Daniel J. Bernstein

Date of birth: October 29, 1971
Occupation: Cryptologist and mathematician

Alexander Klink via Wikimedia Commons

In 1992, mathematics graduate student Daniel J. Bernstein encountered a roadblock he had not expected. A talented programmer deeply interested in cryptography and cryptology, Bernstein had developed an encryption algorithm that he named Snuffle, as well as a research paper on his program. Hoping to avoid any legal complications, he contacted the US State Department to confirm whether he would be legally able to post the source code to his work and the research paper online. The government responded that under the International Traffic in Arms Regulations (ITAR), the code for encryption tools were considered munitions, and Bernstein would have to register as an arms dealer and obtain an export license to post his work on the internationally accessible Internet. After several years of further communications with the US government, Bernstein ultimately filed a lawsuit in 1995 with the goal of changing the federal policy on encryption programs. "Cryptography is a powerful crime-fighting tool," he

explained to Peter Cassidy for *Wired* (1 June 1996). "This is not a case of needing more laws. This is a case of needing more technology." After a lengthy legal battle, the US Ninth Circuit Court of Appeals ruled the US government's regulation of encryption software unconstitutional, determining that work such as Bernstein's qualified as speech and was thus protected by the First Amendment to the US Constitution.

In addition to his court case, Bernstein became widely known as a major researcher and programmer in the field of cryptography. Having completed his doctorate in 1995, he went on to begin a long career with the University of Illinois at Chicago, where he became a full professor in 2005. He was also affiliated for a time with the Netherlands' Eindhoven University of Technology (Technische Universiteit Eindhoven), where he began a part-time professorship in 2012. The author of numerous research papers and an editor of the 2009 book *Post-Quantum Cryptography*, Bernstein is also known for creating qmail, djbdns, and a variety of other tools designed to improve internet security for their users.

EARLY LIFE AND EDUCATION

Daniel Julius Bernstein was born on October 29, 1971, in East Patchogue, New York. He attended Bellport High School, a public school serving East Patchogue and other towns in Long Island's Suffolk County. Bernstein performed well academically in high school, graduating early in 1987. Following graduation, he attended New York University, graduating in 1991 with a bachelor's degree in mathematics. He went on to pursue graduate studies in the Department of Mathematics at the University of California, Berkeley. There, he completed research into computational number theory under Dutch mathematician Hendrik Lenstra, and finished his dissertation, titled "Detecting Perfect Powers in Essentially Linear Time, and Other Studies in Computational Number Theory," in 1995. While still a graduate student, he began his career as a consultant and also worked on his own programming projects, most notably the encryption algorithm Snuffle.

ACADEMIC CAREER

After completing his PhD, Bernstein accepted the position of research assistant professor at the University of Illinois at Chicago, joining the university's Department of Mathematics, Statistics, and Computer Science in the College of Liberal Arts and Sciences. He was promoted to assistant professor in 1998, associate professor in 2001, and full professor in 2005. In 2003, Bernstein also began teaching in the Department of Computer Science in the College of Engineering, moving there permanently in 2008 when he was made a research professor. Beginning in 2012, he held a part-time professorship at the Technische Universiteit Eindhoven in the Netherlands.

In addition to his primary academic positions, Bernstein served as a visiting scholar at the University of Sydney in 2004 and visiting professor at the Danmarks Tekniske Universitet (Technical University of Denmark) in 2006. The year 2006 also saw him serve as senior scientific researcher in the Thematic Pro-

gram on Cryptography at Canada's Fields Institute. Alongside his teaching positions, Bernstein served as principal investigator for National Science Foundation (NSF) on projects dealing with topics such as number theory and cryptography, as well as projects funded by the Cisco University Research Program and the National Institute of Standards and Technology (NIST), among others. Between 2002 and 2006, he was a research fellow of the Alfred P. Sloan Foundation. Bernstein at times struggled with what he described as issues of mismanagement regarding the grant funding he received, many of which he documented on his personal website.

BERNSTEIN V. US DEPARTMENT OF JUSTICE

While a graduate student at Berkeley, Bernstein wrote an encryption program that he called Snuffle, which made use of the mathematical concept known as hash functions. Seeking to publish the code for his program and a set of instructions online and receive feedback from other members of the cryptography community, he contacted the US State Department in 1992 to determine whether he would be allowed to do so. Based on regulations such as ITAR, however, the US government informed Bernstein that the code for his encryption program was considered a form of munition. To publish his work online, where it might be accessed by individuals living outside of the United States, he would need to register as an arms dealer and apply for an export license. The government also indicated that he would be unable to obtain a license due to the nature of his program.

For Bernstein, the US government's policy of treating source code as munitions seemed counterintuitive. "What gets me worked up here is plain old crime," he told Cassidy. "I still remember the first computer intruder I ran into. How disgusted I was at finding out that he had been rifling through my files; how much time I spent trying to figure out if he had destroyed anything. In the years since, I've spent a lot of time thinking about how to stop these criminals. By now, I feel I can really help people protect themselves, but the State Department says I can't share my advice. That's totally disgusting." Believing that the government's policy violated his First Amendment right to freedom of speech, Bernstein partnered with the Electronic Frontier Foundation to sue the US government over the issue in 1995. In the ensuing court case, *Bernstein v. US Department of Justice*, Judge Marilyn Hall Patel ruled that software source code could be considered speech and that the government's attempts to block Bernstein from sharing his work online were unconstitutional. The Ninth Circuit Court of Appeals upheld that ruling in 1999, and Bernstein continued to challenge the federal government's stance on encryption programs over the subsequent years.

