

## Cryptology\*

---

Cryptology, the science of communication secrecy, is bound to censorship by a dual and conflicting relationship: on the one hand, its object has been closely associated with the security interests of the state, which has historically sought to monitor and control the diffusion of cryptological knowledge and technologies; on the other hand, cryptology has provided some of the very means by which various social groups — from the Freemasons to online communities — have eluded censorship and protected the confidentiality of their communications. The history of cryptology thus rides on tensions between technologies of free speech and social control, between ideals of unfettered scientific communication and the secrecy culture of military intelligence.

While traces of cryptological activity have been found in most ancient civilisations, from Mesopotamia to the Roman Empire, systematic development of codes and ciphers awaited the flowering of modern European diplomacy in the 1500's, and the need for means of confidential communication such diplomacy requires. For example, in 1542, the Venetian state employed three “cipher secretaries” assigned to the development of such codes; they enjoyed a relatively high status within Venetian society, any betrayal of the cryptological secrets in their possession was deemed worthy of punishment by death. As codes increasingly gained in sophistication, so did the methods for solving them: by the 18th century most European nations had established “black chambers,” secret organisations specialised in deciphering foreign diplomatic dispatches. Advances in telecommunication technology (telegraph, radio communication) further established the military significance of cryptology while spurring commercial needs for ciphers and codebooks and increasing the diffusion of cryptological knowledge among experts and the general public.

The most famous case of explicit censorship to involve cryptology occurred in the aftermath of the World War I. Stating, rather surprisingly, that “gentleman do not read each other's mail”, the US secretary of state Stimson closed down in 1929 the main American cryptological operation. Unable to find work, its former head, Herbert Yardley, published a sensational tell-all, *The American Black Chamber*: a minor best-seller, it not only detailed the scope of American cryptological activities, but also documented the interception and decryption of Japanese diplomatic dispatches during the disarmament conference of November 1921. The ensuing Japanese fury prompted swift American reaction over Yardley's following literary project: the manuscript of *Japanese Diplomatic Secrets: 1919[-]1921* was seized and impounded by the United States government. While neither Yardley nor his editors faced charges, Congress promptly passed into law the so-called Yardley Act, forbidding “the publication or sale of diplomatic codes obtained by virtue of one's employment by the United States.”

---

\*Blanchette, Jean-François, “Cryptology,” in *Censorship: A World Encyclopedia* (Derek Jones, ed.), vol. 1, pp. 603-604. London: Fitzroy Dearborn Publishers, 2001.

In the 1970's, the emergence of a small but creative academic community of cryptologists would pit the right to unrestricted scientific inquiry against the needs of national security. To the dismay of the intelligence establishment, academics busily exchanged papers, convened international conferences, and founded journals. In the United States, the highly secretive National Security Agency floundered in a number of awkward attempts at stemming this sudden flow of sensitive information. These initial skirmishes culminated in 1982 in an agreement for a voluntary prepublication review program, a procedure in effect. While the NSA expressed "the hope that affected researchers, academicians, writers and publishers will work with us in this endeavour," it supplemented this hope with a liberal use of regulatory measures — export controls, R&D funding, federal standards, patent secrecy — aimed at shaping the research agenda and controlling the diffusion of technologies. Such measures have also been enacted, with varying degrees of stringency, in a number of other countries and international accords. Strictest of all, France required until 1996 authorisation for the mere private use of encryption technologies.

The explosive growth of the internet in the 1990's has further heightened the tensions between the need for the wide diffusion of cryptological technologies necessary for securing electronic information and the fears of law enforcement officials that such diffusion might make their work increasingly difficult. In response to these concerns, the United States government has advocated the adoption of "key escrow" technologies for all digital communication equipment, aimed at preserving law enforcement's capabilities for wiretapping and intelligence gathering. Despite public outcry and widespread doubt over the effectiveness of such systems, the issue remains controversial, and other countries — among them Britain and Canada — have or are contemplating similar proposals.

At the other end of the ideological spectrum, encryption has proved highly valuable to political activists and human rights organizations seeking to protect their electronic communications from governmental intrusion. The popularity of PGP, a free encryption package, placed its author, Philip Zimmerman, at the centre of a criminal investigation probing possible violations of US export regulations. Opposing might with irony, the MIT Press published in 1995 the entire source code of PGP in book form, in effect mocking the bizarre rules permitting the export of cryptography books, but not that of the accompanying software.

These conflicts seem unlikely to disappear in the near future. If the various controls imposed on cryptology have been decried by industry leaders, academics, and civil libertarians alike, governments have lent a generous ear to the concerns of the military and law enforcement communities over the availability of cryptological technologies. While the impact of these technologies will soon be felt at all levels of daily life — from digital signatures to smartcard-based medical records and electronic cash — cryptology's historical status as a highly sensitive military science will continue to warrant its close monitoring by the state. This dual identity is assurance that cryptology

will play a defining role in how the conflict between free speech and social control plays out in the new digital order.

## Further Reading

---

Bamford, James, *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency from the Cold War through the Dawn of a New Century*. New York, Doubleday, 2001.

Dam Kenneth W. and Herbert S. Lin (eds.) *Cryptography's Role in Securing the Information Society*. National Academy Press, 1996

Denniston, Robin, "Yardley's Diplomatic Secrets" in *Cryptologia* 18/2 (1994):81-127

Hoffman, Lance J. (ed.) *Building in Big Brother: The Cryptographic Policy Debate*. New York: Springer-Verlag, 1995

Kahn, David, *The Codebreakers*, New York: The Macmillan Company, 1967; revised edition, New York: Scribner, 1996

Kahn, David, "Cryptology Goes Public" in *Foreign Affairs* 58 (1979):141-159.

Landau, Susan, "Primes, Codes and the National Security Agency" in *Notices of the American Mathematical Society*, 30/1 (1983): 7-10.

Landau, Susan, "Zero Knowledge and the Department of Defense" in *Notices of the American Mathematical Society*, 35/1 (1988):5-12.

Madsen, Wayne, and David Banisar, *Cryptography and Liberty 2000: An International Survey of Cryptography Policy*, Washington, DC: Epic, 2000.

Relyea, Harold C., *Silencing Science: National Security Controls and Scientific Communication*, Norwood: Ablex Publishing Corporation, 1994.

Rosenheim, Shawn James, *The Cryptographic Imagination: Secret Writing from Edgar Poe to the Internet*. Baltimore: The John Hopkins University Press, 1997.

Shinn, Allen M., "The First Amendment and the Export Laws: Free Speech on Scientific and Technical Matters" in *George Washington Law Review* 58 (1990): 368-403.

Zimmerman, Philip R., *PGP: Source Code and Internals*. Cambridge, Massachusetts: The MIT Press, 1995.