CATO INSTITUTE BRIEFING PAPERS

THE MYTH OF SUPERIORITY OF AMERICAN ENCRYPTION PRODUCTS

BY HENRY B. WOLFE

No. 42 November 12, 1998

Executive Summary

Encryption software and hardware use sophisticated mathematical algorithms to encipher a message so that only the intended recipient may read it. Fearing that criminals and terrorists will use encryption to evade authorities, the United States now restricts the export of encryption products with key lengths of more than 56 bits. The controls are futile, because strong encryption products are readily available overseas.

Foreign-made encryption products are as good as, or better than, U.S.-made products. U.S. cryptographers have no monopoly on the mathematical knowledge and methods used to create strong encryption. Powerful encryption symmetric-key technologies developed in other countries include IDEA and GOST. Researchers in New Zealand have developed very strong public-key encryption systems. As patents on strong algorithms of U.S. origin expire, researchers in other countries will gain additional opportunities to develop strong encryption technology based on those algorithms.

THE MYTH OF SUPERIORITY OF AMERICAN ENCRYPTION PRODUCTS

by Henry B. Wolfe

Encryption software and hardware use sophisticated mathematical algorithms to encipher a message so that only the intended recipient may read it. Encryption is the best way to keep electronic messages private and secure. Initially, the U.S. Department of State regulated encryption exports as "munitions" under the International Trade in Arms Regulations, promulgated under the Arms Export Control Act of 1976.[1] Executive Order 13026, issued by President Clinton in November 1996, moved the responsibility to the Bureau of Export Administration, an agency of the U.S. Department of Commerce.[2] Today, U.S. regulation prohibits the export of many products that incorporate strong encryption. One important determinant of the strength of an encryption system is the length of the key to the cipher, measured in bits. Only hardware and software products with a key size of fewer than 56 bits have been approved for export under a general license. The administration has announced that exports of products offering unlimited bit length will be approved to subsidiaries of U.S. corporations worldwide (except for those in the seven "terrorist nations"), to health and insurance companies, and to on-line merchants (in 45 countries). But restrictions remain on many types of encryption products, especially those that would be used by noncommercial groups or individuals for end-to-end encryption of e-mail or other communications.

Licensing requirements and export controls restrict the strength--and thus the quality--of many types of encryption products exported from the United States. Products able to meet the licensing requirements are routinely reduced in their overall security effectiveness and do not meet the requirements of the overseas market. Export controls are intended to keep sensitive technology out of the hands of terrorists and countries hostile to the United States. For export controls to succeed, authorities recognize that the controlled technology must not be available from sources outside the United States.[3]

Henry B. Wolfe has been an active computer professional for nearly 40 years. He has taught computer security at the graduate level at the University of Otago in New Zealand for the past 15 years.

People living outside the United States find it amusing and perplexing that U.S. law regulates the distribution of strong encryption. But anyone outside the United States can easily obtain strong encryption. The source code for most of the popular strong encryption algorithms is available for downloading at no cost. Sites that provide the code, scattered around the world, are not subject to U.S. law.[4] Thus, export controls have little or no relevance outside the United States. At best, export controls are futile.

Supporters of export controls argue that America is the only source of high-quality strong encryption, because encryption algorithms developed elsewhere are inferior in relative security to those originating in the United States.[5] A recent Commerce Department report states, "Our information indicates that, on the whole, American encryption is superior."[6] The report refers to a classified Commerce Department survey of 28 products released in 1994;[7] the analysis of non-U.S. cryptographic systems is inked out in publicly available copies, making it difficult to rebut. But the statement is hotly contested and, obviously, subject to independent analysis.[8] This paper shows that the theory of the inferiority of non-U.S. crypto defies common sense and ignores a number of strong encryption systems developed in other nations.

A good cryptographer needs an in-depth understanding of higher level mathematics, some basic analytical talent, and exposure to the fundamentals of cryptographic history and current techniques. Anyone with an interest in that body of knowledge can have access to it. No geographic attribute significantly influences the qualities necessary to be a cryptographer or gives citizens of one nation any advantage over those of another.

This paper shows that cryptographic products that originate outside the United States are not inferior to those created internally. The notion that overseas computer users will not take the time to modify products to improve their security or seek out strong encryption from sources outside the United States is ridiculous. In addition, strong encryption technology developed within the United States or outside of it readily spreads to other countries in spite of export controls. Although some other countries have export controls (for example, New Zealand), many present no obstacle to the export of encryption products developed there, and the remainder (such as Finland) have in effect no controls at all.[9]

Symmetric Algorithms Developed outside the United States

Among symmetric systems, in which a single key is used to both encrypt and decrypt, IDEA (International Data Encryption Algorithm) stands out as one of the most secure. Developed by Xuejia Lai and James Massey in 1990, the algorithm is patented and the rights are owned by Ascom Systec AG, a Swiss company,[10] IDEA is freely available in source code anywhere in the world via the Internet from Ascom-direct. If it is to be used in a commercial product, it must be licensed from Ascom. Products that use this algorithm are available internationally.

