONDS IN THAT BLANK WAITSPACE EVERY TIME I BLINK SOMEWHEN!

(IF YOU KNOW A FASTER WAY, PLEASE DO TELL ME!)

Oh, SYDNEY... THIS IS A CHEAP RUSE FROM HOLLYWOOD DESIGNED TO AUGMENT DRAMA! TIME TRAVEL IS POSSIBLE BECAUSE THERE ARE INFINITE WORLDS!

AARTI (ARTIST - NOW THAT'S SOME NOMINATIVE DETERMINISM)

Aarti, how did you rearrange molecules and atoms to make never-fading color?

—Michael L. / age 13 / Wyoming

MY RAY JUST AGITATES THE SURFACE MOLECULES OF ANYTHING LONG ENOUGH FOR ME TO SEND A NANOCANNEL PATTERN THAT CHANGES ITS PHOTON ARRAY.

IT DOESN'T CARVE OR CREATE, JUST REARRANGES WHAT'S THERE, BUT MOST SURFACES FADE. SOME FASTER THAN OTHERS. CERTAIN MATERIALS DON'T LIKE THE CHANGE.

Responding to Ronald D's letter in the September issue, Cate doesn't time travel because as Chief Seattle said, "Take only memories, leave only footprints."

What I mean is that if Cate went back in time and stopped the World Wars, she would cause a lot of mishaps. She might cause Aarti's mishaps. She might cause Aarti's great great great great great great grandfather to not meet her great great great great great great grandmother, meaning that Aarti would not exist anymore. I hope this explanation makes sense!

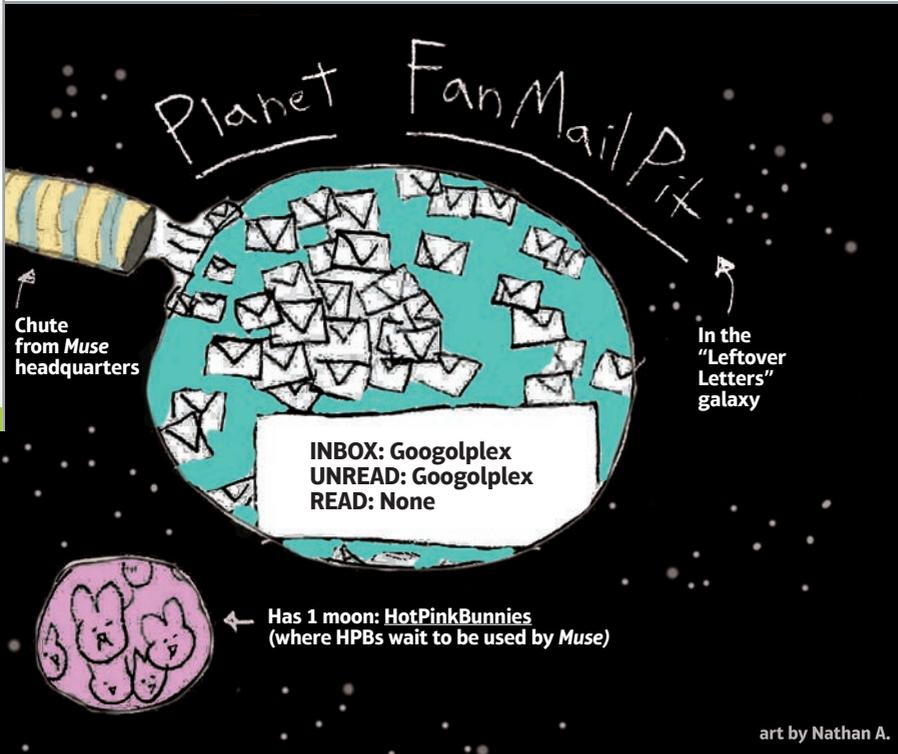
—Sydney L.

EVERY TIME I TRAVEL BACK IN TIME, I INSTANTLY CREATE A NEW TIMELINE. NO MATTER WHAT I DO! I COULD GO BACK AND GIVE MYSELF A WINNING LOTTERY TICKET, BUT THAT WOULD ONLY BE GREAT FOR HER, NOT ME!

I WOULD TRIED TO SEND OUT A THANK YOU CARD BUT I'M HAVING TROUBLE WITH THAT ADDRESS AT THE POST OFFICE. I'LL JUST SAY THANKS HERE INSTEAD!

I have had *Muse* since November/December 2015. Kudos to Caanan Grall for Parallel U and The Editors for making such an amazing magazine. I will never forget you as long as I live.

—IACR AKTR NRC PIA / age 9 / Uae Nir lei Tsc Eoa Of Sa Tm, G2647 g, G2647, Small Magellanic Colud, Local Group, Virgo Supercluster, Laniakea Supercluster

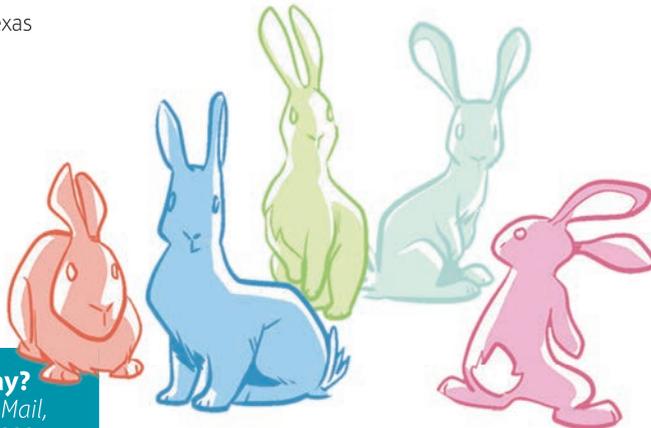


# Planet FanMailPit

I recently learned that one proposed solar system model stated that everything was made up of four elements: fire, water, earth, and wind/air. Shouldn't there have been a fifth element—life?! I mean, what did this guy think?

Also, how big is the fan mail pit (FMP)?! It appears only 10 percent or so actually have their letter in the magazine. The rest go in the fan mail pit. This FMP must be HUGE!!! If *Muse* continues to grow in popularity, you guys will have to create a parallel universe and put a planet called FanMailPit inside of it. Maybe in that universe, there ARE four elements that make up everything.

—NATHAN A. / age 12 / Texas



**Something to say?**  
Send letters to Muse Mail,  
70 E. Lake St., Suite 800,  
Chicago, IL 60601,  
or email them to  
muse@cricketmedia.com.

## Impressive Imaginations

**I am writing to say that the May/June 2017 issue "Water Secrets" contained the craziest letters** I have EVER read, and I love them all. You would have to have a huge imagination to write a letter like that. So, that leaves me thinking . . . are we born with a certain amount of imagination, and it develops? Or are we born with a huge range of imagination, and it decreases over time? If that's true, it explains why the old lady at the grocery store doesn't appreciate me using corn as a laser.

—SAMARA

P.S. Shout-out to The Editors, I don't think you guys get enough credit but I'm probably wrong.

P.P.S. Alien papaya rooster from Mars, I totally believe you about the cheese thing. I have one of you guys as my pet, and they won't stop talking.

## A Fellow Writer

**Thank you, Evan, for showing that 8- and 9-year-olds are quite intelligent** and that there should be (and will be) books where 8- or 9-year-old heroes are, well, heroes. I am working on a book that's like that!

—SYLVIA C. / age 9 / Texas

## The Maker Movement

**I really enjoyed your article on tardigrades** [May/June 2017]. It has always amazed me how they could actually SURVIVE IN SPACE! I mean how cool is that?!?!?! Anywho, I just wanted to say hi to my favorite magazine, and I really hope this letter gets published. (If you are reading this, it obviously has. Hello *Muse* readers!! I'm in a magazine!!)

It would be really cool if you did an article on the maker movement. For those who don't know, it is a movement to take stuff apart, hack things, use cool tech, and learn more about the world around you.

—ETHAN K., SCI-FI WRITER / age 13 / Florida

*Hi Ethan. Glad you mentioned makers. I could spend all day taking things apart, tinkering, and improving stuff, couldn't you?*



—WHATS!

## ANNOUNCING CONTEST WINNERS!

In October 2017, we invited readers to become writers. The challenge? To submit a spooky or suspenseful original short story. We commend every story that arrived—even the ones that made us sleep with the lights on! Check out the winning stories here and on page 46. They really put the AHHH in bravo.

*Woo hoo, Eleanor, Hinke, Lucia, Erin, and Neylan!*

—AARTI



### The Science Fair

BY ELEANOR W. WRITING AS WYNN

RECKLER / age 13 / North Carolina  
Rain pounded down on the roof of Erie Community College on that bleak night of October 30. A night that changed science fairs forever.

Students ran inside to escape the rain. Their sneakers squeaked on the hallways as they walked to Lecture Hall X. The creaky doors welcomed them into the dark expanse.

Judges assured them the power would be back soon and the fair



would go on. The anxious students set up their trifold boards on the tables. Everything was somewhat normal.

Then, a gust of mysterious wind blew open the doors. Lightning flashed, and there in the doorway was a boy with dark hair, appearing to be halfway between mortal and ghost. Behind him rolled a huge cage, eight feet tall with a black cloth over it, looming over everyone darkly. The ghoulish boy whispered something to the judge. Pointing to a table, the judge nodded. The boy strode over and on it placed an unreadable, tattered tri-fold board. Everyone around him shivered.

After one hour of judging, it was the boy's turn. A judge shuffled up and inquired to see his project.

"Gladly." The boy smiled strangely. The cloth plummeted down.

Thunder roared and lightning cracked, revealing the shadow of a giant being in the cage. Someone screamed as a boom shook the hall. The creature's head exploded with wet flesh.

Chaos erupted. People screeched in terror. Students abandoned their projects and fled the hall. Then, somehow,

the lights turned on.

In the cage was a gigantic scarecrow, with its pumpkin-head guts on the floor. The boy had exploded the pumpkin, making everyone think a man's head exploded.

The boy dissolved in the wind and was never seen again, until another rainy night, during a science fair, when a mysterious boy showed up at Erie Community College.

### Nightmare in the Spoon Drawer

BY HINKE Y.

"The old spoon wheezed and cried out, 'It was the fork!'

'Twas the fork that did this to me!' And that was all. He fell over the edge and onto the floor, never to be clean again. That was the moment I realized that one of us was a traitor, an imposter, dare I say it"—sharp intake of breath—"a spork! The most vile of villains, an evil created for the ease of the Big People that slowly drove us out of use, along with our most horrendous enemy, the forks! One of their kind has planted its cold heart in our spoon society, forming an evil so great that one of our elders has died from





it. We must rally together to stop this evil and restore peace in the Spoon Drawer. If you re-elect me, I will stop this madness. Now no more questions, I have business to attend to.”

The mayor pushed his way through the crowd of reporters into the dreary, deserted street. The shadows from The Great Crack From Above shone down, illuminating the figure before him.

It was the creature from his nightmares: half spoon, half fork, an eerie light coming from its four-pronged head. It would have sneered (had it not been—a spork!) as it said, “’Tis I, and I have come for thee! I am the dreaded spork, and I will come to power! Mwah ha ha ha haaa!”

There was a ghastly pallor on the mayor’s polished silver surface.

He was never heard of again.

That terrible nightmare is still out there somewhere, haunting, perhaps, *your* kitchen. He could even be behind you, that laugh stuck in his throat.

Mwah ha ha haaaa!

### Pumpkin Pie

BY LUCIA D. / age 11 /

Massachusetts

“**Hurry Dad!**” I called up the stairs. “If we don’t go now, there won’t be any pumpkins left!”

Yep, typical. We must be the only family that waits until the morning of Halloween to buy a pumpkin. If we didn’t hurry, we wouldn’t have a jack-o’-lantern. So after a rush to the car, we drove to every farm nearby, and nobody had pumpkins. That is, all but one: Gnarly Knolls Farm.

“I don’t know Bella . . .” said Mom after I pointed it out.

But with much begging and pleading from me and my little brother Avery, we found ourselves driving up the driveway to Gnarly Knolls. The big black house loomed above us. We hurried to the patch. There was just one pumpkin left, and it was scarred and gnarly. Next to it on the ground lay one single boot and a watering can. Weird. Anyway, we finally got it into our car, paid at the drop-box, and left.

That evening, at the witching hour, we lit our giant jack-o’-lantern. Ten minutes later, the doorbell rang. We



opened it, expecting a trick-or-treater. But instead, there were just a few mummy wrappings. This happened a few more times. We found a toy sword, a ballet slipper, and a cape. It was almost like the wearers had disappeared.

“Kids these days,” said Dad after the sixth time.

A bit later, Mom and Dad took Avery trick-or-treating. I stayed, determined to figure it out.

The next time the bell rang, I opened the door quick. I saw a pair of legs disappearing through the jack-o’-lantern’s mouth. It burped out a witch’s hat. The pumpkin’s alive! Thinking fast, I ran and got Dad’s axe. I ran outside, swung the axe over my head, and cracked open the jack-o’-lantern. POP! Out came the farmer (that explains the boots and can!) and the trick-or-treaters, all covered in pumpkin guts.

“Well . . . who wants pumpkin pie?” I said, laughing.

#### » RUNNERS-UP

#### Honorable Mention

This month’s runners-up are Arianna G., 12, Vermont; Story S., 11, Sofia, Bulgaria; Xanthe S., 10, Wisconsin; Aggie M., 12, Ontario, Canada; Zoe N., 11, Michigan; Phoebe J., 14; David O., 10; and V. L.



## &gt;&gt; PSYCHOLOGY

## Blue People Share Blue Photos

**D**epressed people share photos on Instagram that are bluer, grayer, and darker than the photos happier people share. Researchers discovered this when they used computers to analyze almost 44,000 photos from 166 volunteers' Instagram accounts. About half of the Instagram users had been diagnosed with depression within the past three years.

The analysis showed that photos posted by people who'd

been depressed tended to look different. On average, they were less bright and had more blue and gray colors. There was also a difference in the filters people preferred. Non-depressed people especially liked a filter called Valencia, which makes photos brighter. Depressed people were more likely to use a filter called Inkwel, which turns color pictures into black-and-white ones. The researchers think the findings might someday help doctors check people for mental illness.

text © 2018 by Elizabeth Preston



>> One of these stories is **FALSE**. Can you spot which one? The answer is on page 37.



>>GEOLOGY

## Record-Setting Ice

**RESEARCHERS DRILLED** a sample of ice from Antarctica that's a whopping 2.7 million years old. Before now, the oldest ice core was about 1 million years old. Air bubbles trapped in the ice will give scientists clues about Earth's ancient climate.



>>MORALS



## Animals Make Bad Teachers

**DID "THE TORTOISE AND THE HARE"** teach you how to take things slow and steady? Did Curious George warn you about the risks of poking around where you shouldn't? Stories for young kids are full of animals that teach lessons about right and wrong, also called morals.

But kids might learn better from human characters.

Researchers in Canada read picture books to children ages 4 to 6. Some kids heard a book about a raccoon that learns to share. Others heard the same

book—but the researchers had changed the illustrations to show human characters, not animals. A third group of kids heard a story about seeds with no moral lesson.

Before and after reading each book, researchers gave kids stickers and told them they could share some with another kid who wasn't there. Kids who heard the story about people sharing gave away more of their stickers afterward. But kids who heard the other two stories didn't. Animals are cuter teachers. But humans seem to be better ones, the researchers say.



>>BOTANY

## This Is What the First Flower Looked Like (Maybe)

**SOMETIME BETWEEN** 140 million and 250 million years ago, the first flower bloomed on Earth. Today its descen-

dants grow all around us in every color, shape, and size. It's hard to imagine what that first blossom looked like. But now scientists have found a way to—almost—peer back in time and see it.

