CATO INSTITUTE BRIEFING PAPERS

Strong Cryptography The Global Tide of Change

by Arnold G. Reinhold

No. 51 **September 17, 1999**

Encryption technology allows people using electronic networks to ensure that the messages they send remain private—secure from hackers, industrial espionage, government wiretap abuses, and spies. Encryption technology will prove vital to the future of electronic commerce. For example, thefts of nuclear secrets from U.S. national laboratories would be much less likely if the labs' commercial software had built-in encryption features that could be used to limit unauthorized access—a type of security product discouraged by export controls.

For years the U.S. government has struggled unsuccessfully to control the export of encryption technology from this country. Those ineffectual controls do, however, adversely affect the competitive position of the U.S. software industry and national security. Despite the controls, powerful encryption products are increasingly available around the world. Those products include Pretty Good Privacy, which offers 128-bit encryption, and many others. This paper provides a list of Web sites where such products may be found, thus establishing beyond doubt the futility of controls. Although some of the Web sites may from time to time disappear, others will spring up in their place.

Arnold G. Reinhold is the coauthor of The Internet for Dummies Quick Reference *and* E-mail for Dummies.

This paper provides a list of Web sites where such products may be found, thus establishing beyond doubt the futility of controls.

Introduction

According to legend, King Canute's ministers believed so strongly in royal divine authority that, to prove them wrong, the wise monarch marched down to the ocean and commanded the tide to stop coming in. He got wet feet and the ministers earned a permanent place of honor in the legion of the ridiculous.

The parallels between Canute's experiment in applied theology and the U.S. government's policy on encryption are becoming more evident each day. As officials try one approach after another to prevent the spread of strong encryption, its availability only grows. Measures announced by the Clinton administration, which will allow the export of encryption products of unlimited strength to subsidiaries of U.S. companies in most countries and to the banking, insurance, health care, and electronic commerce sectors in 42 countries, signify the beginning of the end for cryptographic export controls.[1] It is time to recognize the inevitability of strong, nonrecoverable cryptography and take steps to maximize that technology's benefits to society and deal realistically with its less desirable attributes.

The stated reason for U.S. government opposition to public access to strong cryptography is to preserve the government's ability to gain access to criminal communications through wiretaps and computer data files seized as evidence. Such claims usually invoke a troika of evils—drug dealers, terrorists, and child pornographers—though decades of wiretapping have not halted those crimes.

Also, for much of the 20th century the United States has used intercepted communications as a primary source of information about its adversaries. Cryptoanalytic breakthroughs were more vital to our victory in World War II than was the atomic bomb. The extent to which the United States is still able to break codes used by foreign governments and organizations is a closely held secret. A former Central Intelligence Agency agent was arrested in 1998 for allegedly revealing information about broken codes to two foreign governments, but press reports indicate that his job was to break into foreign government offices to steal cryptographic keys. Widespread commercial use of strong cryptography may hasten the inevitable loss of such intelligence sources, to the extent they are still flowing. In addition, the United States no doubt derives valuable intelligence by analyzing vast quantities of unencrypted communications, a benefit that some observers believe could be preserved by guaranteeing government access to the keys to encrypted communications. However, code breaking is most useful when the parties using the code do not realize that their code has been compromised. Since "back doors" built into crypto products because of legal requirements would be public knowledge, they would have limited use in signals intelligence.[2]

Cryptographic technology is so widespread that it is impossible to stop. If any major governments, terrorist organizations, or drug cartels are not now using strong cryptography, it is not because of lack of availability or lack of reliable suppliers. There are many firms overseas that are willing to provide cryptographic software, and, for better or for worse, some of the cryptographic products most widely available on the international market were originally made in the United States. This paper outlines the availability of strong crypto abroad, underscoring the futility of export controls.

Strong Cryptography

Cryptography is the ancient art and science of transforming information so that it is no longer intelligible to the uninitiated but can be read by those in possession of some special knowledge.[3] That knowledge usually takes the form of a decryption key. Strong encryption performs transforma-

tions using methods that are believed to be impenetrable to anyone not possessing the decryption key.

To be considered strong, any cryptographic system (for computers or pen and ink) must be shown to be free of mathematical weaknesses that make it possible to break.[4] In addition, the decryption keys must have sufficient variability to make trying all key combinations (a "brute force" attack) impractical.

