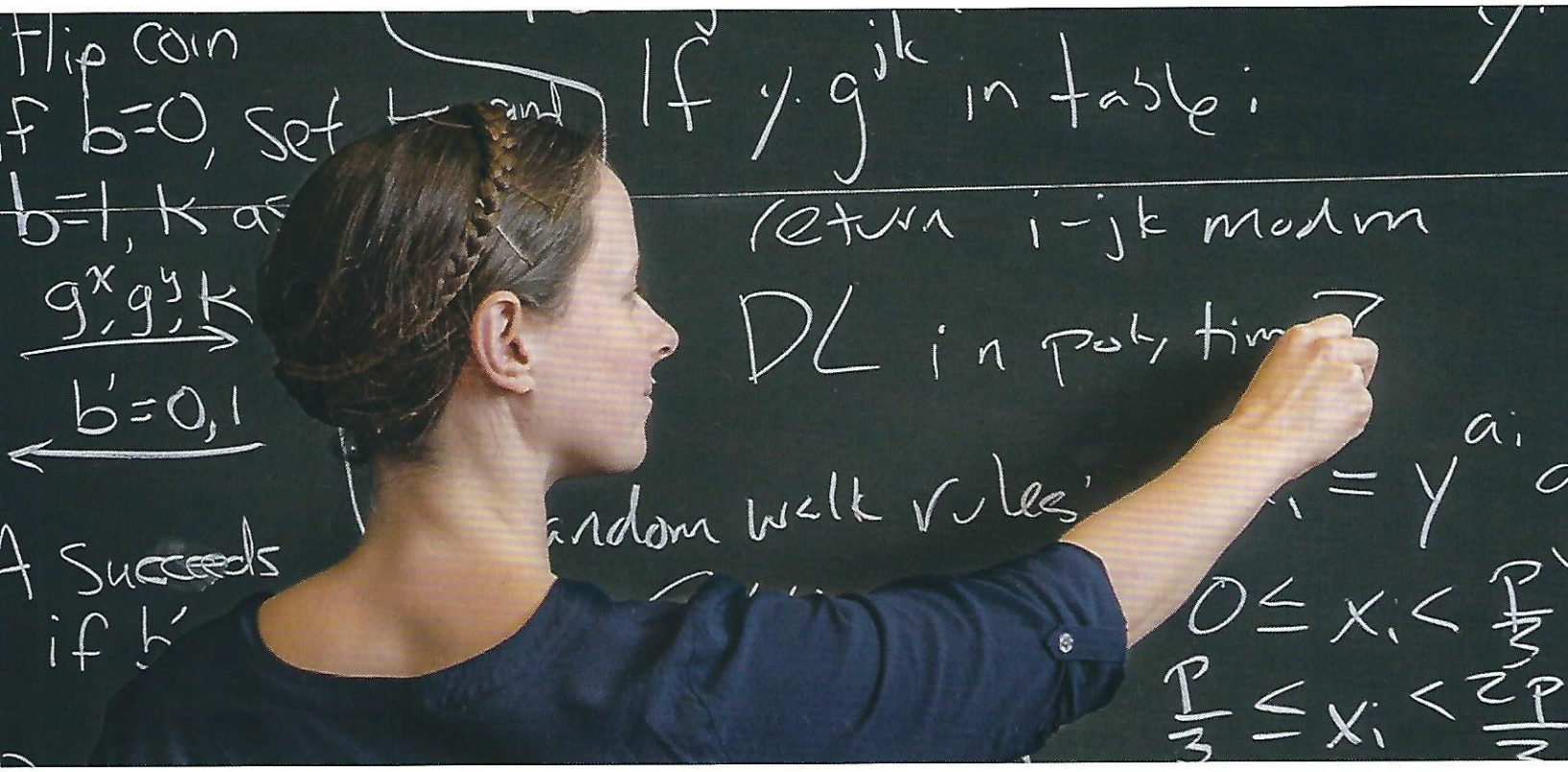


Feats to Fortify Internet Security

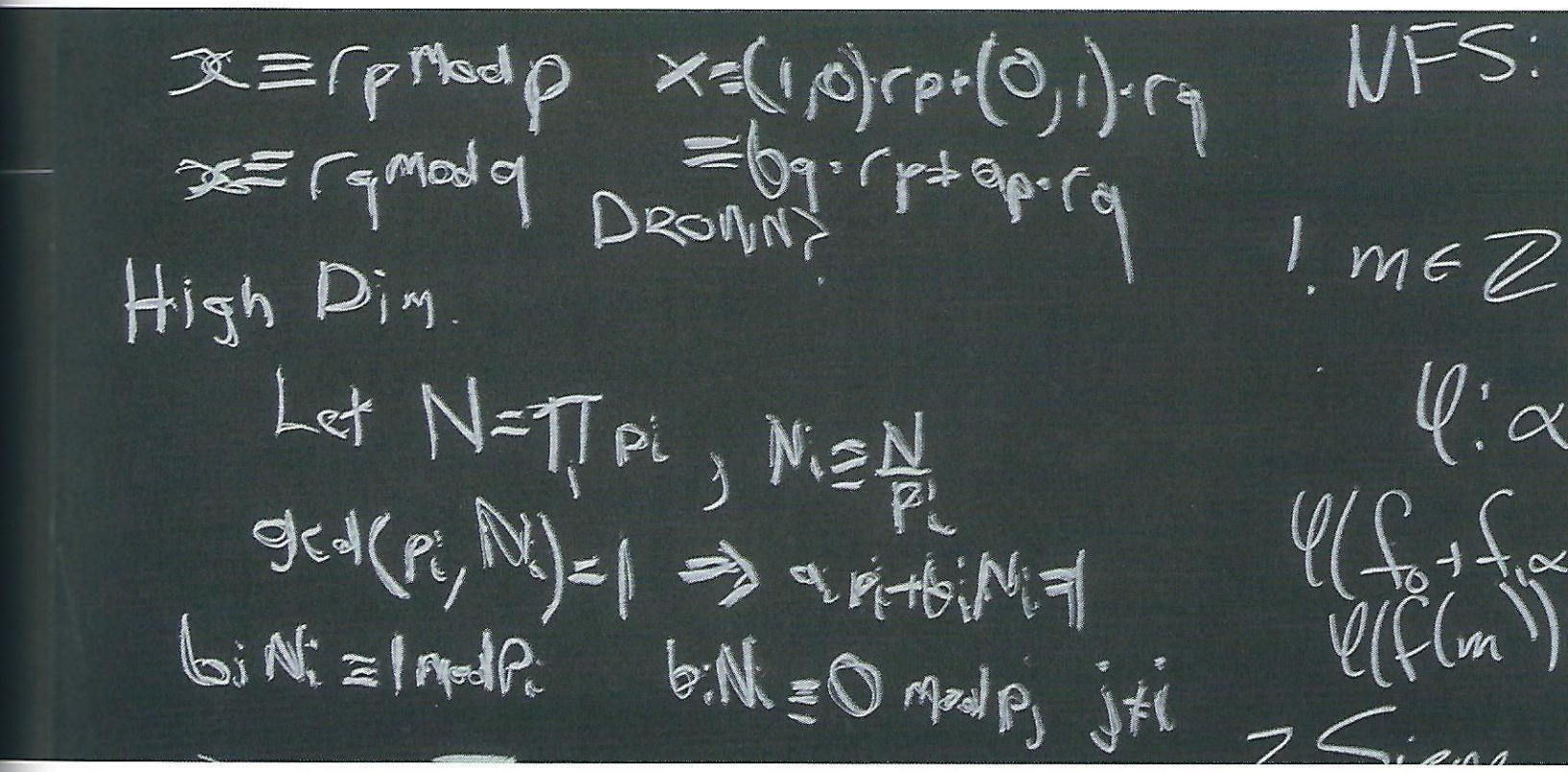
Virtual barricades that keep the world safe from cyber thieves, terrorists, malicious hackers and nefarious actors are reinforced with extremely complex mathematical and computing algorithms. As an influential scholar in the crucial practice and theory of computer security, Nadia Heninger finds consequential digital vulnerabilities, and devises and shares solutions before harm ensues.

"I've made my career in finding subtle cryptographic flaws that turn out to compromise a large number of systems," says Heninger, Magerman Term Assistant Professor in the Department of Computer and Information Science (CIS). She works to make systems more secure by understanding how they fail, generating insights that have prevented grievous losses of data, privacy and security.