Researchers gathered data on the structure of 792 flower species. They combined that information with fossil

evidence and a family tree based on DNA. Tracing the family tree back, they were able to reconstruct the structure of the first flower. The researchers think the flower probably had male and female parts in the same blossom, like many plants do today. And its petals were arranged in rings of three, not in a spiral. (The ancient flower's color, though, is still a mystery.)





»TECH DESK

## A Sleep Monitor That Lets You Sleep

**TO GET** help with sleep problems, people often have to spend a night in a lab. But being away from home, hooked up to wires and machines, can make it hard to sleep at all. So researchers are working on a new sleep-study method—one that lets people doze comfortably in their own beds.

The method uses a plain-looking device that sends low-power radio waves toward a sleeping person. By analyzing how the waves bounce back,

the device can measure a person's breathing and heart rate. In a new study, researchers trained a computer to use this information to judge when a person is in different stages of sleep: awake, light sleep, deep sleep, or REM. (REM stands for rapid eye movement. Dreaming happens during this sleep stage.) Tracking when people are in each sleep stage can help doctors understand and treat their sleep problems—no wires attached.

»SECURITY

## Pigeons Pick Passwords

**TIRED OF** thinking up new passwords for your online accounts? Soon you may be able to let a pigeon pick your password instead. Or peck your password, that is.

A company in France is developing a pigeon-powered system for creating passwords. Users will be able to request a password from their computers at home. They can specify how long the password should be. The request will go to a lab in France, where trained pigeons will peck at a keyboard until they reach the user's desired number of characters. (The pigeons will work in short shifts, and they'll get to fly around and relax during their off time.)

In tests, researchers have found that passwords created by pigeons are harder for hackers to guess than passwords randomly generated by a computer. And you know a pigeon will never choose the password "PASSWORD."



That's the news!  
Go to page 37 to  
see if you spotted  
the false story.



# ALICE & BOB ARE ON THE CASE

Protecting your digital privacy

*by Mary Alexandra Agner | illustrated by Brad Walker*



lice finishes folding her note for Bob. She glances around the classroom. Her teacher is busy. She taps the student in front of her and points to Bob. Alice watches the note cross the room. Instead of passing on the note, though, Mallory opens it. She laughs to herself. Alice frowns. Mallory folds up the note and hands it to Bob. She turns and smiles at Alice. The smile is *mean*.

Alice is determined to get a note to Bob without Mallory—or anyone else—reading it. *Fine*, Alice thinks. *I'll send him a text.*

The text will face some of the same dangers as the note. Luckily, Alice can handle them. She has lots of experience with cryptography. That's the process of hiding or disguising information using codes.

Alice is an expert. She's also a fictional character famous to computer scientists. Alice, Bob, and mean Mallory have appeared in science papers about cryptography and computers for decades. Scientists use them to represent the real world. The characters help show the reasons people have for sending information—and protecting it too.

## THE TOUCHY-FEELY SIDE OF CRYPTOGRAPHY

When Alice tries to pass her note to Bob, she wants him to be the only person who can read it. She doesn't want Mallory to open it. If Mallory does open it, Alice doesn't want Mallory to understand it. And Alice wants Bob to know that the note comes from *her*.

These are the three goals of cryptography. *Private* communication: only Bob reads the note. *Secure* communication: Mallory can't open, understand, or change the note.

*Authenticated* communication: Bob is certain the note comes from Alice.

Most of these cryptographic goals—privacy, security, and authentication—don't have anything to do with computers or math. They focus on identity and trust. Did the note go only to the right person? Can I trust that this note came from the person it says sent it?

## A LITTLE BYTE OF HISTORY

Once upon a time, cryptography was about scrambling letters. Only certain people could read your scrambled-up note. Everyday citizens didn't need to scramble their messages. But leaders wanted to keep political and military information secret.

One famous method for scrambling messages is the Caesar cipher. A historian describes the Roman emperor Julius Caesar writing confidential notes. In the notes, each letter of each word was shifted *forward* in the alphabet by three letters. In English, this means if Caesar wanted to say "A" in his note, he'd put down "D." Instead of writing "Caesar," he'd write "Fdhvdu." This is a very basic form of encryption. Encryption changes a readable message into, well, nonsense. But it works according to specific rules. A person who knows those rules can unscramble the message.

Now we use computers and the

internet all the time. Ordinary people need to turn their messages into nonsense too. Encryption helps keep dishonest hackers from stealing our bank account information or grabbing our credit card numbers.

And here's where math comes in. Cryptographers use math to turn a message into nonsense. Then someone who's not supposed to read it can't figure out the original message. To scramble and unscramble messages, cryptographers use "keys."

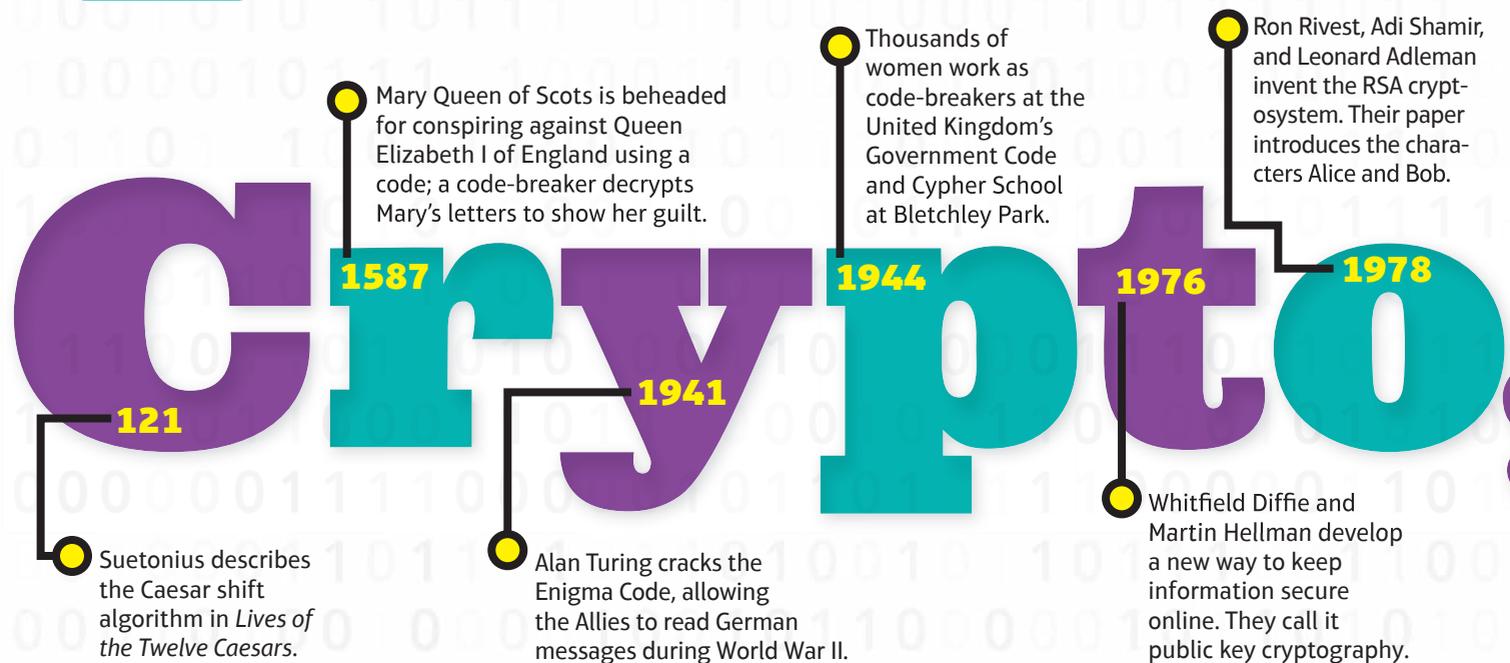
In the 1970s, scientists invented a form of encryption and decryption called public key cryptography. A cryptographic key does the same thing as a real one. It unlocks a message only for the person who has the key. Today, nearly everything you do on the internet uses a form of this encryption.

## ALICE'S ENCRYPTED DAY

Matthew Wright is the director of the Center for Cybersecurity at Rochester Institute of Technology in New York. He says you use encryption "when you connect to sites online, use your credit card, or log in with a password."

Say Alice is using Wi-Fi on her tablet at home. She emails her friends inviting them to her birthday party. Alice's email program may encrypt the message before sending it.

## TIMELINE

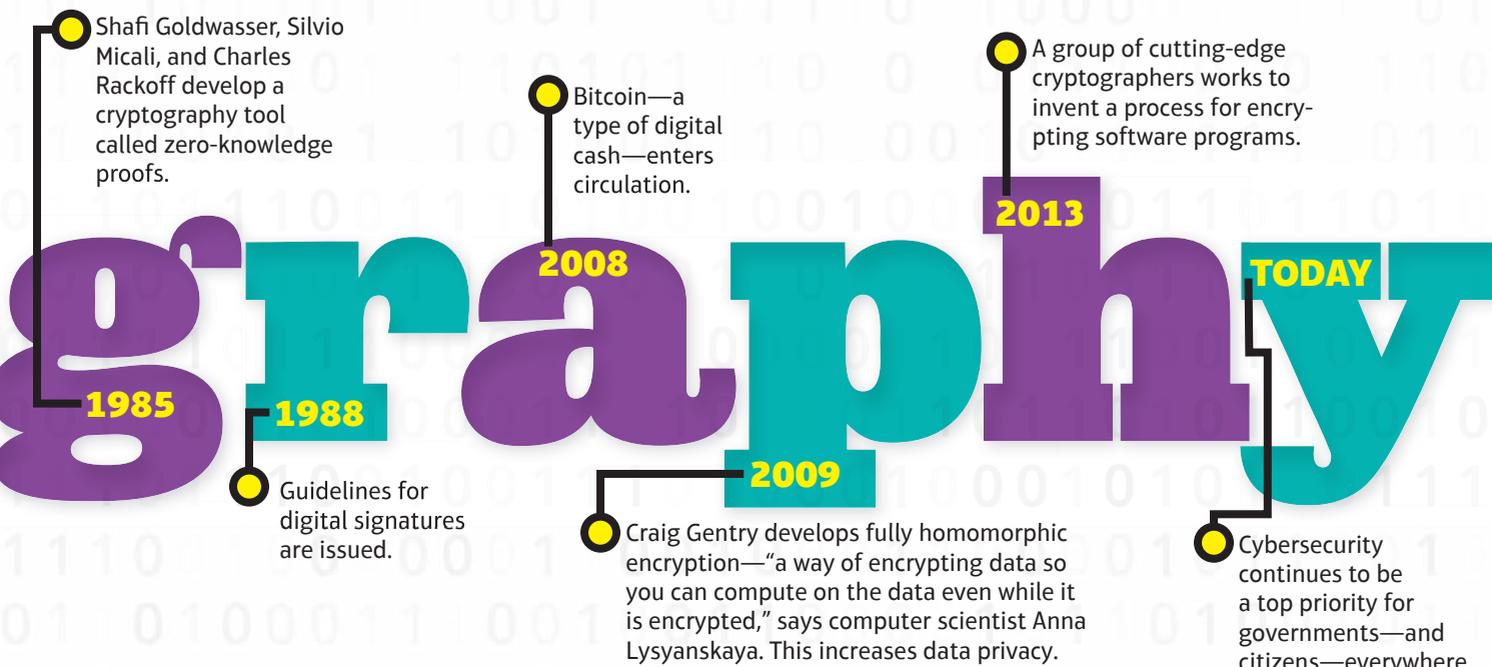


“When you use a wireless connection,” Wright says, “the information is literally flying through the air for anybody’s computer to see.” Wireless connections often use encryption, including the powerful AES cipher. Complex ciphers such as this can prevent Mallory and other hackers from peeking at Alice’s invitation.

When Alice sends a birthday invite, she can also add a digital signature. It proves that she sent it. It also keeps Mallory from changing her invitation. “Digital signatures allow us to establish trust on the internet. [They] allow Alice to ‘sign’ a message and then transmit this signature with her message so that anyone who receives it can check it really came from her,” says Susan Hohenberger. She’s a computer scientist at Johns Hopkins University.

When you swipe or type—or plan a birthday party online—a lot of digital information moves from place to place. It’s usually information that you want to keep private. But all the while, someone like Mallory may be trying to peek. Cryptography will continue to play a large part in our daily lives. Alice, Bob, and a new generation of cryptographers will remain hard at work.

**Mary Alexandra Agner** usually writes in plain English, but she definitely prefers the pigpen cipher to rot13 and the Caesar cipher.



# How to

TRY OUT  
ENCRYPTION  
MATH.

# SHOW IT

# a Secret

by Evelyn Lamb | illustrated by Brad Walker

**T**here's no single best way to scramble, or encrypt, a message. Often, the type of encryption depends on what a message says. Caesar ciphers are just fine if you want to send a quick, secure note to a friend. Those are the codes where you replace every "A" in your message with, say, a "D," every "B" with an "E," and so on (see page 10). But computers can crack them pretty quickly. You'd want a stronger system to keep money or national secrets safe.

Today, many websites use a strong method called RSA encryption. There are several steps along the way from Caesar ciphers to RSA, but we're going to hop, skip, and jump over them to get to the juicy stuff.

$$m^e \equiv m^d \pmod{n}$$

**m:** message

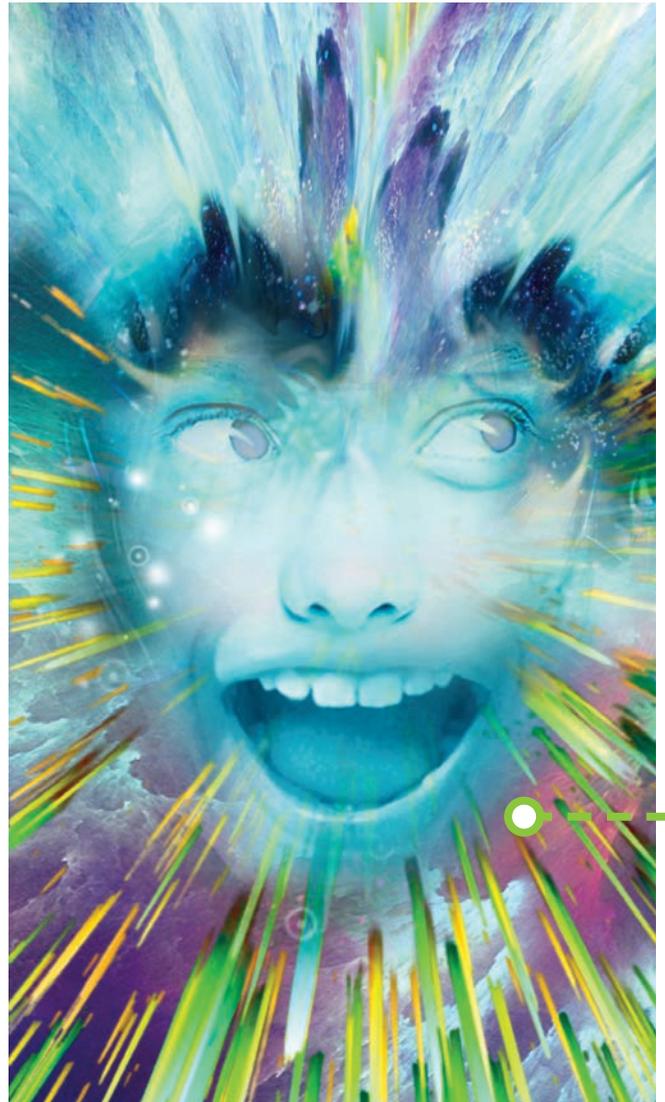
**e:** encryption exponent

**d:** decryption exponent

**mod n:** the remainder when a number is divided by n

**≡:** "equivalent to" in modular arithmetic

**RSA encryption runs on complex math. This equation shows how two exponents work together to allow the right person to understand an encoded message.**





equivalent mod 12, and we use an equals sign with an extra bar to represent that. One great thing about modular arithmetic is that it allows you to work with a finite number of whole numbers rather than worrying about all infinity of them. Any whole number is equivalent to 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, or 11 mod 12. When you work with numbers mod 12, you only have to worry about those numbers, the 12 possible remainders you can get when you divide a whole number by 12.