Computers perform complicated mathematical transformations and brute force attacks much more quickly than unaided humans or vintage machines like the Enigma.[5] Today computers are almost always used to perform encryption and decryption. But strong methods of encryption can be and have been developed and used without the aid of computers,[6] as they were in Thomas Jefferson's day; the process is just more cumbersome.

There are two types of encryption systems for computer systems in use today. Conventional, or symmetric, encryption uses the same key for encryption and decryption. A symmetric key is a string of random bits; the key's variability and strength are measured simply by the number of random bits in it.[7] Cryptographers recommend that, to be reasonably secure, keys should be at least 90 bits long.[8] The world standard is 128 bits because that is a convenient size for computers. There is no technical reason to use shorter keys.[9]

The second type of encryption, public-key or asymmetric systems, uses separate keys for encryption and decryption: the private key and the public key. The private key must always remain secret. The public key is derived from the private key by using a mathematical formula that makes deriving the private key extremely difficult. For example, if two large prime numbers are multiplied together, it is very hard to reverse the operation to deduce the prime numbers if one is given only the product to work from. Public keys must be long enough that known methods of reversing the operations used to derive them from the private keys fail by a sufficient safety margin. RSA Data Security, Inc., a subsidiary of Security Dynamics Technologies, Inc., holder of the patents on cryptography based on multiplying large prime numbers, recommends this type of key be at least 1024 bits long for moderate security and 2048 bits for high security. The U.S. Bureau of Export Administration (known as BXA) considers encryption systems with symmetric keys that are more than 56 bits long or asymmetric keys longer than 1024 bits strong and subjects them to export controls. Although exports to some industries in some countries have been liberalized, a vast array of encryption products is still encumbered by export controls.

Impact of Strong Cryptography Controls

Export restrictions have delayed the introduction of electronic commerce and weakened the position of the U.S. software industry in comparison with its overseas competition. The Economic Strategy Institute issued a report estimating losses to the U.S. economy due to encryption export restrictions at between $37 billion and $96 billion over the next five years.[10]

The recent sectoral relief does nothing to allow U.S. companies to develop encryption products for the great mass of communications, such as email or telephony.[11] Restrictions continue to discourage the integration of encryption into operating systems and computer chips. Without such integration, effective computer security is almost impossible to achieve.

Encryption export restrictions also adversely affect U.S. national security. Recently, Los Alamos National Laboratory shut down the entire classified computer network used to design and validate nuclear weapons because it was so insecure. Allegations of theft of atomic weapons secrets from Los Alamos[12] have prompted

Cryptographic technology is so widespread that it is impossible to stop. If any major governments, terrorist organizations, or drug cartels are not now using strong cryptography, it is not because of lack of availability or lack of reliable suppliers.

calls for tightening export controls. Yet there is a strong case to be made that U.S. export controls on cryptography contributed to those problems.

Encryption is at the heart of all computer security schemes. Fear of export regulations has led mass-market software vendors to simply ignore security. A major reason our national nuclear weapons labs cannot protect restricted data from theft by insiders is that their computers use commercial operating systems. Those operating systems lack the fine-grained transfer controls needed to enforce security policies covering authorized users.

The reason such tools do not exist in commercial operating systems is not an absence of market demand—many industries have a need for such capabilities—but the fact that such tools require strong cryptography and therefore would subject the operating systems that contain them to export controls. Since our commercial software industry depends on export revenue, firms won't develop those features, and the government does not have the ability to develop the tools on its own. Thus, as a result of decades of restrictions on cryptography, not only our national labs but every sector of American society is wide open to insider espionage.

Restrictions continue to discourage the integration of encryption into operating systems and computer chips. Without such integration, effective computer security is almost impossible to achieve.

Key Recovery

Encryption export controls were also designed to provide leverage for the government to foist "key recovery" on an unwilling market. Key recovery, or key escrow, encryption provides the government with a mechanism for recovering a decrypted message without the knowledge of the information's owner or intended recipients. For example, the government might require the deposit of all private keys in "escrow" with a third party; police desiring access to the contents of the message could then approach the third party without notifying the key's owner. The administration's new encryption policy will permit the export of key recovery products under general license after one-time review. There are several problems with that approach.

First, key recovery is cumbersome and expensive. One significant reason is technical problems with rapid access to the decrypted content.[13] Even U.S. government agencies resist using key recovery and prefer nonescrow products.[14] For many applications, there is no need for key recovery features except to meet the demands of law enforcement. Thus there is limited market demand for key recovery systems for stored information—and none for key recovery systems for real-time communications like phone calls. Key recovery systems will be unable to compete with cheaper nonescrow alternatives.