The cryptographic community at large has scrutinized IDEA and deems it one of the most secure cryptographic systems of its kind available today.[11] As have those of most proven algorithms, the details of its workings have been published and the source code is accessible on many Internet sites. According to Bruce Schneier in his book Applied Cryptography, IDEA is his choice for the most secure algorithm of its type.[12] The algorithm uses a 128-bit key. What that means is that the total number of unique keys that can be handled by IDEA is 2^{128}, a truly large number--340 followed by 36 zeros. That number of keys is considered computationally secure. Let us put that into perspective: a brute-force attack (one in which every possible key in the entire key space is tried until the correct one is found) using a billion processors each testing a billion different keys every second simultaneously would take 10^{13} years to go through the entire key space for IDEA.

Another algorithm of interest is GOST (256-bit key), originating in Russia. This symmetric system is thought to be at least as strong as the DES (American Data Encryption Standard) and probably much stronger. The key space of GOST (2^{256}) is defined as 115 followed by 75 zeros. Under certain conditions, the prescribed key space for GOST can be as large as 2^{610}--a number too large to be grasped and certainly far beyond any brute-force attack.

It is worth mentioning that a brute-force attack is at this time the only reasonable attack strategy for both IDEA and GOST. One researcher thought he had identified a weakness in GOST, but unless the attacker can alter certain conditions--rarely the case in normal use--the probability of success "is too low to make the attack practical."[13]

Other symmetric-key strong cryptographic products based in part on U.S. technology have been developed in other countries. One example is TeamWARE Crypto, which is pro-

duced in Finland.[14] This product offers a number of algorithms as options, including Blowfish (448-bit keys), DESX™ (120-bit keys), D3DES (112-bit keys), and IDEA (128-bit keys available under separate license from Ascom). All of those algorithms are believed to provide strong encryption. With a simple and user-friendly interface, TeamWARE Crypto will undoubtedly proliferate globally. It is compatible with the most common operating systems currently available, including Windows 95 and NT.

Another example of a strong encryption product created and available outside the United States is F-Secure Desktop, which runs under Windows 95 or NT. It was created by Data Fellows of Espoo, Finland, and is distributed in more than 50 countries. F-Secure offers the option of choosing either of two symmetric block ciphers: Blowfish or Triple DES. It is inexpensive, easy to use, and easily available inside and outside the United States.

Public-Key Crypto Systems

Asymmetric crypto systems, also known as "public-key" systems, are called "asymmetric" because one key is used to encrypt the message, whereas a different key is used to decrypt it. Every user creates a key pair that has a special mathematical relationship. One key is published freely (the public key); the other mathematically related key (the private key) must be kept private by the owner. Someone wishing to communicate securely uses the public key to encrypt the message, and only the related private key can decrypt it. Asymmetric crypto-systems have the advantage of not requiring keys to be exchanged before secure communications. Conversely, one of the weaknesses of symmetric systems is the inability to find a secure channel to communicate the key.

The RSA (named for Ron Rivest, Adi Shamir, and Len Adleman, its creators) was one of the first public-key systems. The RSA algorithm was developed in the United States and is considered one of the most formidable public-key systems. But there are other public-key systems thought to be equally formidable, such as the ElGamal system.

The security of public-key systems is based on the difficulty of solving certain complex mathematical problems; the harder the problem, the more secure the key. RSA's strenth lies in the difficulty of factoring the product of large prime numbers, given only the product. ElGamal's strength is based on the difficulty of solving the discrete

logarithm problem--that is, it is easy to raise a number to an exponent but difficult to find the exponent, given the result.[15] Other systems are based on other intractable problems.

The ElGamal system is not patented, which gives developers located in many countries an opportunity to use it as a basis for strong new encryption products.[16] Also, the RSA patent expires on September 20, 2000, making it a target of developers around the world.[17]

Indeed, the RSA algorithm is used around the world every time someone uses Phil Zimmerman's Pretty Good Privacy. PGP encompasses three different algorithms (including IDEA, which was not developed in the United States) to accomplish fast public-key encryption. The source code for PGP was placed on the Internet and has proliferated globally. Many believe PGP is the most commonly used encryption software in the world. Even recent versions of PGP are freely available outside the United States in spite of the regulations prohibiting their foreign distribution.

