On Thursday, December 5, 2019, AMS President Jill Pipher spoke to congressional representatives and told her attentive audience about the long history—from Caesar to present—of cybersecurity, the deep theoretical mathematics involved, and the state-of-play regarding both the potential and perils of quantum computing.

After a quick tour of the older history, Pipher turned to describing her own work. In the 1990s, Pipher and her colleagues Jeffrey Hoffstein and Joseph Silverman developed the NTRUEncrypt cryptosystem ([https://bit.ly/2YRy4CH](https://bit.ly/2YRy4CH)). NTRUEncrypt (US Patent # 6,081,597, issued in 2000) is similar in philosophy to other cryptosystems—more familiar to many of us—that rely on factoring large numbers in that it involves a very difficult task of undoing something (factoring) that is very easy to do (multiplying). This system is based on lattices. In the lattice context, the difficult task is related to the shortest and closest vector problems. They describe lattice-based cryptography in chapter 7 of their undergraduate text *An Introduction to Mathematical Cryptography* (Springer, 2nd ed., 2014).

Lattice-based systems appear to be resistant to quantum computer attacks. The government is very concerned about threats to our security in the age of quantum computing. For example, the National Institute of Standards and Technology (NIST) is in the process of selecting one or more public-key cryptographic algorithms through a public competition-like process ([https://bit.ly/2EjbGZ8](https://bit.ly/2EjbGZ8)). It is intended that these algorithms will be capable of protecting sensitive information well into the foreseeable future.

Karen Saxe is an associate executive director of the AMS and the director of the Office of Government Relations. Her email address is kxs@ams.org. For permission to reprint this article, please contact: reprint-permission@ams.org. DOI: [https://dx.doi.org/10.1090/noti2061](https://dx.doi.org/10.1090/noti2061).
including after the advent of quantum computers. Earlier this year NIST announced the twenty-six algorithms that have been submitted and will advance to the Post-Quantum Crypto Semifinals (https://bit.ly/2to7h5j). Lattice-based algorithms are represented well in this group of twenty-six and are considered by many to be lead contenders for effective post-quantum security. NIST also leads a partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development (https://bit.ly/2PmYvwE).

All four shared their passion for science, the importance of evidence-based approaches to their work in Congress, and for the critical importance and timeliness of this particular topic. Senator Reed called for a federal effort, on the scale of the Manhattan Project, around quantum computing. They also recognized that basic mathematics research is often funded by the NSF and that continuing robust federal funding of the NSF is critical for advancements in our field.

Who else was there? In no particular order:

- many staff from congressional offices—representing individual members of Congress and congressional committees;
- a group of students and faculty doing Hill visits with the Association for Women in Mathematics, including current President Ruth Haas;
- several NSF staff members, including National Science Board Chair Diane Souvaine (https://bit.ly/2PMsFbU);
- staff from the National Academies of Science;

This briefing was attended by four members of Congress—Rhode Island Senators Reed and Whitehouse and Representatives Langevin (RI 2) and McNerney (CA 9). All four gave remarks, and Senator Reed introduced Pipher. I was really pleased that the Rhode Island delegation showed in force and that they acknowledged that the AMS headquarters is in Providence. Representative Langevin, especially, discussed cryptography in technical detail; this topic is one of his top legislative priorities (https://bit.ly/38JiltC), and he is one of Congress’s leaders developing legislation aimed at protecting the nation from cyber-attacks.

Representative Jim Langevin.

I organize and host these briefings together with David Eisenbud, the director of the Mathematical Sciences Research Institute (MSRI). David and I have great staff support for these. The first step, which we usually begin 6–12 months ahead of time, is to find a speaker. We look for dynamic speakers who will talk about a topic of current congressional interest. After a speaker and a few dates are selected, we approach the office of a member of Congress whom we ask to help with logistics for the day (this is necessary because only members of Congress can reserve rooms in the Senate and House and Capitol buildings).
The goals of the briefings are to show congressional members and their staff that

1. Mathematics is everywhere.
2. Federally funding theoretical mathematics (especially by the NSF) leads to scientific advances that help secure our nation and improve our health. Pipher’s presentation and also one we held in 2017 with speaker Shafi Goldwasser focused on security, while advances in MRI technology were discussed by David Donoho at our June 2017 briefing.
3. The AMS is a credible resource.


Jill Pipher is the president of the AMS and vice president for research and Elisha Benjamin Andrews Professor of Mathematics at Brown University. She was the founding director of the Institute for Computational and Experimental Research in Mathematics (ICERM), a National Science Foundation mathematics institute.

References

Credits
Article photos are by Allison O’Brien. Author photo is courtesy of Macalester College/David Turner.