**TRY FOR YOURSELF:** Take the number 91. 91 divided by 12 is 8 with a remainder of 7. Another way of saying that is that  $91 = 8 \times 12 + 7$ . So 91 is equivalent to 7 mod 12. To find more numbers equivalent to 7 mod 12, we can add 7 to any multiple of 12. Some examples are 19, 31, and 1,099, which is  $91 \times 12 + 7$ . What is your favorite number equivalent to mod 12? A lot of people like the number 7. What is 8 equivalent to mod 7? What about 33? 7774? (Answers on page 46.)

Before we can work our modular arithmetic magic on a message, there's one small detail. People usually communicate in words, which are made of letters (or characters in some languages). Modular arithmetic works on numbers. Before scrambling a message, we have to figure out a way to convert letters into numbers. There are a number (ha ha) of ways to do that. One possibility is to convert every letter to a two-digit number based on its position in the alphabet. A becomes 01, B becomes 02, and so on. Alice's favorite school subject would become 13012008.

Once the message is converted into a number or string of numbers, we can start scrambling. The basic idea is that Bob will ask Alice to scramble the message in a particular way. That's the public key part of the message encryption. Then Bob will use his private key to undo the scrambling once he gets the message. The particular kind of scrambling will rely on special properties of exponents in modular arithmetic.

An exponent tells you how many times to multiply a number by itself. The exponent 2 in the expression  $5^2$  indicates that you're supposed to take 2 copies of the number 5 and multiply them together. That operation is also called squaring or raising 5 to the second power. We could stick any number in instead of 2. So  $5^{17}$  means that we take 17 copies of the number 5 and multiply them all together, for a much, much larger answer.

When we combine exponents with modular arithmetic, we start saying things like  $5^2 \equiv 1 \pmod{12}$ . That's because  $5^2 = 25$ , and 25 has a remainder of 1 when divided by 12.

RSA relies on the fact that sometimes, when you raise a number to a particular power in modular arithmetic, you get your original number out at the end. Instead of looking at mod 12 now, it will be easier to look at numbers mod 5. In this case, we only have to examine the numbers 1, 2, 3, and 4.

When we raise the number 1 to any power, we always get 1. That's kind of boring. But what happens when we look at

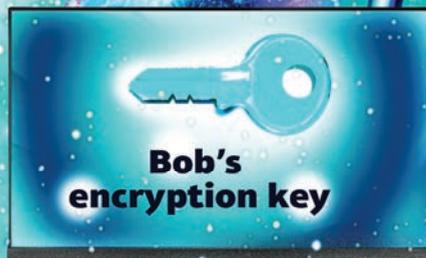
## SENDING THE SECRET MESSAGE

Let's say Alice wants to send a message to Bob using RSA. In RSA, the recipient (Bob) gives information to the sender (Alice). Alice then uses that information to encrypt the message. Bob has both a *public key*, a pair of whole numbers available to anyone, and a *private key*, another whole number he keeps to himself. Alice will use the public key to encrypt the message. Bob will use the private key to decrypt it. If anyone who doesn't have Bob's private key steals the message, it will just look like a caffeinated ferret ran around on the keyboard. Computer scientists refer to systems like RSA as *asymmetric* because Alice and Bob have different information. That's unlike a system like the Caesar cipher, where the sender and receiver have to agree on the details of the shift ahead of time.

How do these mysterious public and private keys work? Math! RSA starts with something called *modular arithmetic*, sometimes known as clock arithmetic. If it's 10 a.m. and you have orchestra practice in five hours, you practice at 3 p.m. Well, obviously, because  $10 + 5 = 3$ , right? Hold on!  $10 + 5 = 15$ , not 3. What's going on here? On a clock, we reset after 12. The fancy mathematical term to describe that is that 12 is the *modulus* of our clock number system. Our clocks work with arithmetic *mod* 12. A mathematician would write something like  $15 \equiv 3 \pmod{12}$ , or  $28 \equiv 4 \pmod{12}$ . The idea is that if two numbers have the same remainder when divided by 12, they're

I want to send a secure message to Bob. Hmm. I'll tell him my favorite subject at school.

**M** +



encryption modulus **n** : 65099131057  
 encryption exponent **e** : 986153243

Alice's message becomes a string of numbers, **M**



Raise to the **e**-th power mod **n**

**M<sup>e</sup> mod n**

$$13012008^{986153243} \text{ mod } 65099131057 = 17113656368$$

Alice sends the message to Bob : 17113656368

the number 2?  $2^2 = 4 \equiv 4 \pmod{5}$ .  $2^3 = 8 \equiv 3 \pmod{5}$ .  $2^4 = 16 \equiv 1 \pmod{5}$ .  $2^5 = 32 \equiv 2 \pmod{5}$ .  $2^6 = 64 \equiv 4 \pmod{5}$ .  $2^7 = 128 \equiv 3 \pmod{5}$ .  $2^8 = 256 \equiv 1 \pmod{5}$ . Do you see a pattern? When we look at powers of 2 mod 5, we get the cycle 2-4-3-1-2-4-3-1... This pattern keeps repeating, and it's 4 steps long. So the 1st power is the same as the 5th power, which is the same as the 9th power, and so on. The 2nd power is the same as the 6th power and the 10th power.

Now let's look at the number 3. When we raise that to successive powers, we get  $3^2 = 9 \equiv 4 \pmod{5}$ ;  $3^3 = 27 \equiv 2 \pmod{5}$ ;  $3^4 = 81 \equiv 1 \pmod{5}$ ; and  $3^5 = 243 \equiv 3 \pmod{5}$ . Just like 2, 3 has a cycle: 3-4-2-1-3-4-2-1...

And finally let's look at the number 4:  $4^2 = 16 \equiv 1 \pmod{5}$ ;  $4^3 = 64 \equiv 4 \pmod{5}$ ;  $4^4 = 256 \equiv 1 \pmod{5}$ . When we multiply 4 by itself over and over mod 5, we just flip back and forth between 4 and 1. 4-1-4-1...

What can we notice when we look at the cycles we get when we raise numbers to successive powers mod 5? The numbers 2 and 3 have cycles of length 4, and the number 4 has a cycle of length 2. The number 1 doesn't really have a cycle. It just stays put no matter what power we raise it to. But whatever number we start with, we know that raising it to the 5th power is the same as doing nothing to it. So is raising it to the 9th, 13th, 17th, 21st, or any other power that is equivalent to 1 mod 4.

If you try to scramble a number by raising it to the 3rd power mod 5, someone else can unscramble it by raising it to, for example, the 7th power because when you're working with exponents,  $(a^3)^7 = a^{21}$  for any number  $a$  you start with. We just saw that when we're working with arithmetic mod 5, any number raised to the 21st power is just itself again.

## WANT TO EXPLORE MORE

about the math of RSA encryption? Resources include *The Code Book: The Secrets Behind Codebreaking* by Simon Singh.

Alice's message decoded

$$M^{ed} \equiv M \pmod{n}$$

$$\begin{array}{c} 13012008 \\ = \\ \text{MATH} \end{array}$$

$$17113656368^{33} \pmod{65099131057}$$

Raise to the **d**-th  
power mod **n**

$$M^e \pmod{n} + \text{Bob's decryption key } d:33$$

Nice, a message from Alice! Let me see if I can decode using my decryption key.

**TRY FOR YOURSELF:** Can you find a number  $n$  so that, no matter what  $a$  is,  $a^n \equiv a \pmod{7}$ ? To start off, we'll test  $a=2$ .  $2^2=4 \equiv 4 \pmod{7}$ .  $2^3=8 \equiv 1 \pmod{7}$ .  $2^4=16 \equiv 2 \pmod{7}$ . For the number 2, we find that as we raise it to successive powers, we get the cycle 2-4-1-2-4-1... When we raise it to the 1st, 4th, 7th, and so on power mod 7, we will always get a 2. What about the numbers 3, 4, 5, and 6? The free online calculator Wolfram Alpha has modular arithmetic built in. You can type your equation into the search bar at [www.wolframalpha.com](http://www.wolframalpha.com). Use the caret symbol, ^, for exponents. (Answers on page 46.)

## DECRYPTING THE SECRET MESSAGE

Bob's public key is the information he shares with the world, which Alice uses to encrypt her message. It consists of an encryption modulus (we'll call it  $n$ ) and an encryption

exponent we'll call  $e$ . He keeps secret another number called  $d$ . He chooses this number so that no matter what the message is, raising it to the  $ed$ -th power will leave it unchanged. In other words, he selects  $e$  and  $d$  so that  $m^{ed} \equiv m \pmod{n}$ , no matter what  $m$  is. He asks Alice to encrypt her message,  $m$ , by raising it to the  $e$ -th power mod  $n$ . So she sends him the message  $m^e \pmod{n}$ . When it comes time to decrypt the message, he raises the transmission  $m^e \pmod{n}$  to the  $d$ -th power mod  $n$  to get  $m^{ed} \pmod{n}$ . Because of how he chose  $e$  and  $d$ , the result is just  $m$  itself.

Let's look at an example. Suppose Bob chooses 5 as the modulus  $n$  with encryption exponent  $e$  equal to 3 and decryption exponent  $d$  equal to 7. If Alice sends a message encoded as the number 2, she would figure out that  $2^3=8 \equiv 3 \pmod{5}$  and send Bob the message 3. Bob would receive that message and raise it to the 7th power because 7 was his decryption exponent.  $3^7=2187 \equiv 2 \pmod{5}$ . Bob accurately decrypts Alice's message: 2.

In the real world, the modulus needs to be a lot bigger. Bob would take two huge prime numbers, probably hundreds of digits each, and find their product. That product would be the encryption modulus. A hacker who wanted to crack the code would have to factor an enormous number to figure out Bob's decryption exponent. That task can take years. If people ever find fast methods of factoring large numbers, a lot of secrets will be a lot less safe. So far, no one has been able to do that.

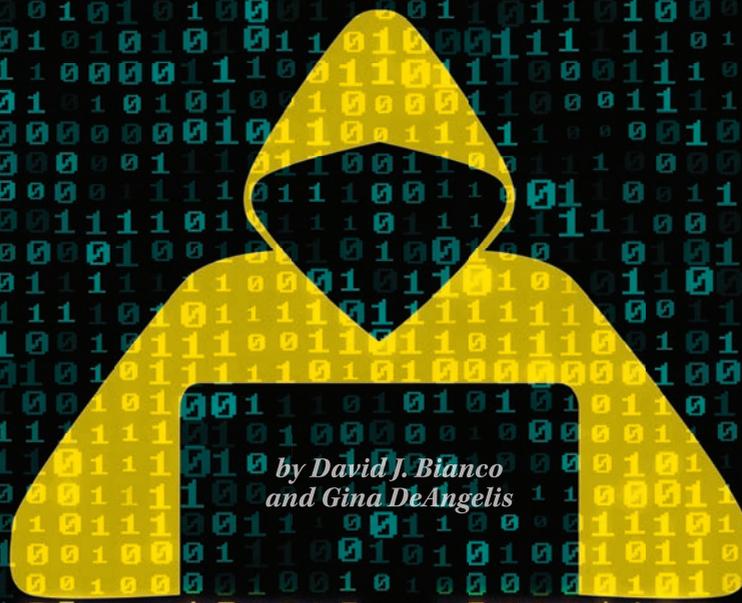
**TRY FOR YOURSELF:** Alice wants to tell Bob her favorite number, 13. If Bob's public modulus  $n$  is 15 and public encryption exponent is 7, what message will Alice send to Bob? For an extra challenge, can you find a decryption exponent  $d$  Bob could use to decode the message? You'll want to use the Wolfram Alpha online calculator to experiment with solutions for this problem. (Answers on page 46.)

In 1915, G. H. Hardy, a famous English mathematician, said number theory—the study of things like modular arithmetic, prime numbers, and relationships between whole numbers—was useless. He didn't mean it as an insult. He loved playing with the ideas in number theory, whether they were useful or not. Today, this "useless" field of mathematics keeps credit cards and national secrets secure.

**Evelyn Lamb** is a math and science writer living in Salt Lake City, Utah. Contrary to popular belief, she has never had a secret identity as an international spy intercepting nefarious plans from supervillains and changing them to embarrassing poetry. All her coded messages are about pizza. Vhqq slccd.

# EEA

If you pay attention to the news, you'd be forgiven for thinking that hackers are bad people. There's always some story about hackers breaking into computers to steal information. Or hackers have locked up computers so the owners can't access their own files without paying a ransom. Those activities are against the law. But not all hackers are criminals. Some use their skills to help people and actually *fight* computer crime.



*by David J. Bianco  
and Gina DeAngelis*

# WITHOUT GOING TO JAIL

## WHAT IS A HACKER?

The terms “hacker” and “hacking” have been around for some time, but it wasn’t until the 1950s and 1960s that those words started to refer to machines and the people who use them. At that time, a hacker was simply someone who was good at solving mechanical problems, especially in clever and creative ways. It was a compliment!

Unfortunately, not everyone with these skills chooses to use them for good. Over time, the meaning of the word “hacker” has changed. Now we speak of “black-hat hackers”—those who commit computer crimes. “White-hat hackers” are those who fight computer crime. Black hats and white hats often have the same skills, but what they choose to do with them is entirely different.

## WHO ARE THE WHITE HATS?

Most white-hat hackers are professionals with a passion for computers. Some white hats work for large companies or other big organizations, like governments, to help protect those networks against black hats. Some research new ways to hack to better understand how to secure computers and networks against new types of attacks.

White-hat hackers hold a wide variety of jobs. They have two things in common, though. First, the people doing these jobs are driven by curiosity about computers and networks; they love to learn new things. And second, what makes them white-hat hackers is their code of ethics.



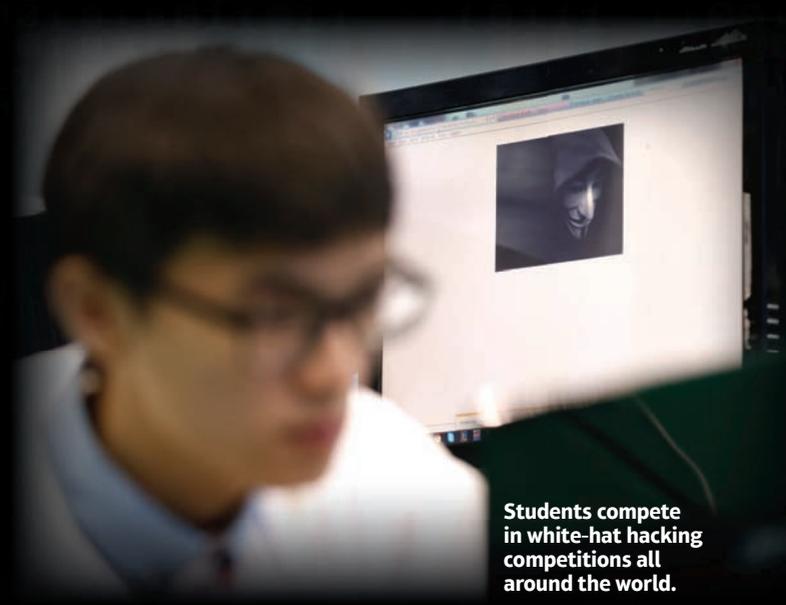
At the National Operations Center at the U.S. Department of Homeland Security, screens outnumber people.