Public-key products have also been developed outside of the United States. A community of interest in New Zealand may prove significant in developing new public-key encryption systems. Two public-key systems have been developed there, and both show promise as competitors to RSA.

The first, called LUC, was developed by Peter Smith of Auckland.[18] That system uses the difficulty of solving problems involving Lucas functions,[19] instead of relying on the difficulty of factoring a product of two large prime numbers. Since 1993 LUC has been subjected to the scrutiny of the cryptographic community, whose members think LUC is as secure as the RSA system. Thus far, no successful attack has been published. New Zealand's export controls have proven no obstacle to LUC's being licensed around the world.

William M. Raike of Auckland created the second public-key system developed in New Zealand, RPK.[20] RPK uses a patented hard-to-crack feature called a "mixture generator,"[21] a complex combination of several cryptographic subgenerators. In cryptography, those generators create keys and provide random noise inputs for the cryptographic algorithm to operate on in creating keys. The security of RPK's algorithm depends on the difficulty of calculating the discrete logarithms in finite Galois Fields.[22] Again, the security of that relatively new algorithm has not yet been invalidated by any successful attack. The complexity of the mathematics involved indicates that RPK is every bit as

secure as RSA or LUC. Raike's company, RPK New Zealand Ltd., has also issued a challenge to the community at large, offering $10,000 (U.S.) to anyone who can break the RPK crypto-system. As has LUC, the system has been licensed for worldwide use and is being aggressively marketed internationally.[23]

The foregoing systems and others show that the development of strong crypto-systems continues worldwide in several communities of interest. The result of any U.S. ban on strong encryption or constraint on its use would be the further development of those systems. Export controls will not prevent the proliferation and use of cryptographic systems across international boundaries outside the United States.

Integration and Quality Issues

In theory, the development of encryption overseas might be hampered by the fact that more than 80 percent of the software used overseas is developed in the United States; perhaps the quality of overseas encryption is limited by failure to integrate well into U.S.-made software. But most strong encryption products will perform quite pleasingly within the standard environment produced by U.S. software manufacturers, including within Microsoft Windows and NT.

A recent example of strong encryption incorporated into a U.S.-produced software product is Netscape. Netscape is the most commonly used Internet browser today; it also can be used to send and receive e-mail. The "crippled" version of Netscape licensed for export can easily be brought to full strength using an ordinary PC. On March 31, 1998, Netscape made its software available in source code form; the version is known as Mozilla.[24] Because the source code contained no encryption routines, the export controls did not apply and the source code quickly found its way outside the United States.

Nine Australian software developers and three from the United Kingdom immediately formed the Mozilla Crypto Group for "fostering the development and integration of full-strength cryptography for this critical package from Netscape."[25] Fifteen hours after Mozilla was released, a Linux version dubbed Cryptozilla was ready for distribution. Shortly thereafter, versions for other platforms, including Windows 95 and NT, emerged. Now, anyone in the world can download a version of Netscape containing strong 128-bit encryption routines from the Internet.[26] That is an excel

lent example of how export controls can be superseded. Export controls do not and cannot work.

Indeed, insofar as export controls prevent U.S. software manufacturers from building encryption into all their word processing and network software, the greatest impact of export controls is to limit the quality of U.S.-made encryption. U.S. manufacturers may export only products of inadequate bit length for most applications, and they are discouraged from offering integrated products. The U.S. Data Encryption Standard, offering a 56-bit key, has been publicly defeated by three separate groups. In the first instance, it took 78,000 computers working in concert for 96 days. In the second instance, it took 50,000 computers working in concert for 39 days. On July 17, 1998, the DES was solved for a third time. That time, the code cracker found the key using one custom-built computer in only 56 hours (at a total cost of $210,000). The DES can no longer be considered adequate cryptographic protection. The plans and technical specifications for the custom-built machine are available around the world. I live in New Zealand, and I have a copy of those plans.[27]

Many software applications that originate in the United States are exported to countries worldwide. A number of the products, including Netscape and the Microsoft Office suite, have built-in cryptography. Both Word and Excel (two applications included in the suite) have a cryptographic feature, which in export versions must be reduced to 40-bit encryption (outside the United States, that condition goes by the politically incorrect term "crippledware"). Most computer users know about the feature and its limitations. Those who want cryptography that has not been deliberately diminished in its capacity to protect their information have the products described in this paper and many others to choose from. Encryption features built into general applications like word processors are convenient. But special-purpose encryption software is just as strong and is designed to overcome any inconvenience built into the U.S.-produced general applications. The cryptographic genie cannot be put back into the bottle.