Second, any attempt to restrict cryptographic technology that does not support key recovery—domestic or international—will violate the First Amendment. For example, export controls amount to a prior restraint on professors of mathematics who want to present their ideas about cryptography to foreign students or to colleagues in foreign countries.[15]

Third, key recovery will create new targets for miscreants to attack. Given the enormous value that the data in key repositories represents, it is only a matter of time before they will be compromised. Even the best security arrangements are vulnerable to bribes, blackmail, and threats of bodily harm. Over time, commitment to security will wither under cost pressures and boredom. Some key recovery systems do not rely on key depositories. Rather, they use another key to encrypt the private key to every communication and attach it to the message itself. The key used to encrypt all the private keys then becomes the focus of attacks and bribery.

The Cryptographic Cat Is Out of the Bag

Many of the arguments about strong cryptography turn on judgment calls or bal-

ancing—for example, when, if ever, does the threat of the use of encryption by criminals justify sacrifices of constitutional guarantees of liberty? But it is a simple matter of fact that export controls are futile because strong cryptography is already widely available to the general public, and to the "bad guys" as well.[16] Why would drug dealers, for example, who now run private airlines, bribe judges, assassinate opponents, subvert armies, and even help elect national leaders, be deterred from obtaining widely available cryptographic software?

Today, anyone anywhere in the world

Links to Strong Encryption

Adam Back's home page with crypto links
http://www.dcs.ex.ac.uk/~aba/

Adam Back's RSA "munitions" T-Shirt homepage
http://www.obscura.com/~shirt/

Bibliography of Quantum Cryptography Steganography bibliography, workshop, mailing list
http://www.cs.mcgill.ca/~crepeau/CRYPTO/Biblio-QC.html

CipherSaber Home Page
http://www.ciphersaber.gurus.com/

Cryptography A-2-Z
http://www.ssh.fi/tech/crypto/

Cypherpunks Tonga
http://www.cypherpunks.to/

The Data Encryption Page
http://www.geocities.com/SiliconValley/Network/ 2811/

EFF "Privacy, Security, Crypto, Surveillance" Archive
http://www.eff.org/pub/Privacy/

Fortify
http://www.fortify.net/

Free Crypto.org
http://www.freecrypto.org/

Mozilla Crupto Group
http://www.mozilla-crypto.ssleay.org/index.php/

Netsurfer Focus on Cryptography and Privacy
http://www.netsurf.com/nsf/v01/03/nsf.01.03.html

PGP and Anonymous Remailers made Simple using Windows
http://home.earthlink.net/~rjswan/pgp/

Ron Rivest's Cryptography and Security collection
http://theory.lcs.mit.edu/~rivest/cryptosecurity.html

Ron Rivest's home page with publications and links
http://theory.lcs.mit.edu/~rivest/

RPK public key cryptosystem page
http://www.rpkusa.com/

RSAEuro
http://www.repertech.com/RSAEuro/

Software Publishers Association report on availability of crypto overseas
http://www.eff.org/pub/Crypto/ITAR_export/non-us_crypto_spa.report

Thawte Digital Certificate Services
http://www.thawte.com/

Where to Find Strong Crypto Online
http://www.jya.com/crypto_table.html

It is a simple matter of fact that export controls are futile because strong cryptgraphy is already widely available to the general public, and to the "bad guys" as well.

with access to the Internet can download Pretty Good Privacy, as well as foreign cryptographic products.[17] PGP was originally written by Phil Zimmermann, who combined several widely known cryptographic algorithms to create a practical cryptographic system for protecting electronic mail and computer files. An unknown person posted PGP to the Internet, and PGP quickly spread throughout the world. The government subjected Zimmermann to a lengthy investigation for possibly violating U.S. export laws but never indicted him, apparently because it could not determine who actually exported the software.

In December 1998 the United States pressured the 33 member countries of the Wassenaar Arrangement, which limits and tracks the export of arms and "dual-use" goods (encryption technology is listed under this category) from country to country, to place controls on encryption products with keys over 64 bits. Sweden, for example, was reportedly threatened with trade sanctions to get it to sign the agreement.[18] But the Wassenaar signatories have wide discretion as to how to implement the controls, and some will elect not to enforce them. Finland, Ireland, Canada, and Germany have announced support for liberal export regimes.[19] France recently dropped its restrictions on domestic encryption up to 128 bits.[20] Support in the United Kingdom for mandatory key escrow has rapidly evaporated.[21] This leaves citizens of almost every country around the world free to use strong crypto domestically—they simply will not buy it from the United States. Some crypto-exporting nations, such as South Africa and Israel, are not Wassenaar signatories.[22] In June 1999 Germany, a Wassenaar signatory, announced its intention to support strong encryption for domestic use and for international export.[23] Countries around the world will see the futility of trying to control the export of strong encryption and respond to strong incentives to help their national companies compete more effectively in the world market.