## THINKING LIKE BLACK HATS

Imagine you have a treasure you need to keep safe. You lock it in a box, put the box in a secret place, and even hide the key somewhere you think no one will ever find it. But what if some thieves think of something you didn't? What if, for example, they watched you hide the box, so they know where it is? Would the lock on the box be good enough to protect the valuables inside, or could they pick the lock and steal the treasure? Or could they just go around the lock entirely and break open the box itself?

If you really want to keep that treasure safe, you have to think like thieves do. Figure out what someone intent on stealing might try to do, and use those ideas to make your defenses stronger. For example, you might use a tough box material that's harder to break. Maybe you take more care to ensure you're not followed when you check on it.

Keeping bad guys out of computer networks is a lot like locking up treasures. Safeguards like firewalls, antivirus software, and encryption help keep attackers out. But attackers are tricky and skilled. And they often have all the time they need to figure out ways around your defenses. Even if you're a white hat, you still need to *think* like a black hat.



Students compete in white-hat hacking competitions all around the world.

## "HERE LET ME BREAK THIS FOR YOU..."

At school, at work, and at home, we're surrounded by computers—desktop and laptop PCs, phones, and tablets. Even devices like some televisions and refrigerators contain internet-connected computers. We trust each of these computers with pieces of our lives. Private messages and



## Wanna Try It?

**You don't have to wait until you grow up to be a hacker.** Your school may have a computer or robotics club, both of which are great places to start learning how to program. Your librarian may also recommend books written especially to help kids learn to code.

There are even hacker conferences for kids all over the country. One of the most well known is r00tz Asylum, held in Las Vegas, Nevada, each summer as part of a larger security conference for adults called DEF CON. R00tz is a mixture of talks and hands-on opportunities where kids learn directly from experts—some of whom are other kids! The topics change every year. They usually include things like hacking wireless networks, breaking encryption, soldering electronics projects, picking locks, and much more. Get hacking!



goofy or embarrassing photos, where we are or where we're going at every moment, what we search for or watch online, and who we talk to. Plus, doctors and governments keep information about each of us on their computers. In some cases, even the act of driving is controlled by computers inside the cars.

We depend on the security of all of these devices for privacy and safety. But it's difficult to know how secure they are. Some manufacturers try very hard to create secure products, and some barely try at all. But when two devices are sitting side-by-side on a store shelf, there's no way for you, the buyer, to know which type you're getting.

That's where vulnerability researchers come in.

A security weakness or flaw is known as a vulnerability. A vulnerability researcher is someone who takes a particular computer, device, or piece of software and uses his or her hacking skills to look under the covers and find out how things work inside. These researchers look for flaws they can use to make the device do things it shouldn't. Sometimes that means getting access to information they

shouldn't be able to see (such as private photos stored in that system). Other times, it could mean making the device do something that may be unsafe (disabling the brakes on a car, for example, or dispensing the wrong medication). Of course, most of this work is performed in a lab on fake data—not real people's information. That means the researchers can test their targets without worrying about violating anyone's privacy or causing real harm.

When researchers do find a vulnerability in a piece of software or a device, they create a small program called an exploit. The exploit demonstrates and takes advantage of the vulnerability. Researchers usually write short papers describing the vulnerability and how the exploit works. They send the papers to the manufacturer's security team to help *them* understand the flaw so they can fix it.

In many cases, the manufacturer will fix the vulnerability in future software and devices. They may also update devices they've already sold. Vulnerability researchers make everyone safer by identifying and helping to fix problems—hopefully before bad guys discover and exploit them.

Cate, we should *not* be seeing this.

Let's fix the flaw, pronto.



## SCOUTS SCORE NEW BADGES

Girl Scouts just earn badges for finding their way in the woods and building campfires, right? Wrong! Starting in late 2018, Girl Scouts will have new ways to earn badges, learning such things as how to keep cell phones secure and to how to hack computers.

Whoa! Aren't Girl Scouts supposed to do good things? Absolutely! Hacking can mean protecting information. So the Girl Scouts of the USA want to encourage scouts to protect computers from thieves, or black-hat hackers. These badges will be all about learning how to be white-hat hackers—and more.

The Girl Scouts, in collaboration with Palo Alto Networks, a cybersecurity company based in California, designed 18 new badges. They aim to encourage greater interest in cybersecurity, a field that currently employs more men than women. The badges will represent achievements such as making sure your social media feed doesn't get hacked, combating cyber-bullying, or avoiding scams and hoaxes. Scouts can also earn badges by learning how to fight online crime such as theft, spying, and data manipulation. For Girl Scouts, earning these badges may be the first step in becoming cybersecurity experts and pursuing careers in this field. So they're still blazing trails. Just in a new direction.

—Peg Lopata



## PLAYING FOR THE RED TEAM

Some white hats hack their way into a company's or an organization's computers. A group of these hackers is called a red team.

Red teams use the same techniques, software tools, and skills as black hats, but they're actually working to help their employers protect networks. A good red team spends a lot of time understanding their company's business and what types of computers and software it uses. They use this information to figure out the most valuable things on the company's networks. Then they plan and execute an attack to "steal" those things.

The red team carries out attacks in secret. If they are successful (and they usually are), they work with the organization's computer administrators to help them understand why the attack worked. Then the organization can protect against that type of attack in the future. The red team is constantly testing their employer's defenses and helping to make sure any holes they find are fixed quickly. Then they go off and secretly plan their next attack.



A “heat map” represents data as colors. This heat map at the Microsoft Cybercrime Center shows computer attacks in Western Europe.

## THE LAST LINE OF DEFENSE

Sadly, no matter how good an organization is at defending its computers, sometimes the bad guys’ attacks are successful. Whether they get into a single computer or an entire network, someone has to kick them out and make sure they can’t get back in. Those “someones” are incident handlers.

Incident handlers act somewhat like your body’s immune response. When an attacker invades the network, incident handlers rush to the scene (virtually) and engage the attacker directly. They do everything they can to slow down and stop the attack. Then they help “heal” the network by kicking out the attackers and bringing everything back to normal.

Incident handlers specialize in figuring out when bad guys have breached the security of their organization.

(A breach is called a “security incident.”) They also know the best way to stop them, hopefully before the bad guys get what they came for. Big companies and governments often have their own team of incident handlers. If they don’t—and sometimes even if they do—they hire a team of consultants to deal with specific incidents.

Incident handlers have to know all the black hats’ techniques so they can recognize bad guys’ moves. And they have to know enough about their organization’s business to deal with the attacks in a way that causes as little trouble as possible. And, because everyone is constantly discovering new vulnerabilities or coming up with new techniques, incident handlers have to be able to recognize and thwart *totally unknown* types of attacks too. They have to be ready for literally anything at any time.

These are just a few examples of the careers available to skilled, ethical hackers. The need will only grow. In the years ahead, look for white-hat jobs that haven’t even been dreamed of yet!

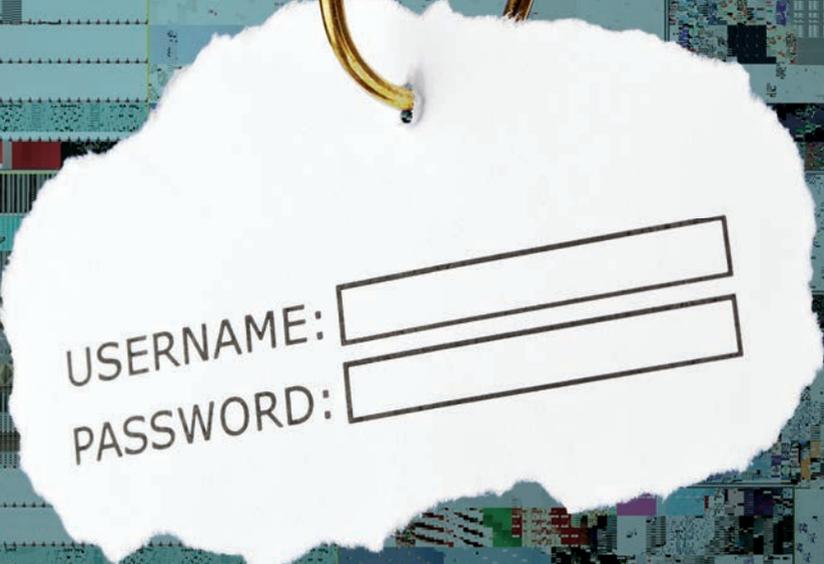
**David J. Bianco** started learning about computers when he was a kid by programming the display models in a department store. By day, he is a security professional who uses his hacking skills to track bad guys and thwart cybercriminals. Kind of like Batman, but poorer and less nocturnal.



Incident handled.

Orange-purple team out. For now.

**Gina DeAngelis** writes books and articles for young people on many subjects. She first wrote about hackers in 1997, and now here she is again. It’s as if there are many more computers today, and the people who operate them are becoming more numerous and powerful. This sometimes makes her think that she got into the wrong line of work.



USERNAME:   
PASSWORD:

by David J. Bianco and Gina DeAngelis

## OPEN SESAME!

Test your password smarts.

**PEOPLE HAVE** been using passwords to protect computer accounts for more than 50 years, so you'd think we'd be pretty good at it. But many of the things we think we know are wrong.

How much do you know about passwords? Take this quiz and find out!

### TRUE or FALSE

- 1) "P455w0rd#" is a good password.
- 2) It's not safe to use the same password for many different sites or accounts.
- 3) You should never write down your password.
- 4) You should never share your passwords with anyone else.



Lorrie Faith Cranor is a computer science professor at Carnegie Mellon University. Cranor made a quilt and a dress that show off her research into "bad passwords."

## ANSWERS

**1)** False. Passwords should be nearly impossible for someone else to guess, which means not using a simple word in English or another language. Many websites have rules to force users to create stronger passwords, like “passwords must contain at least 6 characters, with a mix of upper- and lower-case letters, numbers, and symbols.”

“P455w0rd#” follows many websites’ rules, but it’s still not strong enough. It uses the simple (and guessable) word “password.” And most of the substitutions are common (like “4” for “A” or “5” for “S.”) Computers can test over 100,000,000 passwords per second. So they can easily guess even complex-looking passwords like this one.

**2)** True. We all have a lot of logins to keep track of. It’s tempting to use the same password everywhere. But if your password to one account or website is stolen or guessed, then all your other accounts are at risk too. It’s safer to use different passwords.

**3)** False. With a different password for each account, it can be hard to remember them all. Of course, writing them down in a notebook would solve that . . . but what if you lose the notebook? What if someone else finds it?

You can safely “write down” your passwords in a secure password manager. That’s a piece of software that stores your logins in an encrypted file on your computer, tablet, or phone. It usually syncs between these devices, so you can use it from anywhere. You need to remember only a single master password for the manager itself. The software keeps track of all the others.

**4)** True (mostly). Sharing a password with someone else is like sharing your identity. People you share with can become you, at least for that account, and you’ll have very little control over what they do in your name. So, as a rule, don’t share your passwords.

However, limited sharing may

be a good idea. Some parents require their kids to share passwords to certain accounts so they can monitor what’s happening online.

Another type of sometimes-OK sharing is a little surprising: sharing access to a password manager. Password managers keep your information safe partly by locking out anyone who doesn’t enter the master password correctly. But what if you forget your own master password? Some allow you to choose a parent or trusted friend who can access your account. But they have to ask for access and then wait. During the waiting time, the password manager sends you a message to ask if you want to allow access. If you really did forget the password, you can allow access or do nothing until the waiting period expires, and they’ll get in. But if somebody is trying to pull a fast one on you, you can deny the access, and your passwords remain safe.



## What Are the Magic Words?

Password managers do a great job, but you can also create your own strong passwords that are easy to remember by using a “passphrase.”

How? Take your favorite book down off the shelf, and choose a page and sentence or long phrase at random. Then take the first letters of each word, and all the punctuation, and make a password out of them. Say you choose the book *Alice in Wonderland* and the phrase is:

‘My name is Alice, so please Your Majesty,’ said Alice very politely;

Your password might read:

‘MniA,spYM,’sAvp;

Now that would be hard to guess. Just make sure to choose a fairly long sentence. At least 12 words is best.



**DEVICES THAT  
MEASURE  
BRAINWAVES  
MAKE IT  
POSSIBLE.**

*by Kathryn Hulick*

It's your best friend's birthday. You want to send a text. So you pick up your phone. "Passthought?" a voice says in your ear. You close your eyes. And you imagine diving into a swimming pool. The phone unlocks.

Wait. What just happened? You didn't type a password. You didn't scan your fingerprint. All you had to do was think.



billions of cells. These are called neurons. They use jolts of electricity to communicate. Different groups of neurons control body movements, thoughts, feelings, and more. The brain is always sparking with electricity. Scientists call this electrical activity “brainwaves.”

Scientists can measure brainwaves. All they need are small metal discs called electrodes. The electrodes press against the head in different places. Each one tracks the strength of the brain’s electrical signals. The result is a chart of signals called an electroencephalogram (e-LEK-tro-en-SEF-a-lo-gram), or EEG for short.

## FROM CAPS TO EARBUDS

EEG readers come in many shapes and sizes. Some resemble caps. These may be studded with dozens of electrodes. Others look like headbands or earbuds. Some include only a few electrodes. More electrodes gather more information. But they also make a device expensive and bulky.

Even a big, fancy EEG cap can’t actually read a person’s thoughts. “We are nowhere close to reading anybody’s minds using EEG,” says Chuang.

Brainwaves aren’t detailed enough. The skull muffles the signals. Imagine that you want to listen to a concert. But you have to stay outside the building. It would be harder to hear. Now imagine that several concerts are happening at the same time inside the building. You’d hear noise. But it would be very difficult to make out the words of any one song.



EEG caps aren’t fashion statements. They measure the brain’s electrical signals.

## BRAIN POWER

Today’s phones don’t let you think your password. But in the future, passthoughts may be normal. John Chuang builds and tests passthought systems. He’s an engineer at the University of California, Berkeley. “A passthought is just like a password,” he says. “You get to choose what you want to think about.” You could imagine diving. Or singing “Happy Birthday.” Or your dog doing a trick. If you think the right thought, the system lets you in.

What makes this possible? First, you need a device that can listen to the brain. The human brain is packed with



## CHOOSE YOUR PASSTHOUGHT

In one study, John Chuang's team asked volunteers to try out different kinds of passthoughts. What would you choose for each one?

- ➔ Pick a favorite sport. Imagine a motion in that sport (swinging a golf club, for example).
- ➔ Pick a song and imagine singing it.
- ➔ Pick whatever you want to think about. Make sure it's something you can bring to mind easily.

Still, if you recorded the noise, you could track overall patterns. You could learn to recognize specific patterns. This is what a passthought system does. To use the system, a person first thinks the same thought again and again. Electrodes collect the brainwave patterns each time. The system learns to recognize the pattern. It will let the person in only when it sees a matching pattern.

### THE BEST KIND OF PASSWORD

A good password lets in the right person. But it also keeps others out. This is far from easy. Security experts divide passwords into three categories. The first kind are tokens that you own, like car keys. The second kind use secret knowledge. For example, a bunch of letters and numbers that you type in. The third kind, called biometrics, involve your body. Examples include your fingerprints or the patterns in your eyes.