Conclusion

The arguments for limiting the proliferation and use of strong encryption are mainly emotional. Supporters of export controls insist that strong encryption should be freed for export only with built-in key escrow features. The administration has now announced that all key escrow

products will be exportable after one-time review. In a key escrow system, a third party must be given the secret key that decrypts the encrypted messages. That third party may then give the key to law enforcement agents, unbeknown to either the sender or receiver, to stop the "bad guys" from doing or planning anything harmful. To gain public acceptance of that notion, supporters portray key escrow and export controls as essential to save us from terrorists, drug dealers, child pornographers, and others.

However, those who have argued for key escrow in whatever incarnation have failed to show any proof, scientific or otherwise, that "bad guys" are too stupid to seek out strong encryption without key escrow features. In reality, "bad guys" are unlikely to use anything less than the strongest encryption for their communication and data storage. Conspirators involved in planning capital crimes will not be worried about violating anti-cryptography laws. To conceal their use of illegal cryptography, they could super-encrypt their messages: first encrypt a message with a strong algorithm, and then encrypt that result using the key escrow version.[28]

Even the National Security Agency admits that key recovery schemes will not solve law enforcement's problems with encrypted information. An NSA report on key recovery issued in February 1998 lists at least 18 examples of how such a system could be thwarted.[29] The lone player insisting on key escrow is the Federal Bureau of Investigation. The FBI has not yet shown any material basis for imposing restrictions on cryptographic use by private citizens, nor has it proven that any restrictions imposed would in fact be effective.

Where does that leave us? The result is export control laws that demand an intolerable sacrifice of freedom and privacy for a token, ineffectual commitment to security. Owing to widespread availability of cryptography abroad, criminals and terrorists are unaffected by the rules. But innovative cryptographers in the United States--and many who would use their products around the world--remain bound in red tape. The First Amendment to the United States Constitution guarantees the right to communicate without government interference: "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances." Encryption software and hardware simply enable one to speak in a language unknown to the government. The Constitution

gives the government no power to demand that we provide a translation. Speech in the dialect of IDEA should be free around the world. And it will be. Export controls hurt the United States far more than they help.

Notes

1. C.F.R. secs. 120-30 (1996); see also http://www.eff.org/pub/Crypto/ITAR_export/itar_registry_govt.document.

2. Executive Order 13026, "Administration of Export Controls on Encryption Products," November 15, 1996, http://www.bxa.doc.gov/Encryption/eo13026.htm.

3. A 1982 report (by a panel whose members included academics, researchers, and experts in national security such as Elmer B. Staats, formerly of the National Security Council; Samuel C. Phillips, a former director of the National Security Agency; and William J. Perry, former secretary of defense) concluded that export controls work only when the United States is the only source of information about the technology, or other friendly nations that could also be the source have control systems as secure as ours. National Research Council, Panel on Scientific Communication and National Security Committee on Science, Engineering, and Public Policy, Communications and National Security (Washington: National Academy of Sciences, 1982), p. 65.

4. Pointers to Cryptographic Software, April 15, 1998, Finland,http://www.cs.hut.fi/ssh/crypto/software.html#crypto++.

5. A Commerce Department report noted that, in many of the countries surveyed, "exportable U.S. encryption products are perceived to be of an unsatisfactory quality." Elizabeth Corcoran, "Encryption Rules Hurt Exporters, Study Says," Washington Post, January 17, 1996, p. A11.

6. U.S. Department of Commerce, Bureau of Export Administration, Annual Report, March 4, 1998, p. 257.

7. Of the products surveyed, 21 purportedly used DES, whereas the remaining 7 used proprietary systems. U.S. Department of Commerce and National Security Agency, "A Study of the International Market for Computer Software with Encryption," unclassified report, in The Electronic Privacy Papers, ed. Bruce Schneier and David Banisar (New York: John Wiley & Sons, 1997), pp. 629-34.

8. A 1996 survey by Trusted Information Systems, Inc., notes that "the quality of foreign products seems to be comparable to U.S. products." National Research Council, Computer Science and Telecommunications Board, CRISIS: Cryptography's Role in Securing the Information Society (Washington: National Academy Press, 1996) pp. 127-28. An updated survey finds 656 foreign products, of which 281 use DES. http://www.tis.com. Contesting the idea that foreign-made encryption is of inferior quality, James Bidzos of RSA notes that foreign developers can simply study U.S. patents. James Bidoz, Statement before the Subcommittee on Science, Technology, and Space of the U.S. Senate Committee on Commerce, Science, and Transportation, Hearing on S. 1726, The Promotion of Commerce Online in the Digital Era Act of 1996, or "PRO-CODE," June 12, 1996, transcript, p. 61.