Conclusion

Years of debate about the justifications for export controls have supplied many reasons to think that encryption export controls are costly and unconstitutional—and some sophisticated counterarguments. Commentators new to the debate may find themselves endlessly reviving points the discussion has long since moved past. But the simple reality that strong encryption is widely available around the globe can rescue us from endless debate. The security benefits of strong privacy will be available to everyone; law enforcement can and will adapt. It is time to move forward.

Notes

1. "Administration Updates Encryption Policy," http://www.cdt.org/crypto/admin/whousepress091698.html, p. 1; "Fact Sheet: Administration Updates Encryption Policy," http://www.epic.org/crypto/ export_controls/ wh-factsheet-998.html, p. 1; "Press Briefing by the Vice President," September 16, 1998, http://www.epic.org/crypto/export_controls/wh-transcript-998.html, p. 5; BXA encryption press release, http://www.bxa.doc.gov/PRESS/98/1230Encryption.html; and "Summary of Encryption Policy Update," http://www.bxa.doc.gov/Encryption/EncrypolicyUpdate.htm.

2. Carl Ellison, "Myths and Realities of the Debate over Encryption Policy," in *Economic Casualties: How U.S. Foreign Policy Undermines Trade, Growth, and Liberty*, ed. Solveig Singleton and Daniel T. Griswold (Washington: Cato Institute, 1999), pp. 58–59.

3. Cryptography, which includes traditional codes and ciphers, relies on making a secret message unintelligible to outsiders by jumbling the normal order of letters in a message (transposition) or by substituting other letters, numbers, or symbols for the original letters (substitution). Steganography, by contrast, hides the secret message in other text or a picture. David Kahn, *The Codebreakers (*New York: Scribner, 1967), pp. xiii–xvi.

4. While the methods commonly used for strong encryption have, with one notable exception, never been mathematically proven, experts in the field award this appellation to a number of algorithms that have undergone years of public scrutiny without revealing unacceptable weakness.

5. Enigma was Germany's main cryptographic system during World War II. Engineer Arthur Scherbius first patented Enigma in 1919. A private company marketed the device as a means of protecting business secrets, but it did not sell well and the company went out of business. The machine reappeared again during Hitler's time as a battery-powered device encased in a wooden box, about the bulk of a typewriter. Its operation required three men. Kahn, pp. 420–22. Computing pioneer Alan Turning developed a machine called the Bombe, dozens of which were employed to decrypt Enigma messages for the British government. M. Mitchell Waldrop, "Alan Turing: The Oddball Who Changed the World," *Washington Post*, June 9, 1999, p. H1.

6. Bruce Schneier describes how to do secure cryptography using a deck of cards. See http://www.counterpane.com/solitaire.html.

7. The strength of the keys in an asymmetric encryption system is also measured this way.

8."To provide adequate protection against the most serious threats . . . keys used to protect data today should be at least 75 bits long. To protect information adequately for the next 20 years . . . keys in newly deployed systems should be at least 90 bits long." Matt Blaze et al., "Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security," January 1996, p. 2, http://www.bas.org/policy/index.html.

9. D. James Bidzos, Vice Chair of Security Dynamics Technologies, Inc., Statement to the Senate Commerce, Science and Transportation Committee, Federal News Service, June 10, 1999, p. 4.

10. Erik R. Olbeter and Christopher Hamilton, *Finding the Key: Reconciling National and Economic Security Interests in Cryptography Policy* (Washington: Economic Strategy Institute, 1998).

11. Following the Ninth Circuit Court of Appeals' ruling that current restrictions on the export of encryption were unconstitutional, Hush Communications announced it would integrate 1024-bit encryption into its email service. Lindsey Arent, "Bulletproof Email for the Masses," *Wired News*, May 21, 1999, http:www.wired.com/news/news/technology/story/19804.html.

12. Select Committee of the U.S. House of Representatives, *U.S. National Security and Military/Commercial Concerns with the People's Republic of China* (Washington: U.S. Government Printing House, 1999), vol. 1, p. III.

