MIT SECURITY STUDIES PROGRAM SEMINAR

Cryptography and the Limits of Secrecy

Ronald Rivest
E. S. Webster Professor of Computer Science and Engineering
Associate Director, Laboratory for Computer Science
Massachusetts Institute of Technology

13 October 1999

Cryptography was first developed around the turn of the century, specifically on the eve of World War I, with the advent of radio communications. It achieved major importance during World II, with the efforts to break the German Enigma code and the Japanese Purple code. After the war the US set up the National Security Agency (NSA), as the chief code-making and code-breaking agency. During the 50's and 60's it was a topic of little discussion.

During the 1970's, however, technological developments in information processing made cryptography an issue of importance to civilians, as corporations needed to protect proprietary information as they transferred it electronically from one site to another. In 1976 the National Institute for Standards in Technology adopted an IBM proposal for a data encryption standard. The setting of this standard led to the first public policy controversy over data encryption: IBM proposed a much longer, and more secure, 128 bit key, but a much shorter, 56-bit key, was adopted. This shorter key was allegedly a compromise between IBM and the NSA to achieve a middle ground between the commercial demands of business to encrypt their data, and those of the government to be able to have access to encrypted data. Given advances in technology, the 56-bit key is now considerably less secure than it was in 1976. That standard, therefore, is today being phased out in favor a yet-to-be adopted Advanced Encryption Standard.

The next major development was "public key" cryptography, which took the NSA somewhat by surprise. The use of public key encryption has obvious commercial applications (for example, it allows for the use of "digital signatures" to authenticate messages), but little military application. In 1977 the RSA public key scheme was developed to address this new development.

The policy issues revolve around two issues: Export control and law enforcement. Both issues revolve around the growing demands of commercial industry for strong encryption technology and those of the government, concerned about the technology compromising US security and hampering domestic law enforcement.

Since the 1950's and 60's cryptographic software and hardware has been on the export control list and requires a license or government approval for export. The problem is that while cryptography used to be largely the purview of the military, today it is heavily commercial: cryptography is found in every PC and web browser, and hundreds of millions use it everyday. While it originally had only military application, today it has become primarily a tool for protecting electronic commerce and information on computers that are hooked up to the internet. The internet and the interconnectivity of computers has created increased commercial vulnerability. The use of cryptography, therefore, in addition to helping electronic commerce, can help protect the US information infrastructure. So, society has needs for cryptography, while the government has legitimate security concerns.

Attempts to find a middle ground -- such as the "clipper chip" or public key escrow, allowing government a "back door" -- may introduce more security concerns than they solve, and therefore have proved wanting. Cryptography is a technology that is infeasible to regulate. In many respects, cryptography is like a pair of gloves. It is essentially a protective technology: Gloves can be worn to protect the hands from extreme temperatures, to prevent the spread of disease, etc. Similarly, cryptography can be used to protect data from forgery, eavesdropping or manipulation. And just as criminals can wear gloves so they won't leave fingerprints, criminals can use cryptography to encrypt their communications and hamper law enforcement. Yet, we don't think about trying to legislate the use of gloves. They are too pervasive and cheap to make. Cryptography is the same way: you can download cryptographic software from the web and it will cost less than a pair of gloves.

Professor Rivest is the Webster Professor of Electrical Engineering and Computer Science in MIT's Department of Electrical Engineering and Computer Science. He is a member of MIT's Laboratory for Computer Science, a member of the lab's Theory of Computation Group and a founder of its Cryptography and Information Security Group. He is also a founder of RSA Data Security (now merged with Security Dynamics to form RSA Security). Professor Rivest has research interests in cryptography, computer and network security, and algorithms.

Rapporteur: David Mendeloff