A strong security system uses more than one of these categories. More steps make it more difficult for the wrong

person to get in. But more steps also annoy the right person.

A passthought combines two steps into one. It involves secret knowledge. Only you know your secret thought. It also involves biometrics. Each person has unique brainwave patterns. "If you told me your passthought is singing 'Happy Birthday,'" says Chuang, "I still will not be able to use it. My brainwave signals are different from yours, even though we're thinking the same thought."

What if someone did manage to steal your unique "Happy Birthday" brainwave pattern? Then you could just pick a new thought to think next time. Most biometrics aren't flexible like that. If someone steals your fingerprint pattern, you can't just get a new finger.

### FOILED BY JUMPING JACKS

Passthoughts sound awesome. And they work very well when a person sits quietly and focuses. But what if the person just drank a cup of coffee? Or just did 50 jumping jacks? Those activities both change brain activity.



### ANOTHER MUSE!

Passthought systems aren't yet commonplace. But you can already control some apps and devices with your thoughts. Muse is a brain-sensing headband. Its electrodes track brainwaves. They send the information to an app. This app aims to help people meditate. Its software can supposedly tell calm, focused brainwaves from excited, stressed ones. The app gives points for long periods that appear calm and focused. Other brain-sensing EEG devices allow people to play simple games or even control wheelchairs.





Chuang’s team tested the jumping jacks question. They brought in 10 volunteers. These people put on EEG readers. They counted red rectangles on a computer screen. Next, they did one minute of jumping jacks. Finally, each person counted the same red rectangles again.

The same person counting the same red rectangles should produce the same brainwave pattern. But that’s not what happened. The jumping jacks changed the pattern. Exercise spurs lots of brain activity. This was kind of like adding a very loud band to the crowded concert hall. Chuang’s team couldn’t recognize the red rectangle brainwave pattern in all that extra noise. However, after the volunteers rested for about 45 seconds, the pattern went back to normal.

But a person using a passthrough system might want or need to exercise at the same time. What if a business person is running to get to a meeting on time? With the current system, she wouldn’t be able to log in right away. She’d have to rest first.

And exercise isn’t the only problem. Coffee, medication, or even mood swings can change a person’s brain enough to mess up a passthrough system.

Chuang proposes one way around this problem. A person could record several versions of the same passthrough. One could be at rest, another while running, and a third while drinking coffee. Then the system would recognize all three of those patterns.



A UC Berkeley engineering team uses these earbuds to record brainwaves. They created the earbuds themselves using a 3D printer.

## ARE YOU ACTING LIKE YOURSELF?

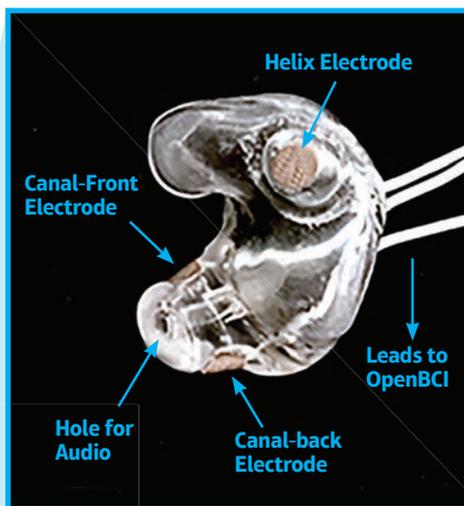
In the future, devices and apps might not need passwords at all. These devices might automatically check who you are. They may watch your face or listen to your voice. They may also collect brainwaves. If this information matches who you say you are, you’re all set. No logins required. “You don’t need to stop even for a few seconds and prove who you are,” says Chuang.

But this raises an interesting question. What if you’re not acting like yourself? Sometimes people get very angry or upset. They may drink alcohol or take drugs. Then, they may make bad decisions. A device that collects brainwaves might be able to tell when someone is acting

strangely. That device could kick the person out until he or she returns to normal.

This could be a good thing. For example, a car could stop a drunk person from driving. But on the other hand, do we really want our devices to decide what we can and can’t do? Also, a device that is always checking identity is always watching. It’s always seeing and hearing you, as long as the device is on.

Maybe you find that creepy. But maybe you don’t. A device that responds to thoughts may be just too cool and convenient.



**Kathryn Hulick’s** passthrough would be imagining swinging on a swing set. Oops. Shouldn’t have told you!



by Peg Lopata

## DAVID BRUMLEY

COMPUTER SCIENTIST AND CYBERSECURITY ENTREPRENEUR

**David Brumley** is on a mission to keep computers secure. As he puts it, his work is “fundamentally about helping support trust in cyberspace.” He also runs contests that teach hacking skills in a safe environment.

Brumley and his team at his

company ForAllSecure are working on protecting computers using automated cybersecurity systems. He says this type of cybersecurity system is like a self-driving car. “I want to make it fully automatic—like an autopilot to protect computers against attackers!”





## WHAT'S THE BEST WAY TO TRAIN A NEW GENERATION OF PEOPLE WHO'LL PROTECT COMPUTERS?

The biggest thing is to give people—hackers—space to explore and permission to think outside the box. Hackers are the only people who make sure computers are safe. Without hackers, who would check that?

## SO HACKERS AREN'T THE BAD GUYS?

Hackers are not criminals. A hacker is someone who explores technology, who is always trying to understand how things really work. Hackers help find problems so that we can create a safer internet. A *criminal* hacker is someone who breaks into computers without permission.

## WHAT'S IT TAKE TO BE A HACKER?

Cybersecurity is like a big puzzle. You're trying to figure out what can happen. Hacking requires three things: grit, creativity, and the desire to learn.

## ARE SOME PEOPLE NATURALLY GOOD AT HACKING?

Anyone can develop hacking skills. It's no harder to learn than basic science or math.

Anyone who decides to learn and keeps at it can become really good. They just have to stick with it and keep learning new things and trying them out.

## SOUNDS PRETTY FASCINATING TO LEARN.

Learning to hack gives you freedom. Technology can shackle people. You get locked in. Hacking is about showing you a way to understand technology so deeply you gain control over it, instead of it controlling you.

## CAN YOU LEARN SOME OF THOSE SKILLS IN CYBERSECURITY COMPETITIONS?

These competitions, called “Capture the Flag” contests (or CTFs), teach computer skills by asking you to hack in a safe environment. PicoCTF, the competition where I'm the team leader, is really a set of puzzles. Each puzzle has an answer. The puzzles usually require you to think about new things, so we provide links to tutorials. Self-learning is huge in hacking.

## DOES PARTICIPATING IN THIS COMPETITION REALLY HELP SOMEONE BECOME A BETTER HACKER?

Playing CTFs is a great way to learn new skills and test yourself against others. PicoCTF works just like any other form of education. You start out with some things that just require critical thinking and then slowly turn up the difficulty. As you progress, you get better. Students who solve all the challenges are some of the most highly sought-after people I know. Some are offered jobs before even beginning college!

## IS THERE ANYTHING UNIQUE ABOUT YOUR COMPETITION?

We focus on offense: finding new vulnerabilities.

## WHEN DID YOU GET INTERESTED IN COMPUTER SCIENCE?

I started using computers in the sixth grade. If I used the computer I didn't have to go to the class in session. It took me a long time to find out that there wasn't just one right way to get started learning about computers. I remember being pretty confused. I eventually found out you could just pick a topic, like programming, look up a tutorial, and go from there.

## HOW DID YOU GET INTO CYBERSECURITY?

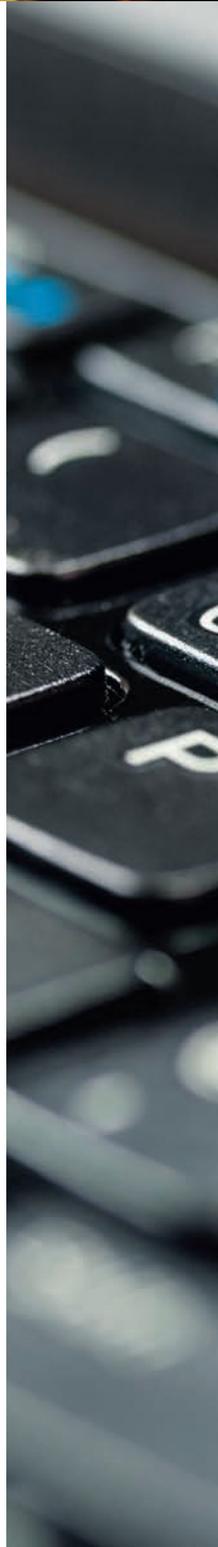
In college, I got a job helping with the university computer systems. I was asked to help out when a criminal broke into the computer. That got me hooked!

## SOUNDS LIKE YOU'RE STILL HOOKED.

I spend most of my free time learning about new things. Right now there are a lot of unknowns and always a chance to research new ways to make computers safe.

---

**Peg Lopata** is a freelance writer living in southern Vermont. Thanks to talking with David Brumley, she's confident she can tackle her computer when it acts up.



# I LIKE THE WAY YOU MOVE!

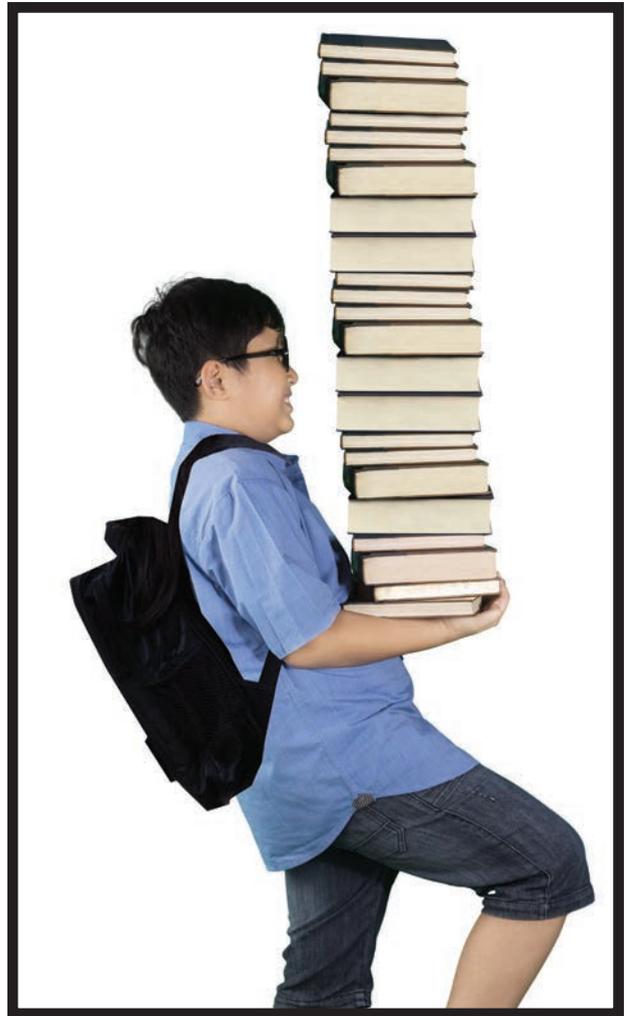
Gait biometrics could help keep the world secure.

*by Rebecca E. F. Barone*



# M

ost of us humans walk around—but that doesn't mean we're all moving the same way. The next time you're with your family or a few good friends, close your eyes and listen to their steps. Chances are you can tell who is who just by the way they walk.



These differences may identify and verify who you are. They're your very own walking password!

## A Walk All Your Own

Try this—fill a backpack with heavy books and then pile another stack of books as high as you can carry. Now walk down a hallway with the backpack on and the books in your arms. Are you walking differently than you would normally?

You're probably taking shorter, slower steps. Both your step length and gait speed have changed. These measures are called *spatio-temporal* metrics. They describe how a person moves through space and time.

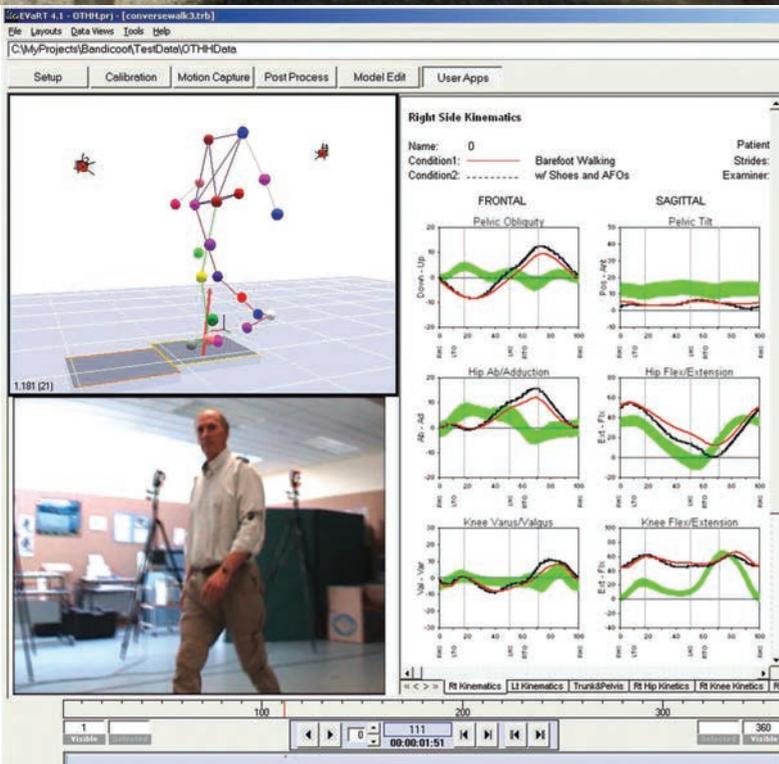
What else happens when you carry a lot of weight? Your ankles, knees, and hips all move differently than they do normally. The study of joint angles in motion is called *kinematics*.

During normal, healthy walking, joint angles differ between people by only a few degrees. Scientists have confirmed that though this difference between people is small, your brain can identify people by their walk alone. One question in gait analysis today is whether

Characteristics that identify you as uniquely *you* are called biometrics. These include parts of your body, like your fingerprints or the pattern of the iris in your eye or the shape of your ear. They also include behaviors, like how you sign your name or the way you walk. All of these features may be used as passwords. Some people have been using fingerprints for years to access computers, phones, or workspaces. Facial biometrics became mainstream technology with the iPhone X. The smartphone unlocks after recognizing the owner's face.

What if your phone stayed unlocked while you walked around with it, but shut down if an unknown person carried it around? What if doors only opened for people whose gait they recognized through security cameras or other sensors? Identification based on the way we walk, or gait biometrics, may offer a new layer of security.

Walking is pretty simple. It's just putting one foot in front of the other. But somewhere within that motion, also called *gait*, little differences make each walk unique.



reflective targets. Special mo-cap cameras record only the light reflected from these targets. They do not record the surrounding area, equipment, or other people. The cameras record hundreds of frames per second. This means the cameras snap hundreds of individual images every single second while they're recording.

A powerful computer program takes in information from the cameras and assembles it to make a model. The program can figure out the positions of the reflected targets down to the millimeter. Building the model is like connecting the dots to make a new picture of the subject for every single frame.

The model helps scientists studying gait to examine how each part of the body moves during walking. The computer model can show the joint angle of any part of the body as well as useful info like gait speed and step length.

## Real-World Data

Outside of the lab, devices need to figure out gait metrics without the help of mo-cap cameras. Luckily, smartphones and many intelligent electronics already contain the sensors they need to determine spatio-temporal information.