13. Bruce Schneier, "Is Escrow Dead, And What Is Wassenaar?" Panel discussion at Conference on Computers, Freedom & Privacy '99, Washington, April 8, 1999.

14. An intragovernmental memo states:

> Police forces are reluctant to use "escrowed" encryption products (such as radios in patrol cars). They are more costly and less efficient than non-escrowed products. There can be long gaps in reception due to the escrow features—sometimes as long as a ten second pause. Our own police do not use recoverable encryption products; they buy the same non-escrowable products used by their counterparts in Europe and Japan.

William Reinsch, Under Secretary of Commerce and head of the Bureau of Export Administration, "Memorandum for Deputies Subgroup on Cryptography," November 25, 1996, p. 1, http://www.epic.org/crypto/key_escrow/reinsch_memo.html; and Electronic Privacy Information Center press release on the Reinsch memo, March 25, 1998, http://www.epic.org/crypto/key_escrow/ reinsch_memo_release.html.

15. In *Bernstein v. United States*, 1999 U.S. App. LEXIS 8595 (9th. Cir 1999), the court affirmed that the Encryption Export Administrator's attempt to require mathematician Daniel Bernstein to submit an encryption algorithm that he wished to discuss with foreign colleagues and students was an unconstitutional prior restraint.

16. The latest survey, by Professor Lance Hoffman of George Washington University, identified at least 167 foreign cryptographic products that use strong encryption in the form of these algorithms: Triple DES, IDEA, BLOWFISH, RC5, or CAST-128. New producers of encryption products have appeared in six new countries since December 1997. The foreign availability study is available at http://www.computerprivacy.org.

17. PGP became very popular on the Internet and a company, PGP Inc., was formed to commercialize the technology. In 1997 PGP Inc. was sold for $36 million, and it is now part of Network Associates Inc.

18. "Sweden Threatened with Trade Sanctions over Encryption Change?" *Nordic Business Report*, March 15, 1999, electronic document.

19. Joanne Wallen and Dan Sabbagh, "7 Days; An Outbreak of Harmony," *Computing*, June 3, 1999, p. 24.

20. Ken Cukier, " France Heralds Fall of Its Crypto 'Maginot Line,'" *Communications Week International*, February 1, 1999, p. 1.

21. Duncan Campbell, "Computing and the Net: Cave-in on a Key Measure," *The Guardian*, March 11, 1999, p. 4. See also http://www.cabinet office.gov.uk/Innovation/1999/encrytion/index.htm.

22. Thomas Parenty, director of Data and Communications Security Sybase, Inc., in testimony on behalf of the Business Software Alliance before the Subcommittee on Courts and Intellect-ual Property of the House Committee on the Judiciary, said:

> Many countries, such as Israel and South Africa, who export strong encryption are not signatories to the Arrangement. . . . The Wassenaar Arrangement . . . removed any reporting requirements, the sole official means for actually monitoring what countries are doing. Although the Arrangement left open the possibility that countries might individually control 128-bit encryption, we are skeptical that they will do so. There is no penalty for failing to control 128-bit encryption, and most countries are actually moving towards encouraging the use of stronger encryption. Finally, a country could technically comply with the Arrangement, while still permitting easy exports of strong encryption.

Federal News Service, March 4, 1999.

23. The official translation of Germany's new policy states, "The Federal Government considers the capability of German manufacturers to develop and manufacture secure and powerful cryptographic products as crucial to security of nation, business, and society. It will take actions to improve the international competitiveness in this field." The new policy supposedly will also simplify the export review process. Federal Ministry of the Interior, Federal Ministry of Economic Affairs and Technology, "Cornerstones of German Encryption Policy," Bonn, June 2, 1999, http://jya.com/de-crypto-all.htm. See also "Germany Endorses Strong Crypto," *Wired News Report*, June 3, 1999, http://www.wired.com/news/news/politics/story/20023.html.

Published by the Cato Institute, Cato Briefing Papers is a regular series evaluating government policies and offering proposals for reform. Nothing in Cato Briefing Papers should be construed as necessarily reflecting the views of the Cato Institute or as an attempt to aid or hinder the passage of any bill before Congress. Additional copies of Cato Briefing Papers are $2.00 each ($1.00 in bulk). To order, or for a complete listing of available studies, write the Cato Institute, 1000 Massachusetts Avenue, N.W., Washington, D.C. 20001, call (202) 842-0200 or fax (202) 842-3490. Contact the Cato Institute for reprint permission.