The Export of Cryptography in the 20th Century and the 21st

Whitfield Diffie and Susan Landau

Introduction by Whitfield Diffie and Susan Landau

Our efforts have focussed on two parallel tracks. The first has been to remove the government restrictions on the deployment of cryptography. Simultaneously we have worked on new issues affecting security, including new threats, new policy problems, and new technical directions.

This paper does not report the results of research in the usual sense. It reports the outcome of seven years work whose results are measured not in increased knowledge but in an improved environment for Sun development and Sun marketing. The lifespan of Sun Microsystems coincides closely with the era of globalization. To compete in the global economy economy, Sun, like other large companies, must have access to markets all over the world. One important limitation on this access has been US export−control regulations. The report describes the results of a decade−long battle to reconcile the export regulations with the realities of modern business and technology. Success was achieved in the year 2000 with sweeping improvements in the regulations. This environment will lead to new products and improved functioning of existing products both in Sun's core business areas and in developing areas such as wireless communications.

For most of the era of electronic communication, encryption −− protecting communications by scrambling them −− was largely the province of the government. Before modern electronics, encryption was too expensive for widespread business use. Most development was done by the government and kept secret for exclusive government use. Cryptography was treated as a weapon under the export−control laws and encryption systems could not be exported for commercial purposes, even to close allies and trading partners.

During the 1980s and 1990s cryptography emerged from its role as an obscure technology used by the government to protect its communications to a necessary underpinning of Internet commerce. The rise of the personal computer and the Internet changed cryptography from an exotic military−only technology into a critical technology of Internet commerce. Despite this, the government was slow to accept the new reality. Industry efforts to develop and use cryptography were thwarted by government export−control regulations, which emerged as the dominant government influence on the manufacture and use of encryption technlogy. Making repeated attempts to continue its domination of the field, by the late 1990s the US government held a stance that was barely tenable in the rest of the world. Influences varying from the rise of open−source software to European indignation at evidence of US communications intelligence came together to force a change.

PAPERS, BOOKS, REPORTS, OP−EDS:

S. Landau, S. Kent, C. Brooks, S. Charney, D. Denning, W. Diffie, A. Lauck, D. Miller, P. Neumann and D. Sobel, ‘‘Codes, Keys and Conflicts: Issues in U.S. Crypto Policy,’’ ACM Press, 1994.
http://info.acm.org/reports/acm_crypto_study.html

S. Landau, S. Kent, C. Brooks, S. Charney, D. Denning, W. Diffie, A. Lauck, D. Miller, P. Neumann and D. Sobel, ‘‘Crypto Policy Perspectives,’’ Communications of the ACM, Vol. 37 (August 1994), pp. 115−121.

Susan Landau and Whitfield Diffie, ‘‘Cryptography Control: FBI Wants It, but Why?,’’ Christian Science Montitor, October 6, 1997.
http://www.csmonitor.com/durable/1997/10/06/opin/opin.2.html

Whitfield Diffie and Susan Landau, Privacy on the Line: the Politics of Wiretapping and Encryption, MIT Press, 1998.
http://mitpress.mit.edu/book−home.tcl?isbn=0262041677

‘‘Standing the Test of Time: The Data Encryption Standard,’’ Notices of the American Mathematical Society, March 2000, pp. 341−349.
http://www.ams.org/notices/200003/fea−landau.pdf
Reprinted, in translation, in ‘‘Surveys in Applied and Industrial Mathematics,’’ TVP Publishers (Moscow), Vol. 7, No. 2 (2000), pp. 240−258.

‘‘Communications Security for the Twenty−First Century: the Advanced Encryption Standard,’’ Notices of the American Mathematical Society, April 2000, pp. 450−−459.
http://www.ams.org/notices/200004/fea−landau.pdf
Reprinted, in translation, in ‘‘Surveys in Applied and Industrial Mathematics,’’ TVP Publishers (Moscow), Vol. 7, No. 2 (2000), pp. 259−281.

‘‘Advanced Encryption Standard Choice is Rijndael,’’ Notices of the American Mathematical Society, January 2001, p. 38.
http://www.ams.org/notices/200101/200101−toc.html