Accelerometers, which measure changes in speed, are a standard feature in many smartphones. They help the phone know when you rotate it to switch from portrait to landscape mode. Today, apps also use them in everything from virtual reality to pedometers to gait analysis. Gyroscopes help collect additional data by determining the phone's orientation relative to Earth's gravity.

Measuring acceleration is one of the most basic parts of gait analysis. Every time your foot hits the ground when you take a step, it stops moving. By measuring this change in speed, an accelerometer can record when each foot strikes the ground. Measuring how often this happens

we can make the computers inside phones, security cameras, and other electronics intelligent enough to recognize the differences like our brains can.

## Mo-cap Chat

Scientists use motion capture technology (mo-cap for short) to perform state-of-the-art gait analysis. You may be familiar with mo-cap. Have you ever watched how special effects are created for action movies or video games? If you've seen an actor wearing a black bodysuit covered in shiny little balls, you know what we're talking about! Scientists and Hollywood special-effects companies use the same motion systems.

Mo-cap subjects wear suits dotted with small, highly





helps calculate gait speed. Engineers can also use this information to figure out the distance between steps. Getting so much information from this simple sensor is important because accelerometers are included in almost every smart device we carry.

To take gait analysis to the level of biometrics, though, engineers must be able to match a particular gait to just one person. Pattern-recognition software makes this possible. These computer programs take in large amounts of data and find patterns that are hard for humans to spot.

Gait speed and step length are only two of the simplest patterns, or metrics, that a gait biometrics program might recognize. But these two metrics can change for any person. Remember how your step length and joint angles changed while carrying books? Are these metrics and those from the pattern-recognition software enough to consistently identify you as you?

Amazingly, yes! Research has shown that your smartphone can learn to recognize you by gait speed and step length—and by other features determined by pattern-recognition software. Gait speed and step length are good starting points in simple cases. In more complex cases, like when terrain changes or when someone is carrying heavy loads, pattern-recognition software may ID people based on mathematical analysis. Intelligent algorithms use advanced math to find the nuggets of identification buried in all of the changes.

Scientists have performed most of these experiments, however, in controlled environments in labs. More work is still needed to prove that similar results occur outside of the lab. But researchers say it looks promising.

## Fooling the System

Passwords can be hacked. Could a security system based on gait biometrics be fooled too?

It's not easy. Researchers have found that people need to use special equipment to trick a gait biometrics system. To successfully imitate someone else's walk, the trickster has to use a treadmill to control gait speed. He or she also needs a computer to tell when steps are too large or too small. But, even with all of these tools in place, it still takes several practice sessions learning how to walk like someone else to fool a computer program.

Of course, the more information a system has, the harder it is to hack. For example, online banks often require multiple steps to log in. In the same way, a more secure gait biometrics system will measure more metrics. Some state-of-the-art research systems are developing methods to record kinematics, such as hip or torso movement, using wearable sensors. If these sensors were incorporated into our everyday devices or clothing, this additional information would increase the security of gait biometrics.

## Tomorrow's Passwords

Coming up with new and more secure ways to identify you—and keep everyone else out—will always be a tricky problem. There are still challenges to overcome, like integrating the complex software into smartphones and adding kinematics, but one day, biometrics like gait may be all you need to keep your world secure. You'll never have to worry about forgetting your password again. It's all in the way you move!

Science writer **Rebecca E. F. Barone** always forgets her passwords. She thinks gait biometrics is a great way to free up brain space to remember other things... like where she hid her chocolate.

## COLOR BY NUMBERS

Watch what happens when math and art come together.

When some people think about numbers, they imagine colors, shapes, and patterns.

Picture the whole numbers from 1 to 256. Each of these numbers is either a prime number (divisible only by itself and 1) or a composite number (the product of two or more primes). The only exception is 1, which is in a category all by itself. So, 2, 3, 5, 7, 11, 13, 17, and 19 start off the list of primes. The other numbers (4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, and so on) are composites.

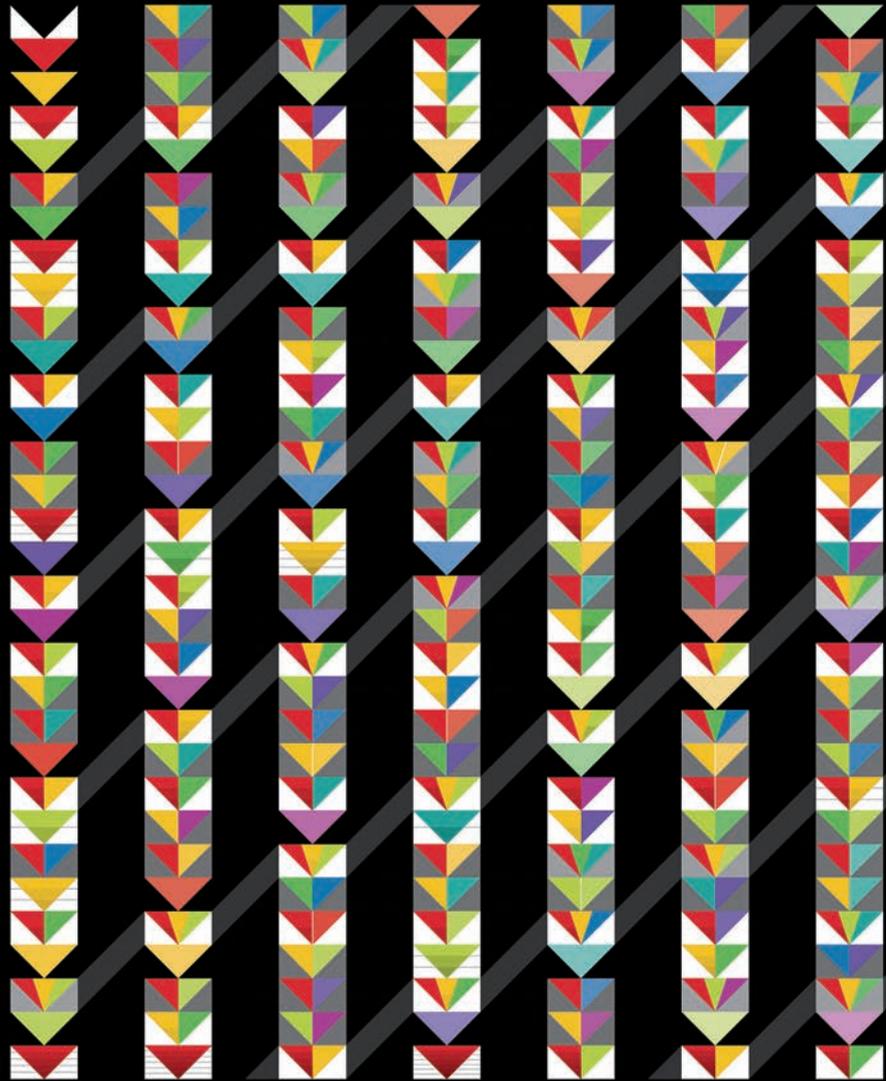
Artist and math lover

Margaret Kepner has translated these numbers and their properties into a vivid design. It combines the beauty of art with the logic of mathematics. Creating her colorful designs on a computer, Kepner has explored a wide range of mathematical topics, from magic squares, tiling patterns, symmetry, and knots to fractals and movements on a chessboard. “My background in mathematics provides me

with a never-ending supply of subject matter,” Kepner says. “I particularly like to combine ideas from seemingly different areas.”

Her design for “Prime Goose Chase” is based on a traditional pattern for sewing together rectangular and triangular patches to make a quilt. Often referred to as “wild goose chase,” this pattern features long columns of triangles.

Kepner’s artwork shows the numbers from 1 to 256 in eight





In artist Margaret Kepner's design, triangles with unique colors represent prime numbers. Subdivided triangles represent composite numbers.

columns of 32 triangles. Each number has its own triangle. A black triangle represents 1 at the upper left corner. Primes are shown as triangles of a single, unique color. You'll notice that 2 is red, 3 is gold,

5 is yellow-green, continuing up to 19, which is magenta. Larger primes repeat the colors of the first eight primes, but mixed with increasing amounts of white.

Triangles representing composite numbers are subdivided. For example, because  $6 = 2 \times 3$ , the triangle for 6 is half red and half gold. In the case of 4, which is a square number ( $2 \times 2$ ), Kepner divides the triangle

horizontally, with the top and bottom parts a slightly different shade of red. Other visual clues, such as the background color, highlight additional number properties.

To Kepner, this artwork serves as a visual table for the study of number patterns, such as the distribution of prime numbers. "As I work," she says, "I like moving back and forth between a math concept that intrigues me and the creation of visual images that interpret this concept in different ways."

Of course, Kepner's design isn't the only way to represent these numbers and their properties. Can you come up with your own scheme?

**Ivars Peterson** is a freelance writer, blogger, and author of *The Mathematical Tourist*. He loves looking for the math hidden in paintings and sculptures displayed in art galleries.



### 3/14: Happy Pi Day!

Mathematician and artist John Sims has tackled the mysteries of the number pi, the ratio of a circle's circumference to its diameter. Starting with 3.14159265, the decimal digits of pi run on forever. There's no apparent pattern to help make it easier to work out the digits or memorize them.

Sims started out with a drawing of pi's decimal digits on a square grid. Successive digits formed a spiral from the center. He then gave each digit from 0 to 9 its own color, producing a checkerboard of colored squares. Amish quilters in Sarasota, Florida, turned the pattern into a genuine quilt with a black border.

What would you do with the digits of pi?



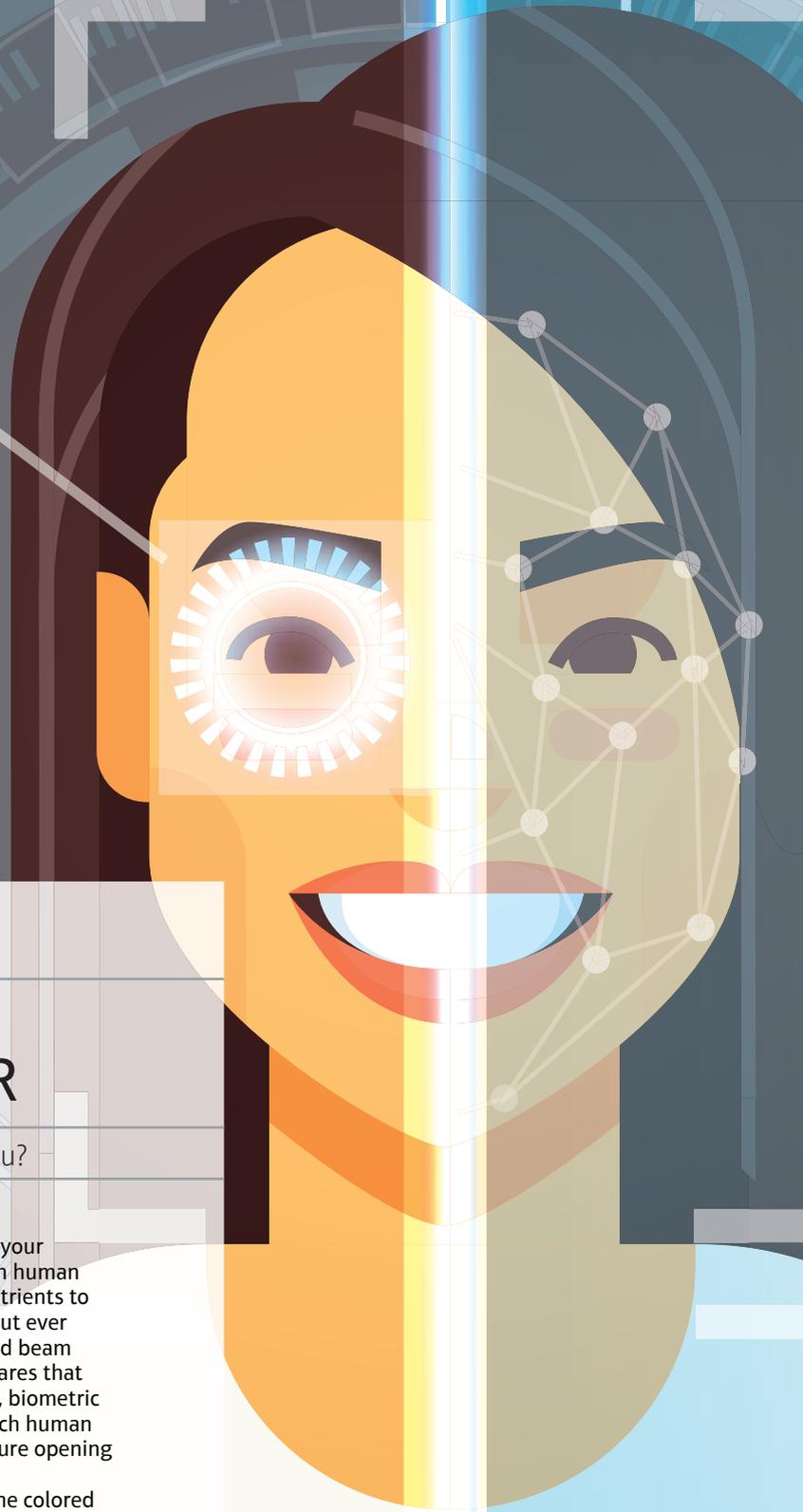
by Nick D'Alto

## FINDING YOUR UNIQUENESS FACTOR

Can 8 questions identify the one and only you?

**WHEN YOU GO ON VACATION**, airport cameras may scan your retinas—the image-forming surfaces inside the eyes. Each human retina has a unique pattern of blood vessels delivering nutrients to its cells. (Amazingly, you see past these tiny vessels without ever noticing them!) In retinal scanning, a low-powered infrared beam maps the shapes of these vessels. Then a computer compares that pattern to a database. In today's security-conscious world, biometric identification—detecting the unique characteristics of each human body—could provide the ultimate measure of safety. Picture opening a lock, where *you* are the key.

From the unique pattern of radiating lines in the iris (the colored portions of your eyes) to the characteristic shape of your palms, any distinctive physical trait may identify you. All biometrics systems include ways to observe a trait and to describe it—often mathematically—and then compare it to known examples.



## Try Out Low-Tech Biometrics!

Imagine you're in a room filled with strangers. They all look close to your age. Another kid in the room has a list of characteristics. Her goal is to introduce herself to the person who matches all of those characteristics. That's you! But she's never met you before. Will she be able to identify you based on your visible traits and behaviors? In effect, can biometrics spot the one and only you?

Let's test the chances that your unique characteristics can ID you. Most people don't have retinal scanners or fingerprint kits handy. So we'll need a simpler method. To start, just answer the questions below.