9. See Global Internet Liberty Campaign, "Cryptography and Liberty: An International Survey of Encryption Policy," Washington, February 1998.

10. Ascom Systec AG, IDEA (International Data Encryption Algorithm), April 14, 1998, Switzerland, http://www.asco m.ch/ systec/security/ideafuture.html.

11. Bruce Schneier, Applied Cryptography, 2d ed. (New York: John Wiley & Sons, 1996), pp. 318-23.

12. Ibid., p. 319.

13. J. Kelsey, B. Schneier, and D. Wagner, "Key-Schedule Cryptanalysis of IDEA, G-DES,GOST, SAFER, and Triple-DES," Advances in Cryptology--CRYPTO 96 Proceedings (New York: Springer-Verlag, 1996), pp. 237-51; see also Schneier, p. 323 (discussing IDEA).

14. TeamWare Group, "TeamWARE Crypto," Helsinki, Finland, April 14, 1998, http://www.teamw.com/teamware/products/ twcrypto.htm.

15. In cryptography, the discrete logarithm problem is also known as an elliptic curve system. Solving the problem requires calculating two unique integers (a public key and a private key) that will generate a specific shared point on an elliptic curve. The shared "final point, when converted to an integer, acts as the secret key and can be used to pass information securely. . . . It's precisely the inability of the attack algorithms to solve the elliptic logarithm problem that allows the user to get essentially the same

security from a 163-bit ECC (elliptic curve crypto) system as they would from a 1024-bit RSA or DSA system." Roderick Simpson, "Privacy by Geometry: Elliptic Curves and Low Cost-per-Bit Crypto Strength," Wired, December 12, 1997, p. 112.

16. Public Key Partners, the owners of the five major public key patents, may take the position that the Diffie-Hellman patent covers this algorithm, but their patent on Diffie-Hellman expired on April 29, 1997.

17. Schneier, p. 474.

18. "The LUC Family of Public-Key Cryptographic Algorithms," April 9, 1998, New Zealand, http://www.luc.co. nz/whatis. html.

19. In cryptography, Lucas functions are used in a way similar to exponentiation. Lucas functions are equivalent to solving "the discrete log problem for a particular sub-field of a finite field." Bob Silverman of Mitre Corporation, "Newsgroups: sci.crypt," December 29, 1992, http:// www.funet.fi/pub/crypt/mirrors/ftp.dsi.unimi.it/ LUC/luc_ vs_rsa.

20. "RPK Public Key Cryptography," April 1998, New Zealand, http://crypto.swdev.co.nz/overview.htm.

21. Ibid.

22. Ibid.

23. E-mail from William Raike to Solveig Singleton, August 12, 1998.

24. Distributed Systems Technology Centre, "Australia Organizations Spearhead Project to Put Security Back into the Web," April 3, 1998, Australia, http://www.dstc.edu.au/ media_releases/Mozilla.html.

25. Mozilla Crypto Group, "Putting Strong Cryptography Back into Mozilla," April 11, 1998, http://mozilla-crypto. ssleay.org/index.php.

26. Michael Stutz, "Cryptozilla Thwarts Feds Crypto Ban," Wired, April 3, 1998, http://www.wired.com/news/news/ technology/story/11465.html; and Mozilla Crypto Group; "Mozilla Crypto Group Achieves SSL Enabled 'Cryptozilla' in under 1 Day," April 2, 1998, http://mozilla-crypto.ssleay.

org/ press/19980401-02/index.php.

27. Electronic Frontier Foundation, Cracking DES: Secrets of Encryption Research, Wiretap Politics and Chip Design (Sebastopol, Calif.: O'Reilly & Associates, 1998).

28. National Research Council, CRISIS, p. 270; see generally Hal Abelson et al., "The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption," Center for Democracy and Technology, Washington, June 1998.

29. National Security Agency, "Threat and Vulnerability Model for Key Recovery," February 18, 1998, http:// www.fcw.com/pubs/fcw/1998/0413/web-nsareport-4-14-1998.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. Contact the Cato Institute for reprint permission. Printed copies of Cato Briefing Papers are $2.00 each ($1.00 each for five or more). To order, or for a complete listing of available studies, write the Cato Institute, 1000 Massachusetts Avenue, NW, Washington, DC 20001-5403. (202) 842-0200, FAX (202) 842-3490.

E-mail cato@cato.org
World Wide Web http://www.cato.org.