HOUSE OF CARDS

"Nadia has helped to discover some of the most interesting and impactful threats to security that affect businesses and individual privacy worldwide," notes J. Alex Halderman, director of the Center for Computer Security and Society at the University of Michigan, and a frequent research collaborator. "She is one of the best people currently bridging the areas of theory and systems in the field of computer security, and she has achieved seemingly magical results in breaking cryptography, combining an excellent level of mathematical depth with a passion for real-world problems that affect the security of millions of people."

Ethical dedication to the public good informs the deft timing with which she works to share her crypto-sleuthing discoveries. "The security of real-world systems can seem like a fortress with a security system described as 'military grade cryptography certified by agencies following best practices,'" says Heninger. "If you think from the perspective of an attacker, it's a house of cards."



Nadia Heninger, Magerman Term Assistant Professor in Computer and Information Science, considers some of the mathematical ideas underlying the security of public-key encryption, which is used to securely transmit information across the internet.

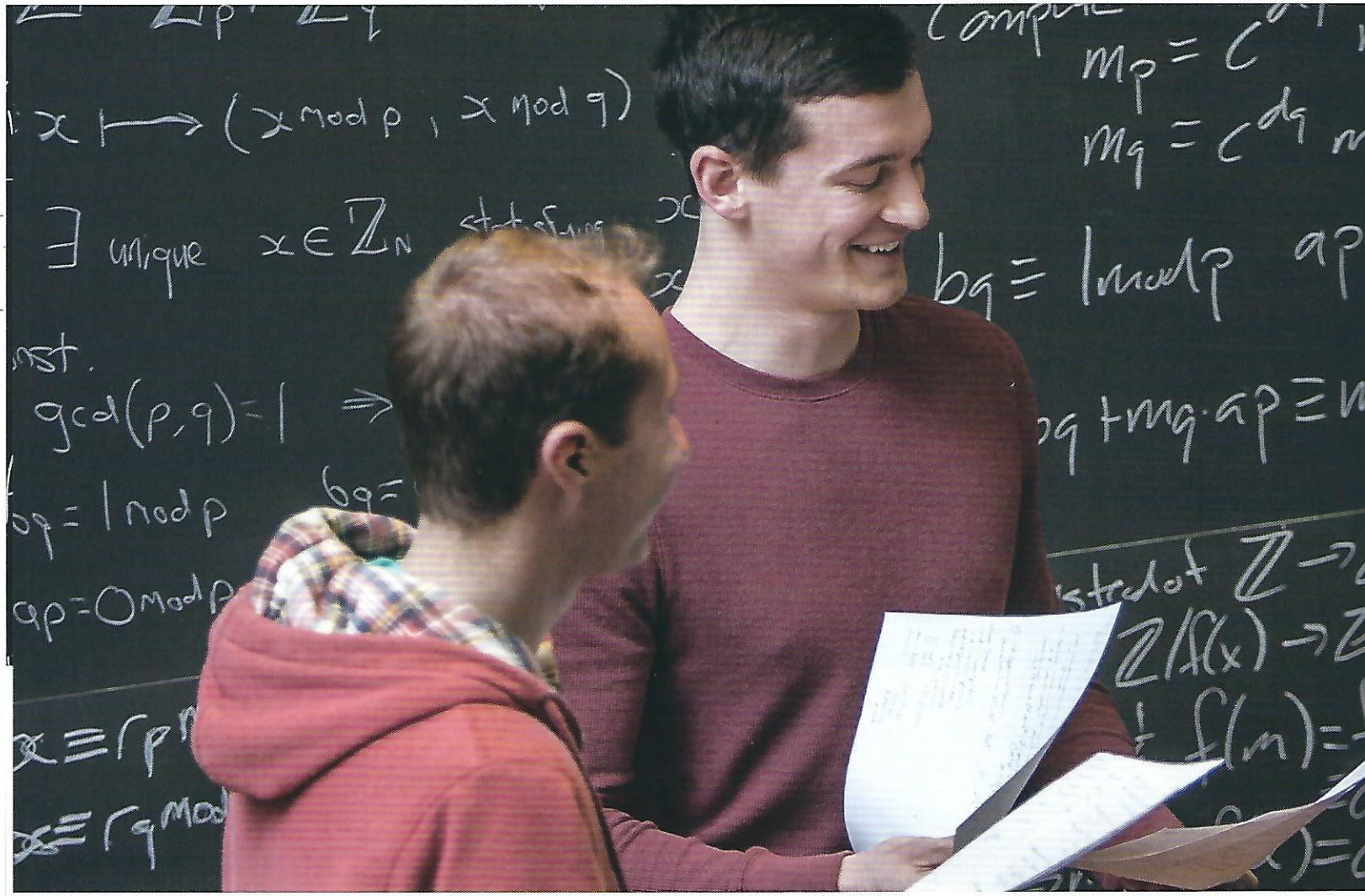
Heninger not only trains her graduate students to spot security vulnerabilities, but also to effectively disclose them so that affected companies and governments can make needed repairs before discoveries are published and flaws are used maliciously. "With all of my recent work, companies have been very responsive and have put out patches and the like," she says.