### You'll need

- » The questions and data below
- » Pen or pencil and paper
- » Calculator, optional

#### Start with these questions.

- 1. Which describes you: male or female?** (Male 0.50, Female 0.50)
- 2. What color are your eyes?** (Brown 0.41, Blue 0.32, Hazel 0.15, Green 0.12)
- 3. Are you a righty or a lefty?** (Righty 0.90, Lefty 0.10)
- 4. Do you wear glasses?** (Yes 0.30, No 0.70)
- 5. Fold your arms. Do you fold them right over left, or left over right? (Try the other way—isn't that clumsy?)** (Left/Right 0.50, Right/Left 0.50)
- 6. Clasp your hands. Do you clasp left over right, or right over left? (Doesn't the other way seem strange?)** (Left/Right 0.50, Right/Left 0.50)
- 7. Stick your tongue out slightly. Can you make your tongue into a "u"?** (Yes 0.80, No 0.20)
- 8. For this last one, you'll need to get barefoot. Which is longest: your big toe or your second toe? Or are they both the same?** (Big toe\* 0.70, Second toe\*\* 0.20, Both same 0.10)

#### Now follow these instructions.

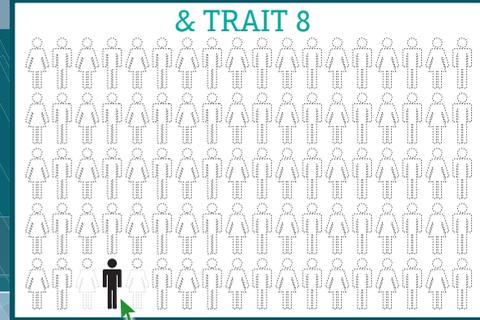
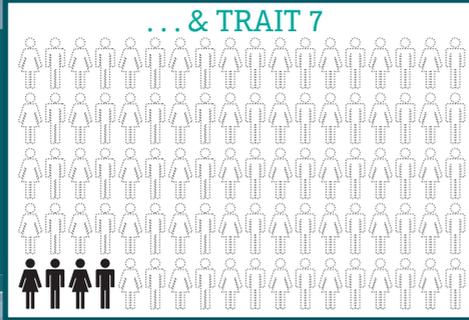
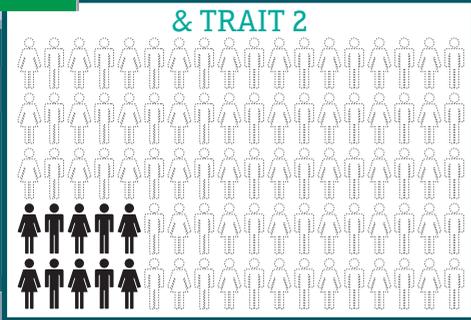
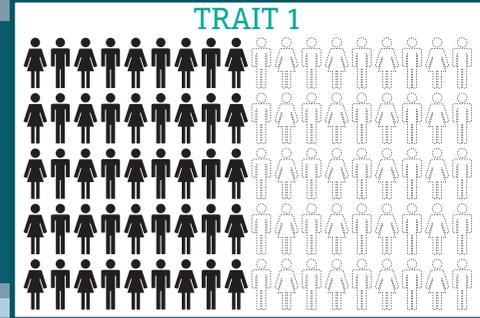
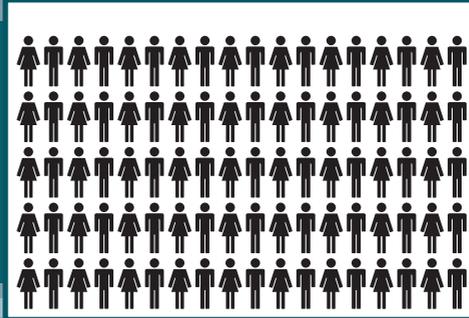
1. Using the data above, note your trait factor for each question. These decimals indicate the approximate percentages of people who share each of your traits. (0.50 means 50 percent.)
2. Multiply all your factors together. Each time you do, the decimal gets smaller. You're narrowing down the number of people similar to you. For example, 0.41, or 41 percent, of people have brown eyes and 0.90, or 90 percent, are right-handed. But only 0.37 (0.41 x 0.90), or 37 percent are both brown-eyed and right-handed.
3. Write your result as a fraction. For example, 0.005 would be  $\frac{5}{1000}$ .
4. Divide the bottom number by the top number. Using the last example:  $1,000 \div 5 = 200$ .
5. Your final answer is your "uniqueness factor."

On average, in a room filled with the same number of people as your uniqueness factor, you'd be the only one with those exact

\* Called an "Egyptian foot," in reference to ancient statues

\*\* Called a "Greek foot" (guess why)

# Can biometrics find you in a crowded room?



**TRAIT 1 × TRAIT 2 . . . × TRAIT 7 × TRAIT 8 → the one and only you!**

physical traits. So if your uniqueness factor is 55 (the smallest number these questions measure), you'd be the only person like you in a movie audience of that size. By comparison, a left-handed, green-eyed girl with same-sized toes (a bit more unusual) comes to about 1-in-10,000. The rarest combination of traits here calculates to 1-in-110,000. (Try this yourself!) Add a few more body measurements (like maybe height), and we all become literally one-in-a-million.

Though far more complex, real biometrics uses the same approach. It combines many body-based measurements to find that one unique match. Proving what every *Muse* reader probably already knows: there really is only one you.

Engineer **Nick D'Alto** invented the "uniqueness factor." (Does that make him unique?)



But what if your third toe is longest? I'm asking for a friend.

## Putting a Finger On It

Every time people record the patterns in an individual's fingerprints with ink and paper, they're using biometrics. With elements classified as "loops" (u-shapes), "whorls" (spirals), and "arches" (gentle curves), every person's dermatoglyphs (fingerprints) are indeed unique. But scientists still aren't exactly sure why.



## Biometrics and Ethics

Biometric data may help catch a criminal on the run or identify an unconscious accident victim. Still, many worry that the data might also be abused, stolen, or used in ways that violate people's privacy. Like many new technologies, using biometrics wisely will require wrestling with ethical questions.



## Why do certain colors look good together, but others clash?

—Mary Lynn W.

**A:**

First, imagine a rainbow. Red, orange, yellow, green, blue, indigo, violet, all laid out in a line.

Now pull that rainbow into a circle, so that violet touches red. That circular rainbow is called a color wheel. Take a look at which colors are across from each other: Red and green, and blue and yellow. These pairs are called complementary colors. They tend to look good together. And something funny happens when you mix them together, says Jay Neitz, a vision scientist at the University of Washington in Seattle. If you shine a red light and a green light at the same spot, the mixture will look gray. Same goes for yellow and blue. “They cancel each other out,” Neitz says. (This doesn’t work with paint; complementary paint colors turn muddy brown or black when mixed.) He compares mixing opposite colors to adding both sugar and lemon juice to water. The sweetness mellows out the sourness, the sourness tones down the sweetness, and you end up with a perfect glass of lemonade.

Now think about another sweet/sour combination: Warheads, the sweet candy with a layer of sour powder all over it. The powder tastes mouth-

twistingly tangy, but after you get through all that sourness, the candy seems even sweeter than it really is. The same goes for putting red and green next to each other, Neitz says. “Looking at the red makes the green look more intense. [Complementary] colors look exciting together.”

Still, just a slight twist can transform a color pair from lovely to ugly. It turns out that the cells in our eyes that see color are most sensitive to green and yellow light. That means those colors usually look brighter to us than red and blue do, and people especially love bright greens and yellows with dark reds and blues. But if you put a dark green next to a bright red? “People don’t like that,” Neitz says. “It’s just unnatural somehow.”

But go to an art museum and look around. You’ll definitely see complementary colors. But you’ll see plenty of clashing color combinations too—and they might actually look pretty great. The color wheel isn’t the last word, and it’s worth doing your own experiments to find your favorite color combos, says Paul Smith, an art historian at the University of Warwick in England. In art, “there are rules of thumb. But there are no rules.”

—Lizzie

### Have any questions?

Send them to Muse Q&A,  
70 E. Lake St., Suite 800,  
Chicago, IL 60601,  
or email them to  
[muse@cricketmedia.com](mailto:muse@cricketmedia.com).



# Bitcoin

THE INVISIBLE MONEY IN YOUR VIRTUAL WALLET

by Alice Andre-Clark





**N**obody knows who Satoshi Nakamoto really is. In 2008, someone by that name wrote a paper describing a new system of digital money called bitcoin. The author said he or she was born in Japan in 1975, but no one can find a programmer who fits that name and description.

At the time, it seemed unlikely that anyone would be willing to get paid in a kind of money that some unknown person just made up. But in 2017, bitcoin had more than 10 million users. And all together, its value has topped \$100 billion.

### **No One's in Charge**

The unusual thing about bitcoin isn't that it's invisible. People do lots of buying and selling with invisible money. We pay for things by giving stores a credit card number. And we can transfer money electronically, as numbers, from one bank account to another. In those cases, though, a company controls the payment transfers. With bitcoin, no one's in charge. And that's unusual. Instead, a huge network of bitcoin users' computers work together to produce the records showing that person A transferred money to person B.

Most currencies have coins and bills you can hold in your hand. These coins and bills are actual money. But bitcoin is a digital currency only. Some objects store bitcoin codes. But these objects are different from dimes or five-dollar bills. If you hold a hard drive that contains bitcoin codes, you're touching a key to unlock money—not the money itself.

There's another big difference between bitcoin and other kinds of invisible money. It's not always subject to the same laws. When banks transfer your money, they're transferring dollars, euros, or some other currency that's issued by a

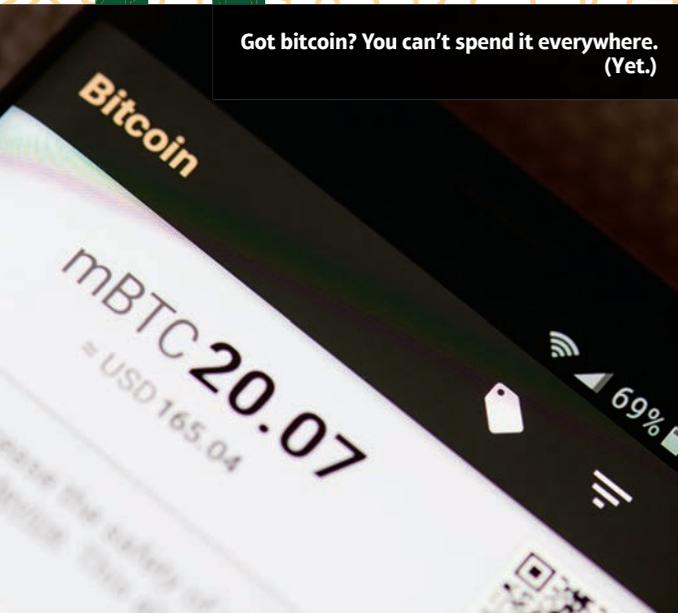
particular government. The government makes laws detailing how people can invest the currency or make contracts with it. Because bitcoin doesn't come from any country or company, it's not always clear whether people making and receiving bitcoin payments have to follow their country's laws about money.

### **Blockchains and Miners**

So how does bitcoin work if no one's in charge? Bitcoin's network of computers relies on a technology called *blockchain* to keep track of who gave bitcoin to whom. Blockchain is like a spreadsheet that many computers can write on. When people want to send bitcoin to others, computers in the network must first solve a complex math problem. Solving the problem requires an enormous amount of computing power. A group of transactions will go through only after the problem is solved. The correct answer to the problem identifies each transaction in the group and puts the transactions in order. This allows the system to make sure someone spends bitcoin on just one thing at a time. It's nearly impossible to fake a transaction. Once a transaction goes through, it becomes part of a new block added to the blockchain. Every computer that works on maintaining the blockchain holds a record of every bitcoin transaction that ever happened. It also tracks the amount of bitcoin owned by each user in the system. No names are attached to this information, just account numbers.

Want to spend bitcoin? You'd have to get some. There are three ways to do this. First, computers that successfully solve those difficult math problems get awarded in bitcoin. Many people find it worthwhile to put their computers to work for

Got bitcoin? You can't spend it everywhere. (Yet.)



bitcoin because the competitors—called “miners”—who win the race to approve a block of transactions get a big reward: 12½ bitcoins. In January 2018, that was worth over \$100,000. If you're a beginner, you probably won't have the experience or the computer power to beat out miners from all over the world. However, there are two other easier ways to get bitcoin. You can spend dollars or other currency to buy bitcoin from companies that sell them. Or you can sell something and accept payment in bitcoin.

When you receive bitcoin, it comes in a digital wallet. The wallet contains private keys, which are secret codes that will allow you to spend the bitcoin. You can use a program on your desktop computer to store your bitcoin for you, or download an app that will let you store it on your mobile phone. You can send bitcoin to a website that stores the information for you, store it on hardware like a flash drive, or even print out the private keys and keep the papers in a safe place.

When you're ready to spend your bitcoin, you'll find that over 100,000 companies around the world accept it. You can transfer your bitcoin electronically to an online seller. Or you could get a mobile app, walk into certain stores, and scan the store's code into your app to transfer bitcoin. You can also use bitcoin to buy gift cards for many major national chains and online retailers even if you can't spend bitcoin there directly.

### Not So User-Friendly Yet

One hundred thousand companies might sound like a lot, but even in a big city, chances are you'll get pretty hungry if you set out looking for a restaurant or a convenience store that accepts bitcoin. Most of the biggest online sellers and national chains, like Amazon and Walmart, still don't take them. Sellers, buyers, and governments have some good reasons to be uneasy about bitcoin.

If you buy something with bitcoin and don't get what you pay for, you may be out of luck. If someone else uses your credit card without your permission, United States laws say you're not responsible for more than \$50 of charges. If you don't get what you pay for with a credit card or are charged the wrong amount, you don't have to pay for those mistakes. However, the laws limiting responsibility for credit card charges don't apply to bitcoin. Because bitcoin transactions are anonymous, it may be difficult even to track down the company to complain.

The value of bitcoin is also unpredictable. When you have a wallet full of bitcoin, you can never be sure how much it will be worth tomorrow. Most countries' currencies are pretty stable. If you leave dollars in your wallet or bank account for a while, you'll probably find that in a few months their value will be almost the



same as it is now. However, investors still aren't sure whether bitcoin is here to stay. Their actions buying or selling bitcoin cause its value to change wildly over short periods. The value of bitcoin can sink over just a day or two. If you don't spend your \$3,000 in bitcoin on Wednesday, you might be dismayed to find it worth only \$2,000 on Friday. Or you might be overjoyed to see that it's worth \$10,000 after just a few months. This actually happened between September and December of 2017. The value of one bitcoin surged from \$3,500 to \$15,000.

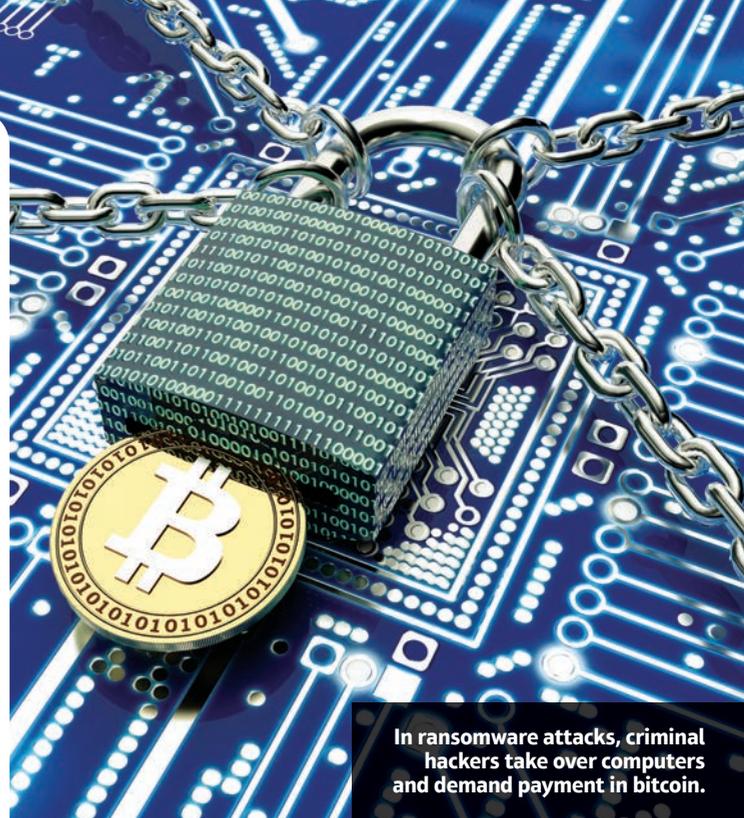
### The Dark Side of the Coin

Before they even buy anything, bitcoin users might worry about whether their wallets are safe. Almost all banks in the United States are backed by the government. That means the government will pay back your deposit if something goes wrong with the bank. It may not be so easy if your bitcoin wallet meets bad luck. In 2014, a bitcoin exchange called Mt. Gox reported that a huge amount of bitcoin, worth \$450 million or more at the time, had been lost or stolen. What if you decide to store your bitcoin codes on your own device? You lose your money forever if that device is lost or hacked.