QMAIL

A skilled programmer as well as a researcher and teacher, Bernstein became known for a number of key projects, the results of which he made freely available online. One of the most significant of those was qmail, a mail transfer agent (MTA) that he began to work on in the mid-1990s after identifying issues in the

security of popular MTAs used by internet service providers (ISPs) during that period. An MTA is a type of software that transmits email from the sender's computer to the recipient's computer. Security holes in popular MTAs such as Sendmail particularly concerned Bernstein, as they made computers vulnerable to malicious attacks.

Bernstein's work on qmail began in earnest late in 1995. "I had just finished teaching a course on algebraic number theory and found myself with some spare time," he wrote in his paper "Some Thoughts on Security after Ten Years of qmail 1.0" (2007), which summarized the history of the project. "The final kick to get something done was a promise I had made to a colleague: namely, that I would run a large mailing list for him." Bernstein began a beta test for qmail in January of 1996 and released qmail 1.00 in February of the following year. The program's June 1998 release, qmail 1.03, remained the definitive version for the next decade. Bernstein's new MTA proved popular among users and multiple large companies during the years following its release, among them Yahoo! and the ISP NetZero. Confident in his creation's high level of security, Bernstein offered a $500 reward to the first person to find and document a security hole in his program. He increased the reward to $1,000 in 2007 after no security holes were found.

"Most 'security' efforts are designed to stop yesterday's attacks but fail completely to stop tomorrow's attacks and are of no use in building invulnerable software."

DJBDNS

Bernstein also received extensive attention for his work on djbdns, a group of software elements designed to be a more secure alternative to the prevailing Domain Name System (DNS) servers. As was the case with qmail, the software was created in response to security vulnerabilities within popular options available to internet users. Bernstein also reportedly objected to the manner in which DNS server software such as BIND was written. By 1999, he began writing his own alternative, djbdns, which he released in an alpha version late that year. Another incarnation of the software, djbdns 1.05, was released in early 2001. Bernstein later placed his software in the public domain to encourage the free use and distribution of his work.

As with qmail, Bernstein announced that he would pay a reward to the first person to find a vulnerability in his djbdns. In 2009, an information security professional named Matthew Dempsky successfully identified and patched the first known security hole in djbdns. In response to that discovery, Bernstein acknowledged the bug and agreed to pay the promised reward. "Even though this bug affects very few users, it is a violation of the expected security policy in a reasonable situation, so it is a security hole in djbdns," he wrote to the djbdns mailing list, as reported by Ryan Naraine for *ZDNet* (6 Mar. 2009). "Third-party

DNS service is discouraged in the djbdns documentation but is nevertheless supported. Dempsky is hereby awarded $1000."

OTHER WORK

Over the course of his career, Bernstein established himself as an expert in internet security and a major figure in cryptography and related fields. In addition to qmail and djbdns, he created a variety of other security-related tools, including daemontools, programs used to manage services with the UNIX operating system, and the Salsa20 and ChaCha families of ciphers, used for encrypting data. For Bernstein, the need to continually innovate in security and encryption remains constant due to both the increasingly connected nature of the world and invasions of personal privacy by both governments and corporations. "My views of security have become increasingly ruthless over the years," he explained in "Some Thoughts on Security." "I see a huge amount of money and effort being invested in security, and I have become convinced that most of that money and effort is being wasted. Most 'security' efforts are designed to stop yesterday's attacks but fail completely to stop tomorrow's attacks and are of no use in building invulnerable software. These efforts are a distraction from work that *does* have long-term value."

Alongside his teaching and programming work, Bernstein is a prolific public speaker and delivered more than 450 lectures between 1987 and 2019. Although his interests are wide ranging, he focused particularly on post-quantum cryptography during the second decade of the twenty-first century. The term *post-quantum cryptography* refers to forms of cryptography designed to withstand attacks by a quantum computer, a proposed computer that many cryptography experts believe would be able to break some of the encryption algorithms in common use on the twenty-first-century Internet. In addition to delivering numerous talks on the subject, Bernstein edited the 2009 book *Post-Quantum Cryptography* with fellow cryptography experts Johannes Buchmann and Erik Dahmen. Bernstein has published widely in major journals, in the proceedings of numerous conferences, and on his own website. A proponent of making research papers available to a wide audience, including individuals without access to costly print journals and databases, Bernstein typically posts copies of his papers online and urges other researchers to avoid publishing with journals or publishers that prohibit researchers from doing so.

SUGGESTED READING

Bernstein, Daniel J. *D. J. Bernstein*, cr.yp.to/djb.html. Accessed 18 Jan. 2019.

Bernstein, Daniel J. "Some Thoughts on Security after Ten Years of Qmail 1.0." *cr.yp.to*, 2007, cr.yp.to/qmail/qmailsec-20071101.pdf. Accessed 18 Jan. 2019.

"Bernstein v. United States Department of Justice." *FindLaw*, 6 May 1999, caselaw.findlaw.com/us-9th-circuit/1317290.html. Accessed 18 Jan. 2019.

Cassidy, Peter. "Reluctant Hero." *Wired*, 1 June 1996, www.wired.com/1996/06/esbernstein. Accessed 18 Jan. 2019.