HENINGER FINDS CONSEQUENTIAL DIGITAL VULNERABILITIES, AND DEVISES AND SHARES SOLUTIONS BEFORE HARM ENSUES.

OBSOLETE ENCRYPTION

In March 2016, Heninger and collaborators disclosed a serious vulnerability in 33 percent of websites that use HTTPS, the cryptography that secures the web. While there was no evidence the flaw had been exploited, it would have allowed attackers to break encryption and steal or read sensitive communications, including passwords, credit card numbers, trade secrets or financial data. This vulnerability was an example of the potential for catastrophic security failures caused by government policies from the '90s that weakened cryptography, according to drownattack.com, created by Heninger and her coauthors. They did not release the attack code (executable in under a minute with a personal computer), and instead shared detailed instructions to protect against this vulnerability.

Another recent example of her clout: Heninger's 2015 paper, *Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice,* noted a critical security flaw in eight percent of the top one million websites. On servers supporting obsolete government encryption parameters—designed to allow backdoor surveillance—communications



can be accessed by an attacker using today's more powerful computers. Before that paper appeared in the *Proceedings of the ACM Conference on Computer and Communications Security,* she and her coauthors disclosed the vulnerability to all major web browser companies, which rapidly deployed suggested repairs.

An urgent round of sleuthing began in mid-December 2015 when Juniper Networks cryptically announced that its network devices, used for firewalls and virtual private networks by a high proportion of global businesses, had been compromised with unauthorized, secretly embedded code. Heninger's lab joined ten other researchers in a collaborative race to analyze the implications. "If a significant portion of Juniper systems are vulnerable, that means much of the world's internet network traffic is also vulnerable," says Shaanan Cohney, a second-year doctoral student in Heninger's lab. He noted (in February), "We're still trying to understand how this vulnerability works, when it happened, who is responsible and what else is vulnerable."

HENINGER AND COLLABORATORS DISCLOSED A SERIOUS VULNERABILITY IN 33 PERCENT OF WEBSITES THAT USE HTTPS.

In January, a U.S. congressional committee began investigating claims that subtle flaws in Juniper's technology had been introduced via National Security Agency specifications that created a digital backdoor (for government access). "While our current work focuses on technical topics, not politics, we strongly posit that the use of digital backdoors is dangerous because the U.S. government can't control who will use these," Cohney says.

Heninger and second-year doctoral students Shaanan Cohney (left) and Luke Valenta (center) discuss a new result on mathematical lattices in cryptography.

"We're having a national and international discussion on what the limits of government surveillance should be," adds Heninger. "There's an ethical level to that discussion, a philosophical, political and technical level. My work addresses the technical level. The 'security and privacy trade-off' is language used by politicians and law enforcement—that you can either have privacy or be secure. But that's not how the internet functions. Being able to use cryptography to keep data away from hackers is critical to our security."

CODE-BREAKING HOMEWORK

Heninger joined Penn's faculty in 2013, and appreciates the presence of colleagues in related security, theory, data science and public policy fields. She especially enjoys teaching. "It's fun. You're constantly reevaluating what you're doing and teaching."

Students who take her undergraduate class, CIS 331: Introduction to Networks and Security, often enroll next in CIS 556: Cryptography, a graduate-level course for which she devised a clever way to assess readiness: students must design programs to attack and decrypt each of their six homework problem sets. "Successful students really like this challenge," says Luke Valenta, a second-year doctoral student and teaching assistant. "Hours and sometimes days of struggle with a problem ingrain the concepts in your mind so you actually remember them later on."

Cohney adds, "What makes Dr. Heninger special is her concern for the development of her doctoral students, not just as excellent researchers, but as moral individuals who can analyze their work through the lens of public good and policy."

By Jessica Stein Diamond