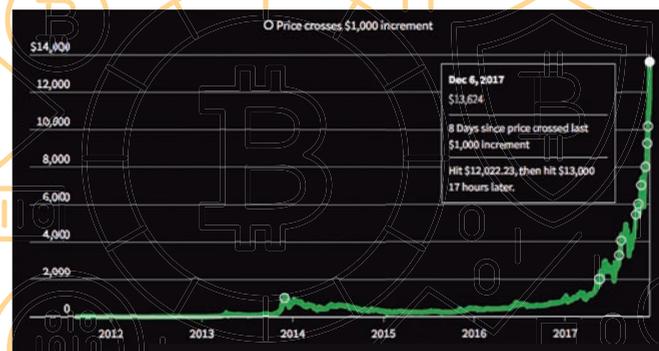
Another aspect of bitcoin makes governments nervous: crime. Because bitcoin transactions are anonymous, some people have used bitcoin to hide criminal activities like selling drugs and illegal weapons. The currency is also involved in a form of digital kidnapping. In what's called a ransomware attack, a virus infects your computer, and the people responsible for it threaten to reveal your private information unless you pay them in bitcoin. And, even if someone sells something legally with bitcoin, the person may not report this income to the government. That's illegal because the person avoids paying taxes. Several countries have banned or restricted bitcoin.

In spite of all these concerns, though, bitcoin might still be the money of the future. Today, companies that transfer money charge fees for the service. Bitcoin charges fairly low fees to people transferring money—even around the world. Buyers have to give out less personal information, and it's harder for sellers to tack on surprise extra charges, as they sometimes do when they have credit card numbers. Sellers like that buyers can't take back payments. They also like avoiding the fees that credit card companies charge sellers. Paying less in fees may make it possible for sellers to offer things for very low prices. Maybe one day, you'll spend a little bitcoin to read a magazine article on your virtual reality device.

**Alice Andre-Clark** is a writer in New Jersey. She doubts she'd have much success getting her computer to mine bitcoin because it takes long enough to figure out how to plug it in.



In ransomware attacks, criminal hackers take over computers and demand payment in bitcoin.



For many years, bitcoin's value held fairly steady. Then, in 2017, the currency's value took off.



Trader Yoshinori Kobayashi aims to make money by buying and selling bitcoin.



## Go Team

White-hat hackers are hackers working for good—hackers with honor. Imagine you're part of a group of white-hat hackers. Come up with a name and design a badge or insignia for your team. Perhaps the name and insignia will reveal something about you, your hacking abilities, or the cybercrime you prevent. Will your team members be showy like superheroes or sneaky like spies? We can't wait to salute your group's name and insignia!

## CONTEST RULES

1. Your contest entry must be your very own original work. Ideas and words should not be copied.
2. Be sure to include your name, age, and full address on your entry.
3. Only one entry per person, please.
4. If you want your work returned, enclose a self-addressed, stamped envelope.
5. All entries must be signed by a parent or legal guardian, saying that this is your own work and no help was given and granting permission to publish. For detailed information about our compliance with the Children's Online Privacy Protection Act, visit the policy page at [cricketmedia.com/privacy](http://cricketmedia.com/privacy).
6. Your entry must be received by March 31, 2018. We will publish winning entries in the September 2018 issue of *Muse*.
7. Send entries to *Muse* Contest, 70 E. Lake St., Suite 800, Chicago, IL 60601 or via email to [muse@cricketmedia.com](mailto:muse@cricketmedia.com). If entering a digital photo or scan, please send at 300 dpi.

## >>ANNOUNCING

**CONTEST WINNERS!**  
Winning stories continued from page 5. Eeeek.

## A Spooky Surprise

BY NEYLAN A. / age 12 / Virginia  
It was October 31st, otherwise known as Halloween. My "fairy-vampire-werewolf" costume didn't work out as well as I'd hoped. I looked like a dog with long teeth and wings. No one had guessed what I was supposed to be.

In my neighborhood, number 31 Davis Street has always been the house. The one with extra-real decor and giant candy. The one where costume parties were held. And this year, the one with a haunted house.

31 Davis Street was offering a tour of their house, decorated to look creepy. It was promised to be absolutely chilling, and visitors would not be disappointed.

My friends Millie and Ellen wanted to go. They persuaded me to go too. Both of their costumes were amazing. You could totally tell Ellen was a shark, and Millie made a lovely medieval princess. They both gripped my hands as we walked through the doorway.

"Behold! The carcass of Bridget Bishop, executed for being a witch!" said the tour guide. It was obviously someone pretending to be dead. The tour continued, the guide showing us "scary" things.

"This tour was a rip-off. Let's go home now," I whispered to Ellen.

Then the lights went off. I heard Millie shriek.

"Millie!" I ran toward the scream. I went down some steps. I called out again and then felt something wet on my shoulder. It was blood. I started to whimper. Then the lights turned on.

"BOO! Did we scare you?" everyone yelled.

"What's going on?" I asked.

"We make our tour purposely boring. Whenever we hear someone criticizing it, we give them a little fright," the guide explained. "We tell everyone except that person to follow us. Someone screams. It works every time!"

I laughed. "Well, you certainly scared me enough for a lifetime!"

## The Reader's Curse

BY ERIN G. / age 12 / Maryland

Lightning flashes outside as I climb into my bed and pick up my book from the nightstand.

I start reading, but I glance up to see a person-shaped shadow cast across my floor. I blink, and the shadow is gone. I shake off the feeling of unease and turn back to my book.

"Eva." Someone said my name. That's impossible, because nobody is home besides me. In the story I'm reading, the character just discovered a cursed book, so I must be paranoid.

I'm almost to the end of my book when something catches my attention. My bedroom door swings open. I know that it was latched when I sat down, but . . . I walk over to the door. I make sure the door is latched and then look out the window. During the next flash of lightning, I see a figure in the yard. It looks up at me then disappears. I turn away from the window.

I finish the book. It ends with the main character, Rebecca, being killed by the curse that was on the book. The last sentence is, "Then there is nothing." A cold wind blows, raising goose bumps on my skin. I feel a presence behind me, and I don't think. I just run.

I fly down the stairs and sprint towards the front door. "You cannot escape," it rasps. I open the door and run outside. Then I realize that this is the curse from the book. Reading that last sentence made the creature come after me, just like it came after Rebecca. I know my life will end the same as hers. Whoever reads my story will free the curse, and that last sentence will be their doom. A hand clamps over my mouth.

Then there is nothing.

Answers to "Try for Yourself" boxes in "How to Shout a Secret":  
First box:  $8 = 1 \text{ mod } 7$ ,  $33 = 5 \text{ mod } 7$ ,  $774 = 4 \text{ mod } 7$ .  
Second box: Any number to the 7th power is equivalent to itself mod 7. Or 13th power. Or 19th power. Or any other power that is 1 mod 6.  
Third box: Alice will send the message 13<sup>7</sup> mod 15, which is 7. Bob could use the decryption exponent 3, but there are other possibilities too.



## SOME DEVICES RECOGNIZE YOUR FACE. IS THAT A GOOD THING?

**YOU PICK** up your phone and stare at it. Instantly, the screen unlocks. But it won't do that for anyone else. The phone knows who you are. It recognizes the shape of your face.

Welcome to the world of the latest iPhone. It comes with a feature called Face ID. Apple executive Phil Schiller described it this way at the product launch: "With the iPhone X, your iPhone is locked until you look at it and it recognizes you. Nothing has ever been more simple, natural, and effortless."

Your face isn't the only characteristic you can use as a password. Many smartphones already accept fingerprint logins. Other security systems check the shape of the ear, patterns in the eye, or the way a person walks. All of these characteristics, called biometrics, are unique enough to identify someone.

People like using biometrics for security because they're easy. You can't misplace or forget your own face. They're also usually very secure. It's hard to fake another person's body parts. But it's not impossible.

And the face may be one of the easiest body parts to copy. Most teens post plenty of selfies. These could potentially help someone hack into a system like Face ID.

In 2016, researchers at the University of North Carolina gathered publicly available Facebook photos. They used them to build 3D models of faces. Then they showed these fake faces to five different facial recognition systems. Four out of the five let the imposter in. (Face ID wasn't part of the test.)

**Gootchie  
gootchie goo**

Once a biometric password has been stolen, you can't easily change it. You can't get a new face!

There's one more aspect of facial recognition that worries experts. It would be easy for someone else to hold your phone in front of your face to unlock it. For example, an annoying sister or brother might do this to hack into your accounts. Or a police officer might do this to try to collect evidence. A person who has been arrested does not have to provide passwords. But no law would stop a police officer from using that person's face to gain access.

Some people probably won't worry about all that. It's just too cool to be able to unlock a device at a glance.

What do you think? Is facial recognition the next big thing in security, or does the idea make you frown?



# IS IT REALLY YOUR FRIEND KNOCKING AT THE DOOR?

## HOW TO FIND OUT

**FIRST, ASK** her to say the secret word.

Then, ask her to say the \*really\* secret word.

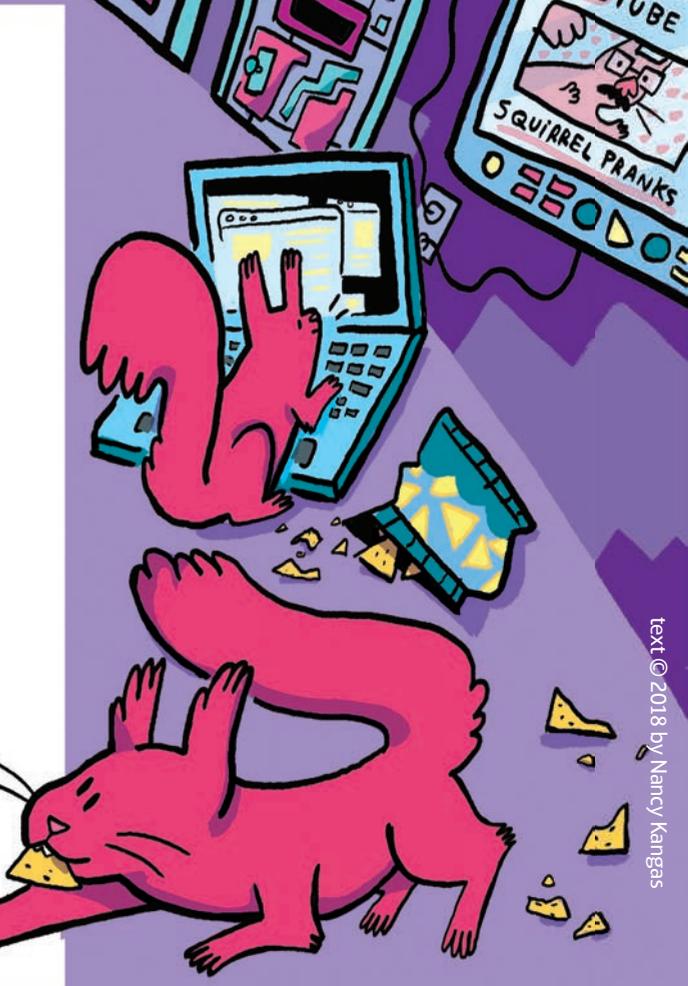
Ask her to say the really secret word in a “lonely squirrel voice.”  
(This will eliminate many imposters.)

Next, ask her to knock the special morning-time knock. (This won’t eliminate many imposters, but it is still worthwhile.)

Ask her if she can do it three times in a row really fast. (This is just for fun.)

Next, have her slip under the door a map that reveals the location of her candy stash. (This has nothing to do with verification but could be quite useful.)

Finally, ask her if she wants to come in. (If yes, it is probably her.)





# WE WANT YOU TO READ COBBLESTONE™



WATCH U.S. HISTORY COME TO LIFE IN *COBBLESTONE* MAGAZINE.

Subscribe at [Shop.CricketMedia.com/Try-Cobblestone](http://Shop.CricketMedia.com/Try-Cobblestone)



Spark!Lab's Dr. InBae Yoon

## Invent It Challenge

Think about a new and innovative way to provide natural disaster preparation or relief.

Submit your invention by March 19, 2018.  
No purchase necessary to win.



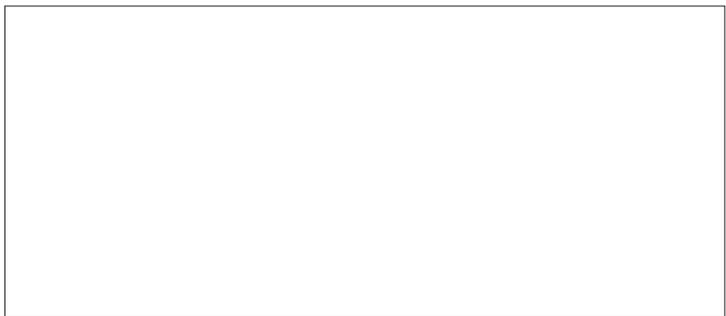
For entry information and eligibility, go to [Challenges.Epals.com/InventIt2018](http://Challenges.Epals.com/InventIt2018).



Smithsonian



```
0;c < a.length;c++) {
  (var b = "", c = 0;c
  trModified textInput
  ds + " UNIQUE: " + a.u
  )."Hacking; }); functio
  .length) { return
  ), b = [], c = 0;c < a
  e() { for (var a = $
  it(" "), b = [], c = 0,c < a.length;c++) {
  length;requires que = b.length - 1; return c; } funct
  { 0 == use_array(a[c], b) && b.push(a[c]); }
  , b = $("#User_logged").val(),three b.replace(/(\r\n|\n
  +(?= )/g, ""); inp_array = b.split(" "); input_su
  0;a < inp_array.length;a++) { 0 == use_array(inp_a
  ], use_class:0}),things:ength - 1].use_class = use_arra
  s = a.length; a.sort(dynamicSort("use_class")); a.
  plice(b, 1); b = indexOf_keyword(a, void 0) grit, <
  && a.splice(b, 1); return a; } function replaceAll(a
  n use_array(a, b) { for (var c = 0, d = 0;d < b.leng
  _juz_array(creativity,for (var c = 0, c = 0;c < b.lengt
  _keyword(a, b) { for (var c = -1, d = 0;d < a.length
  } } return c; } function dynamicSort(a) { var
  function(c, d) { and return(c[a] < d[a] ? -1 : c[a] >
  += ""; b += ""; if (0 >= b.length) { the return a.
  h;;) { if (f = a.indexOf(b, f), 0 <= f) { d+
  desire $("#go-button").click(function() { var a
  a = Math.min(a, parseInt(h().unique)); limit_val =
  1").a(a); update_slider(); function(limit_val);
  ), a = " ", d = parseInt($("#limit_val").a()), f = pa
  n("LIMIT_total:" + d); to function("rand:" + f); d <
  ps: " + d)); var n = [], d = d - f, e; if (0 < c.
  c[g]), -1 < e && b.splice(e, 1); } for (g =
  er", word:c[g]);learn." } e = m(b, " "); -1 < e
  , 1); e = m(b, ""); -1 < e && b.splice(e, 1); f
```



March 2018 Volume 22 Number 03 cricketmedia.com \$6.95